# General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance

Khairur Razikin[1*] and Agus Widodo[2]
[1−2]Computer Science Department, BINUS Graduate Program - Master of Computer Science,
Bina Nusantara University
Jakarta 11480, Indonesia
Email: [1]khairur.razikin@binus.ac.id, [2]awd2098@gmail.com

***Abstract*—The use of technology in the era of the Industrial Revolution 4.0 is essential, marked by the use of technology in the economy and business. This situation makes many companies in the payment sector have to improve their information technology security systems. In Indonesia, Bank Indonesia and the Financial Services Authority (Otoritas Jasa Keuangan - OJK) are agencies that provide operational permits for companies by making Payment Card Industry-Data Security Standard (PCI-DSS) certification as one of the requirements for companies to obtain operating permits. However, not all companies can easily get PCI-DSS certification because many companies still do not meet the PCI-DSS requirements. The research offers a methodology for measuring the level of technology and information maturity using general cybersecurity requirements adopted from the cybersecurity frameworks of CIS, NIST, and Cobit. Then, the research also performs qualitative calculations based on interviews, observations, and data surveys conducted on switching companies that have been able to implement and obtain certification. PCI-DSS to produce practical cybersecurity measures, in general, can be used as a measure of the maturity of technology and information security. The results and discussion provide a model assessment tool on the procedures and requirements needed to obtain PCI-DSS certification. The maturity level value of PT XYZ is 4.0667 at maturity level 4, namely quantitatively managed, approaching level 5 as the highest level at maturity level.**

***Index Terms*—General Cybersecurity Maturity Assessment Model, Best Practice, Payment Card Industry-Data Security Standard (PCI-DSS)**

Received: Jan. 11, 2021; received in revised form: March 21, 2021; accepted: April 06, 2021; available online: Aug. 30, 2021.
*Corresponding Author

## I. INTRODUCTION

THE development of the world of science and technology globally has increased very rapidly. It is applied in almost all sectors of life, especially in the economic and business sectors. This development can be seen from all forms of transactions that can be done using e-money or payment cards. One proof of technological developments in the financial world is the emergence of switching companies. A switching company is a form of company that provides technological facilities in processing payments using cards.

Then, the Payment Card Industry-Data Security Standard (PCI-DSS) is a set of security standards regulated by the Payment Card Industry Security Standards Council (PCI SSC). It aims to secure credit and debit card transactions from data theft and fraud [1]. However, PCI SSC does not have the legal authority to compel providers to comply with this rule. It is a requirement for any business that processes credit or debit card transactions. PCI certification is also considered the best way to protect sensitive data and information. It helps businesses to build long-lasting and trusting relationships with their customers. Therefore, in Indonesia, through Bank Indonesia and the Financial Services Authority (Otoritas Jasa Keuangan - OJK), PCI-DSS certification is one of the requirements in the operation of payment card services [2, 3]. However, in practice, many companies still have difficulty understanding the concept and application of PCI-DSS. Some companies only focus on improving technology, increasing revenue, and automating transaction processes without reviewing and improving the human element. The control process for information technology security is often overlooked. They also lack a first-step

guide to implementing PCI-DSS compliance.

PCI-DSS has 12 high-level requirements, and some companies fail to meet the minimum necessary security controls to secure cardholder data while the data are transmitting, in processing, and being stored. The company's inability to enforce security controls can lead to the failure of PCI-DSS compliance. Weaknesses that may occur from internal and external factors due to failure of exercising controls must be identified as soon as possible to avoid information security leaks that can cause time, cost, and effort loss and put the company's business at risk [4–6].

The research offers an independent measurement method of information security maturity adopted from the integrated capability maturity model based on the general cybersecurity framework model, along with things that need to be applied to the organization. The research focuses on measuring the maturity level of information security in companies in implementing 12 high-level PCI-DSS requirements. The proposed PCI-DSS approach model suggests a mechanism for measuring information security using the proposed model to achieve PCI-DSS compliance. Research with the proposed model by providing real examples of the application of PCI-DSS compliance has never been done before. Hence, the research can be be used as a model assessment tool in implementing information security and procedures for obtaining PCI-DSS certification.

## II. Literature Review

### *A. Payment Card Industry (PCI) Regulation for Switching Company in Indonesia*

The switching company provides the infrastructure that functions as a center or link for forwarding payment transaction data through a network using card-based payment instruments, electronic money, or fund transfers [3]. To realize a safe payment system, the government, through Bank Indonesia and the Financial Services Authority, have issued regulations on the implementation of payment services, including:

1) Bank Indonesia regulation number 19/8/PBI/2017 concerning the national payment gateway [7],
2) Financial Services Authority regulation number 77/POJK.01/2016 on information technology-based lending and borrowing services [2],
3) Bank Indonesia regulation number 18/40/PBI/2016 concerning the implementation of payment transaction processing [3].

Those regulations explain the implementation of information system security standards by switching providers, payment gateway operators, electronic wallet operators, and banks operating proprietary channels at least. The fulfillment of certification and system security and reliability standards are generally accepted or stipulated by Bank Indonesia or the authorities or related institutions [2, 3, 7].

TABLE I
The Level of Payment Card Industry-Data Security Standard (PCI-DSS).

| Level | Criteria |
|---|---|
| 1 | Merchants process over 6 million card transactions per year. |
| 2 | Merchants process 1 to 6 million transactions per year. |
| 3 | Merchants handle 20,000 to 1 million transactions per year |
| 4 | Merchants handle fewer than 20,000 transactions per year. |

### *B. Payment Card Industry-Data Security Standard (PCI-DSS) Compliance*

PCI-DSS is an information security standard for organizations that handle branded credit cards from major card schemes. The PCI standards are mandated by card brands but administered by the PCI SSC. PCI SSC was founded in 2006 by American Express, Discover, JCB International, MasterCard, and Visa Inc. The founding members share ownership, governance, and performance of the organization's work equally. Each incorporates the PCI-DSS as part of the technical requirements for their respective data security compliance programs. The mission of the PCI SSC is to enhance the data security of global payment accounts by developing standards and support services that promote education, awareness, and effective implementation by stakeholders [8].

Payment security is very important for the merchant, financial institution, or other entity that stores, processes, or transmits cardholder data. The PCI-DSS helps to protect the security of the data. It defines operational and technical requirements for organizations that accept or process payment transactions and software developers and manufacturers of applications and devices used in those transactions [9]. There are four levels of PCI compliance, as shown in Table I.

The PCI-DSS includes technical and operational system components that are included in and or connected to cardholder data [9]. The purpose of the PCI-DSS is to protect cardholder data wherever the data are processed, stored, or transmitted. The control and security processes required by PCI-DSS are critical to protecting cardholder account data, including PAN – the main account number printed on the front of the payment card. Merchants and other service providers involved with payment card processing may not store sensitive authentication data after authorization. It includes sensitive data printed on the card or stored on the chip or magnetic stripe of the card and a

Cite this article as: K. Razikin and A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance", CommIT (Communication & Information Technology) Journal 15(2), 91–104, 2021.

TABLE II
PAYMENT CARD INDUSTRY-DATA SECURITY STANDARD (PCI-DSS) GOAL AND REQUIREMENT.

| ID | Goal | ID | Requirement |
|---|---|---|---|
| G1 | Build and Maintain a Secure Network | R1 | Install and maintain a firewall configuration to protect cardholder data |
| | | R2 | Do not use vendor-supplied defaults for system passwords and other security parameters |
| G2 | Protect Cardholder Data | R3 | Protect stored cardholder data |
| | | R4 | Encrypt transmission of cardholder data across open, public networks |
| G3 | Maintain a Vulnerability Management Program | R5 | Use and regularly update antivirus software or programs |
| | | R6 | Develop and maintain secure systems and applications |
| G4 | Implement Strong Access Control Measures | R7 | Restrict access to cardholder data by business need-to-know |
| | | R8 | Assign a unique ID to each person with computer access |
| | | R9 | Restrict physical access to cardholder data |
| G5 | Regularly Monitor and Test Networks | R10 | Track and monitor all access to network resources and cardholder data |
| | | R11 | Regularly test security systems and processes |
| G6 | Maintain an Information Security Policy | R12 | Maintain a policy that addresses information security for employees and contractors |

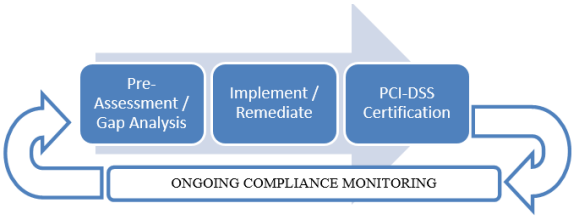


Fig. 1. Payment Card Industry-Data Security Standard (PCI-DSS) compliance life cycle.

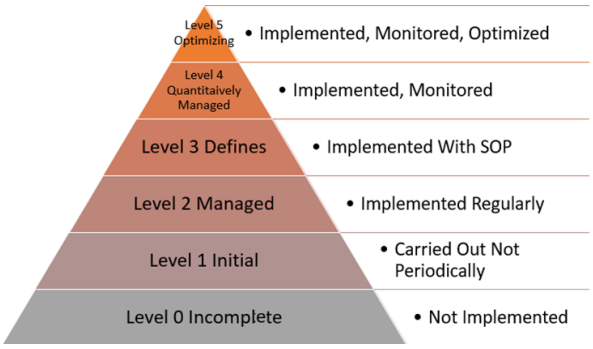


Fig. 2. Capability level.

personal identification number entered by the cardholder. There are 6 main objectives which are divided into 12 requirements in PCI-DSS [10]. The objectives can be seen in Table II. Then, the implementation of compliance with PCI-DSS is carried out regularly to ensure that technology and information security are maintained (see Fig. 1).

### *C. Cybersecurity Maturity Model of Payment Card Industry (PCI)*

This proposed cybersecurity maturity model is intended as a tool for evaluating an organization's ability

TABLE III
CAPABILITY LEVEL.

| Level | Description |
|---|---|
| 0 | Incomplete: Incomplete approach to fulfill the intent of the practice area. |
| 1 | Performed: The initial approach to fulfill the intent of the practice area |
| 2 | Managed: Apply level 1 practice. A simple but comprehensive practice that addresses the full intent of the practice area. |
| 3 | Defined: Built on level 2 practices. Using organizational standards and adapting to address project and job characteristics. Focusing on achieving project objectives and organizational performance. |
| 4 | Quantitatively Managed: Built on level 3 practice. Using statistical and other quantitative techniques to understand performance variation and detect, correct, or predict focus areas to achieve quality and process performance objectives. |
| 5 | Optimizing: Built on level 4 practice. Using statistical and other quantitative techniques to optimize performance and improve to achieve quality and process performance objectives. |

to meet its security objectives. The proposed model defines the processes that manage, measure, and control all aspects of security. It relies on four core indicators for benchmarking and as an aid to understanding security needs in organizations. These indicators are driven by the goal to achieve security needs.

Capability Maturity Model Integration (CMMI) has a capability level or ability level. Capability level applies to the achievement of institutional performance and process improvement in individual practice areas. These practice areas are converted into practice groups labeled level 0 to level 5. It provides an evolutionary pathway for performance improvement. Each level builds on the previous level by adding new functions that result in increased abilities. The capability level has six levels for each core process, as shown in Fig. 2 and described in Table III [11, 12].

The CMM-PCI model places the institution in five

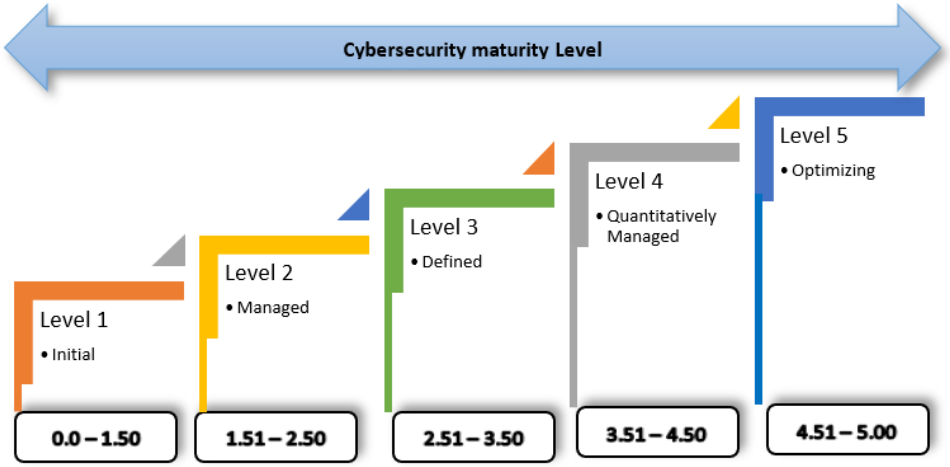


Fig. 3. Cybersecurity maturity level.

TABLE IV
CYBERSECURITY MATURITY LEVEL – PAYMENT CARD INDUSTRY (PCI).

| Level | Description |
|---|---|
| 1 | Initial: In this condition, the institution at this level has not implemented CMMI. |
| 2 | Managed: Institution has several processes that are often used in every development project, but there is no overall uniformity. |
| 3 | Defined: Institution has implemented a defined process, and all teams understand how the process should work. |
| 4 | Quantitatively Managed: Institution is increasingly structured and open to the existing system. It begins to apply the concept of quantification to each process that is always monitored and controlled in every work process. |
| 5 | Optimizing: This level is the peak level in the CMMI model. At maturity level 5, the institution has achieved all specific and generic goals at levels 2, 3, 4, and 5. It focuses on continuous process improvement through technological innovation and process optimization that are constantly monitored and analyzed. Hence, it can provide an optimal system. |

maturity levels. The degree of maturity in CMMI is shown in Fig. 3 and described in Table IV [11]. Based on Fig. 3, each maturity level is determined by the criteria for being vulnerable to weight values to identify the results of the analysis and interpretation of interview data and questionnaires on information system management. There are 0.0 to 1.50 for level 1, 1.51 to 2.50 for level 2, 2.51 to 3.50 for level 3, 3.51 to 4.50 for level 4, 4.51 to 5.00 for level 5.

### *D. Previous Research*

In the first previous research, the best practice model of PCI-DSS compliance is carried out with quantitative and qualitative approaches that utilize different instruments in data collection to analyze and assess information on security capabilities (maturity) [4, 13]. This model consists of four maturity levels - None, Initial, Basic, and Capable. The proposed Information Security Maturity Model-Payment Card Industry (ISMM-PCI) model is intended as a mechanism or tool for measuring and determining organizational information security maturity.

The model helps organizations to easily identify key success factors and gaps (weak points), provide guidelines for better managing information security, and formulate the best strategy for improvement to achieve PCI-DSS compliance. The main advantage of ISMM-PCI over other ISMMs is its ease of use. However, this model does not describe every process required as an initial step towards preparation for PCI-DSS certification.

The second previous research offers a Holistic Cybersecurity Maturity Assessment Framework (HCY-MAF) based on a process methodology called Capability Maturity Model (CMM) [14]. The proposed model consists of 15 security categories and 6 maturity levels. The model is implemented on an online platform.

Then, it can be used as a self-assessment and auditing tool, facilitating organizations to perform gap analysis and receive automated compliance reports and graphical representations of their security postures. The information to be gathered from the platform can be used, following the aggregation and anonymization processes of the National Cyber Security Center (NCSC), to identify current security issues and prioritize future security plans and funding actions. However, this previous research does not present an example of what an organization must do to comply with cybersecurity.

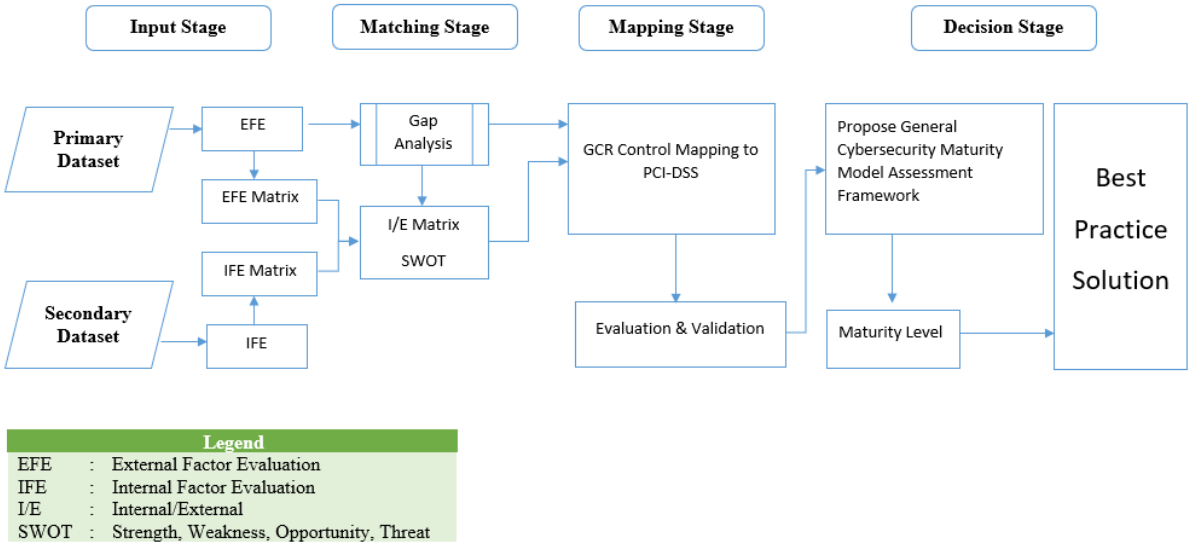


Fig. 4. Research stages.

TABLE V
CAPABILITY LEVEL VALUE.

| Level | Activity |
|---|---|
| 0 | Incomplete Process |
| 1 | Performed Process |
| 2 | Managed Process |
| 3 | Established Process |
| 4 | Predictable Process |
| 5 | Optimizing Process |

## III. RESEARCH METHOD

### A. Model Development Framework

In Fig. 4, it consists of four stages. The first stage is the input stage. The stage collects primary data as External Factor Evaluation (EFE) and secondary data as Internal Factor Evaluation (IFE). EFE is obtained through a literature study on the standard cybersecurity framework requirements, while IFE is cybersecurity implementation data in agencies. Furthermore, the second stage is the matching stage by conducting a gap analysis to produce a General Cybersecurity Requirement (GCR). The GCR is analyzed on EFE and IFE data to produce a SWOT matrix. In the third stage, the mapping stage is when the GCR mapping process is carried out against the PCI-DSS. Then, the evaluation and validation are conducted by the expert in the cybersecurity field. The last stage is the decision stage. It is the analysis stage by using GCR as a general cybersecurity maturity model assessment framework to determine the value of index maturity at agencies so that they can provide best practice solutions in achieving PCI-DSS compliance.

### B. Data Collection Method

The research uses a questionnaire method that is adjusted to the standard cybersecurity framework. It is adopted by the cybersecurity maturity model method. The sizes in this model include ordinal sizes and nominal sizes. The ordinal size is the number given. The number means the grade. The nominal number 0 is used for the object with the lowest level, and the number 5 is used for the object with the highest level. Table V shows the capability level value.

The selection of the sample of respondents uses the purposive sampling technique. The selection of a sample of respondents is done by referring to personal competencies that interact directly with IT governance [11]. In the research, interviews are conducted with stakeholders concerned with the IT division at PT XYZ. From the interview, two respondents, who are directly concerned with the field of information system security in the institution, are obtained [15].

## IV. RESULTS AND DISCUSSION

### A. The Proposed General Cybersecurity Requirement Maturity Model

Cybersecurity maturity assessment identifies the level of strength and weakness of the cybersecurity process in an organization. It determines how closely the cybersecurity process is related to identify best practices. A cybersecurity maturity assessment is usually conducted to identify areas where cybersecurity processes can be improved. The research proposes a general cybersecurity maturity assessment model that can be used to inform cybersecurity gaps about how

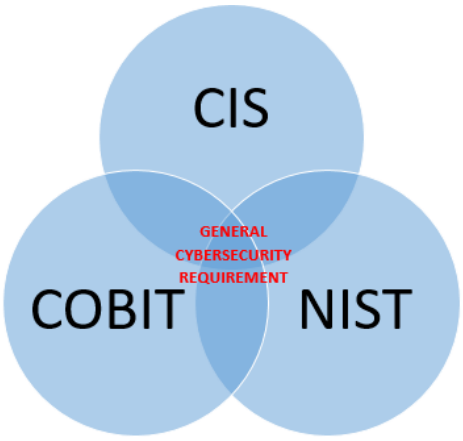


Fig. 5. Cybersecurity framework.


Fig. 6. Domain of general cybersecurity requirement.

well an organization's cybersecurity processes are with best-practice processes. The model can also be used as a gap analysis tool and a check against existing PCI-DSS compliance. Thus, organizations can use the model to determine how well the terms of the contract are met.

This cybersecurity standard integrates industry standards and best practices to help organizations manage their cybersecurity risks. It provides a common language that enables staff at all levels in an organization and all points in the supply chain to develop a common understanding of cybersecurity risks. Regulations on technology security standards and information systems are adopted to standard cybersecurity frameworks, including CIS, NIST, Cobit, and others [16, 17]. This framework is developed into several security standard regulations that can be implemented in organizations following the object of information technology security. Figure 5 shows the cybersecurity framework.

Based on the adoption of technology and information security standards, a general cybersecurity framework can be formed, which is divided into three categories, namely IDENTIFY & DETECT, PROTECT & RESPOND, and RECOVER. For the record, the DETECT category in the NIST framework is combined with the IDENTIFY category with the assumption that the identification process is a process that is not much different from the DETECT process. Then, the RESPOND category is combined with the PROTECT category, assuming that the PROTECT process is a description of the RESPOND process so that it is related to one another. Figure 6 illustrates the domain of general cybersecurity requirements.

Based on the main domains in Fig. 6, a table of requirements and sub-requirements can be formed to define in more detail the control areas. It can be seen in Table VI. It shows the composition of the GCR framework that consists of three factors, namely domain, requirements, and sub-requirements. Domain factor has three parts which are modifications of the NIST cybersecurity framework. Meanwhile, the requirement factor has 15 requirements and detailed sub-requirements of the requirements. These two factors are a combination of formulas from three cybersecurity frameworks: NIST, CIS, and COBIT.

Domain data in general cybersecurity requirements are mapped against the PCI-DSS requirements, as shown in Table VII. The research maps the goals and requirements of the PCI-DSS into the GCR. PCI-DSS has 6 goals and 12 requirements. Those are aligned to 3 domains and 15 requirements contained in the GCR. The codes of G1 to G6 are PCI-DSS goals, and codes of R1 to R12 are PCI-DSS requirements.

The resulting area domain is then analyzed using the SWOT method. External factor evaluation data are obtained from a literature study of the cybersecurity frameworks (NIST, CIS, and COBIT). Then, the data are combined with internal factor evaluation data obtained through the interview process and direct observation. It results in the GCR framework. Furthermore, those data are the object of analysis in the SWOT analysis method to produce a SWOT factor, as shown in Table VIII.

### *B. The Result of Direct Observations.*

Table A1 in the Appendix shows the observation results of mapping the GCR against the PCI-DSS aligned with the company's implementation. The implementation has been approved by Qualified Security Assessor (QSA) as evidence to obtain PCI-DSS certification. This observation is also accompanied by interviews with IT officers about everything needed

Cite this article as: K. Razikin and A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance", CommIT (Communication & Information Technology) Journal 15(2), 91–104, 2021.

TABLE VI
GENERAL CYBERSECURITY REQUIREMENT (GCR).

| Domain | Requirement | Sub-Requirement |
|---|---|---|
| IDENTIFY & DETECT | ID 1: Asset Management | |
| | ID 2: Risk Management | |
| | ID 3: Supply Chain Management | |
| | ID 4: Logging and Audit Management | ID 4.1: Logging Management<br>ID 4.2: Network Time Protocol (NTP) Management |
| | ID 5: Threat Management | ID 5.1: Anti Virus Management<br>ID 5.2: Intrusion Prevention System (IPS)/Intrusion Detection System (IDS) management |
| | ID 6: Security Testing | ID 6.1: Security Assessment<br>ID 6.2: Compliance Checking |
| PROTECT & RESPOND | PR 7: Management Policy and Procedure | |
| | PR 8: Identity Management and Control Access | PR 8.1: Access Control<br>PR 8.2: Authentication Mechanism<br>PR 8.3: Authorization |
| | PR 9: Physical Environment Security | PR 9.1: Monitoring Infrastructure<br>PR 9.2: Segregation System |
| | PR 10: System & Application Security | PR 10.1: Segmentation Network<br>PR 10.2: Management Patch<br>PR 10.3: System Security<br>PR 10.4: Application Security |
| | PR 11: Data Security | PR 11.1: Encryption<br>PR 11.2: Data Classification |
| | PR 12: Management People | PR 12.1: Security awareness training Program<br>PR 12.2: Tracking People |
| | PR 13: Change Management | |
| RECOVER | R 14: Incident Management | R 14.1: Incident Response Management<br>R 14.2: Backup and Restore Mechanism |
| | R 15: Business Continuity & Disaster Recovery | R 15.1: Business Continuity Plan<br>R 15.2: Disaster Recovery Centre |

TABLE VII
MAPPING GENERAL CYBERSECURITY REQUIREMENT (GCR) TO PAYMENT CARD INDUSTRY-DATA SECURITY STANDARD (PCI-DSS).

| Goal | Requirement | General Cybersecurity Requirement |
|---|---|---|
| G1 | R1 | ID1<br>PR9.1<br>PR9.2 |
| | R2 | ID10.3 |
| G2 | R3 | PR11.2 |
| | R4 | PR11.1 |
| G3 | R5 | ID5.1<br>PR10.2 |
| | R6 | PR10.1<br>PR10.3<br>PR10.4 |
| G4 | R7 | PR8<br>PR9.2 |
| | R8 | PR7<br>PR8 |
| | R9 | PR7<br>PR9 |
| G5 | R10 | ID4.1<br>PR9.1 |
| | R11 | ID4.1<br>ID6.1<br>ID6.2<br>PR10.2 |
| G6 | R12 | PR7<br>PR12.1<br>PR12.2<br>PR13<br>R4 |

to achieve PCI-DSS certification, including technical and management requirements. It is done to obtain a score for the conformity of the GCR to the PCI-DSS compliance that the company has implemented. Each GCR component implemented by the company will get a weighted value to measure the company's maturity level.

### C. Topology

PT XYZ applies topology based on segregation and private connection. Each system is separated from the functions and network segmentation. Every connection to a banking institution uses a dedicated Multiprotocol Label Switching (MPLS) of peer-to-peer links. Meanwhile, interconnection from card payment equipment uses a dedicated Access Point Name (APN) provided by the telecommunications provider. The company has also implemented security at the network layer using the Cisco ASA Firewall and Cisco Switches and mitigated corporate cyberattacks using the Cisco FireSIGHT intrusion prevention system. The used infrastructure is a virtual machine-based infrastructure in the On-Premise Data Center. Besides, PT XYZ has also implemented high availability infrastructure by building Disaster Recovery Centre DRC with a distance of 30 km from the main data center. The technology infrastructure and information system built by PT XYZ can affect the value of the agency's maturity level on the compliance of cybersecurity compliance standards.

TABLE VIII
MATCHING STAGE PROCESS.

| Method of Analysis | | General Cybersecurity Requirement | | | |
|---|---|---|---|---|---|
| | | Strengths | Weaknesses | Opportunities | Threats |
| EFE<br>IFE | (NIST + CIS + COBIT) Interview, Questionnaire, and Direct Observation | Make it easy for users in doing the checklist cybersecurity standards | Need a more detailed explanation against the implementation domain in the area | Be self-assessment of other regulations | Allow for missed domains or subdomains against specific requirements |

IFE + EFE = Cybersecurity Framework + I + Q + D = GCR

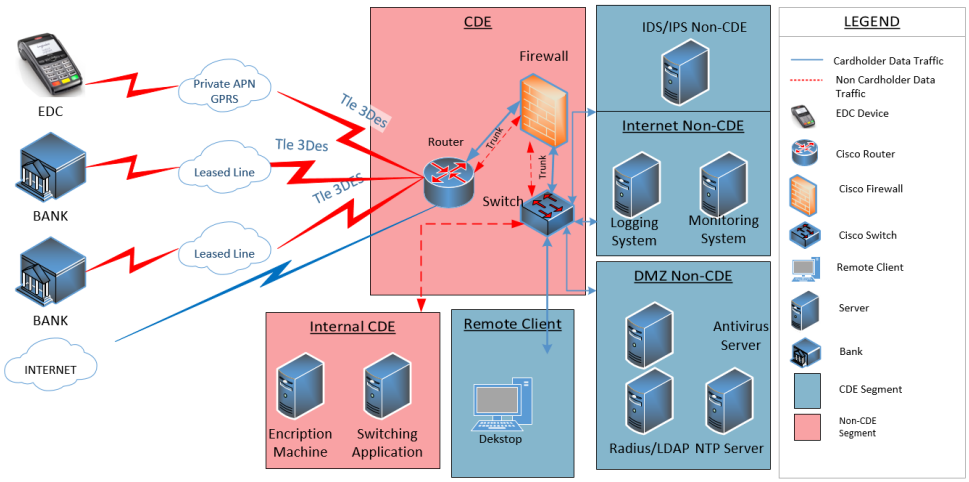


Fig. 7. Topology of PT XYZ.

The following is the main data center infrastructure topology owned by PT XYZ in Fig. 7.

### D. Maturity Model Data Processing

Analysis and interpretation of interview data and questionnaires to information system managers can be used as research findings. Based on the calculation of the maturity level, the gap can be seen and can determine the expected value to be made. PT XYZ has met information security standards required criteria as shown in Table A1 in the Appendix. The results of the questionnaires given to and filled in by respondents get results as seen in Table IX. Due to limitations, data pages are not displayed as a whole.

Table IX shows the result of respondents' answers for each GCR requirement. The respondents' answers are on a scale of 0 to 5 for each question according to the level of application of GCR requirements in the company. The implementation scale level refers to the capability level value in Table V. Based on the value obtained from the respondents, there will be a tendency for the respondent's answer. Furthermore, based on this value, the calculation is carried out to obtain the maturity existing index value for each domain using a Likert scale in Eq. (1).

$$\text{Index} = \frac{\sum \text{Answers to most questions}}{\sum \text{Question}} \quad (1)$$

From the index calculation on the questionnaire data, the results are as shown in Table X. The index value obtained in Eq. (1) is the existing maturity level for each domain. The existing maturity level is the current maturity level. This value is used to obtain the maturity level gap.

Table X shows the result of the current maturity index value for each GCR requirement. The value given by the respondents is divided by the number of questions for each requirement. Next, based on Table X, the research will look for the existing index or maturity level values in each domain of ID, PR, and R by adding the cumulative values in each domain using Eq. (2). The results are in Table XI.

$$\text{Maturity Domain} = \frac{\sum \text{Index of each domain}}{\text{Number of requirements}} \quad (2)$$

Table XI refers to the maturity index value for each domain in the GCR obtained through Table X. The Identify and Detect (ID) domain gets a maturity

TABLE IX
QUESTIONNAIRE RESULTS.

| GCR | Value from Respondents |
|---|---|
| ID 1 | 5 |
| ID 2 | 0 |
| ID 3 | 0 |
| ID 4 | 10 |
| ID 5 | 10 |
| ID 6 | 10 |
| PR 7 | 5 |
| PR 8 | 10 |
| PR 9 | 10 |
| PR 10 | 20 |
| PR 11 | 10 |
| PR 12 | 4 |
| PR 13 | 4 |
| R 14 | 10 |
| R 15 | 10 |

TABLE X
THE EXISTING INDEX MATURITY.

| GCR | Value from Respondents | Number of Questions | Index/ Maturity Existing |
|---|---|---|---|
| ID 1 | 5 | 1 | 5 |
| ID 2 | 0 | 1 | 0 |
| ID 3 | 0 | 1 | 0 |
| ID 4 | 10 | 2 | 5 |
| ID 5 | 10 | 2 | 5 |
| ID 6 | 10 | 2 | 5 |
| PR 7 | 5 | 1 | 5 |
| PR 8 | 10 | 2 | 5 |
| PR 9 | 10 | 2 | 5 |
| PR 10 | 20 | 4 | 5 |
| PR 11 | 10 | 2 | 5 |
| PR 12 | 4 | 2 | 2 |
| PR 13 | 4 | 1 | 4 |
| R 14 | 10 | 2 | 5 |
| R 15 | 10 | 2 | 5 |

TABLE XI
INDEX OF MATURITY DOMAIN.

| Domain | Index Maturity |
|---|---|
| ID | $5+0+0+5+5+5/6 = 3.3333$ |
| PR | $5+5+5+5+5+5+2+4/7 = 4.4286$ |
| R | $5+5/2 = 5$ |

index value of 3.33, and the Protect and Respond (PR) domain achieves 4.42. Meanwhile, the Recover (R) domain has a maturity index of 5. All three values of the index are used to find the past maturity value gap for each domain. Based on the results of the maturity index for each domain in Table XI, it can be compared with the target of the maturity index. Then, the maturity gap for each domain is obtained, as shown in Fig. 8.

The level of security can be determined by the maturity level of all activities carried out in the GCR with Eq. (3). The achievement value of 4.0667 means that the maturity level of the GCR is at the level of quantitatively managed. This level means that institutions are increasingly open to technological developments by applying

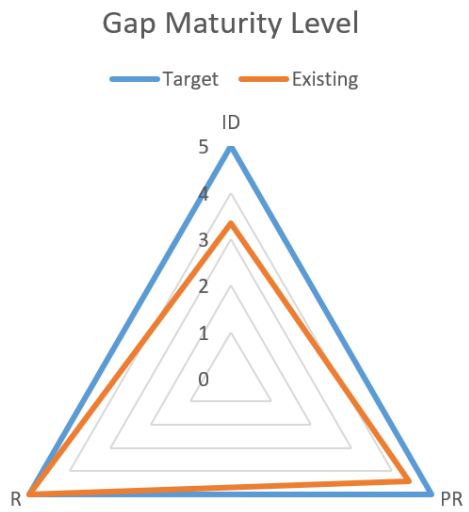


Fig. 8. Gap maturity model.

the concept of quantification in each process and monitoring each process. It can be concluded that the general cybersecurity maturity model assessment framework can be a best practice solution in achieving PCI-DSS compliance. The maturity level is taken from i(ID1)+i(ID2)+i(ID3)+i(ID4)+i(ID5)+i(ID6)+i(PR7) +i(PR8)+i(PR9)+i(PR10)+i(PR11)+i(PR12)+i(PR13) +i(R14)+i(R15). The data are 5+0+0+5+5+5+5+5+5+5+5+2+4+5+5.

$$\text{Maturity Level of GCR} = \frac{\sum \text{Maturity level}}{\text{Number of domain}} = \frac{61}{15} = 4.0667 \quad (3)$$

### E. Evaluation and Validation

The proposed model defines 15 sets of metrics to measure organizational competence or maturity in terms of a set of best practices, skills, or standards in PCI-DSS compliance. Metrics are organized into categories and measured on a performance scale. The level metric is based on empirical data that has been validated in practice, and each level in the model is more mature than the previous level. By applying the framework proposed, agencies can achieve progressive increases in cybersecurity maturity. For example, at maturity level 3, the organization has moved from management that the organization has several often-used processes in every development project, but there is no overall uniformity.

Based on the experience gained from this project and to ensure the accuracy of the proposed method, the researchers conduct interviews with IT experts

Cite this article as: K. Razikin and A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance", CommIT (Communication & Information Technology) Journal 15(2), 91–104, 2021.

TABLE XII
THE RESULT OF VALIDATION.

| GCR | Information Security Triad | | |
|---|---|---|---|
| | Confidentiality | Integrity | Availability |
| ID 1 | | | ✓ |
| ID 2 | | | ✓ |
| ID 3 | | | ✓ |
| ID 4 | | ✓ | |
| ID 5 | | ✓ | |
| ID 6 | | ✓ | ✓ |
| PR 7 | | ✓ | ✓ |
| PR 8 | ✓ | | |
| PR 9 | ✓ | | |
| PR 10 | ✓ | | |
| PR 11 | ✓ | | |
| PR 12 | | ✓ | ✓ |
| PR 13 | | ✓ | |
| R 14 | | ✓ | ✓ |
| R 15 | | ✓ | ✓ |

TABLE XIII
THE RESULTS OF INTERVIEWING THE EXPERT.

| No | Question | Expert's answer |
|---|---|---|
| 1 | What are the regulations that must be obeyed by institutions related to the Republic of Indonesia's state policy for the business of switching companies? | It is to ensure the security of information technology by following information security certification. |
| 2 | What do institutions need to do to meet the PCI-DSS requirements? | Implementing PCI-DSS compliance is based on the PCI-DSS Guideline by utilizing existing best practices. |
| 3 | How does the PCI-DSS certification cycle work? | PCI-DSS certification is an assessment process carried out on an ongoing basis to ensure that cardholder data security remains safe. |
| 4 | Who is responsible for customer data security? | It is every entity that is involved in the transaction process, from payment to the settlement. |
| 5 | How are the ways to control PCI-DSS compliance? | Control is carried out by monitoring regularly. |
| 6 | Can this general cybersecurity requirement be used as an independent assessment of other technology and information security regulations such as ISO 27001 and GDPR? | If it is mapped against ISO 27001, it only covers 30%. However, if it is the mapping against GDPR, it is around 80%. |
| 7 | Based on the general security requirements that have been made, in your opinion, are there any domains that are missed? | For a case study, a switching company is sufficient. |

as a validation and evaluation method so that it can be developed into a broader framework. The interview is conducted by performing the domain accuracy contained in general cybersecurity requirements for cybersecurity modes, namely confidentiality, integrity, and availability or what is known as the CIA triad. Tables XII and XIII are the results of interviews conducted with Mr. Taro Lay as an IT Expert in Indonesia.

Table XII is the result of the validation of the requirements in the GCR against the security principle. Each requirement in each domain in the GCR is aligned with security principles. It is done to validate whether each requirement in the GCR has at least one security principle, so it can be said that it is feasible as a requirement in the security aspect. The results show that every requirement in the GCR domain meets at least one security aspect.

Besides, the validation and evaluation methods are also carried out by giving several questions to the expert. The questions are given to find out whether there are missed technical and management requirements that may have to be met by the company to get PCI-DSS certification (see Table XIII). It also sees the possibility of developing a suitable model to be used as other security certification requirements.

## V. CONCLUSION

PCI-DSS is a security standard used for companies engaged in the payment card industry established by the PCI SSC. PCI-DSS certification is one of the requirements for companies engaged in payment card services as stipulated in Bank Indonesia regulations and the Financial Services Authority regulations as regulatory holders in Indonesia. However, not all companies are able and easy to get PCI-DSS certification because there are still many companies that do not meet the PCI-DSS requirements. The research offers a methodology for measuring the level of technology and information maturity using general cybersecurity requirements adopted from the cybersecurity frameworks of CIS, NIST, and COBIT.

There are 6 goals which are divided into 12 requirements that must be met to achieve PCI-DSS compliance. In the case study of PT XYZ as a company engaged in the payment card (switching company), the general cybersecurity maturity model can be used as an independent assessment to measure maturity and readiness and a reference in achieving PCI-DSS compliance. Using the general cybersecurity maturity model assessment framework, the maturity level value of PT XYZ is 4.0667. It is at maturity level 4, namely quantitatively managed, approaching level 5 as the highest level at maturity level. This result is relevant because of PT. XYZ has received the PCI-DSS compliance certificate. Hence, it can be concluded that the general cybersecurity maturity model assessment framework can be a best practice solution in achieving PCI-DSS compliance.

This proposed method can also be adopted for cybersecurity compliance in other countries. In future research, it is expected that the GCR framework can be developed for other cybersecurity compliance such as ISO 27001, GDPR, or others by adding regulatory

factors for each country. The regulatory factors for each country may be different to achieve cybersecurity compliance.

## ACKNOWLEDGEMENT

Thank you to Mr. Taro Lay for giving his time and knowledge to validate and evaluate the general cybersecurity requirements framework in the research. Mr. Taro is a member of the Information System Security Association (ISSA) - Indonesian Chapter to contribute to cybersecurity education in Indonesia. Then, he is also a virtual world education trainer implemented in Europe, East, and Southeast Asia.

## REFERENCES

[1] PCI Security Standards Council, "Document library." [Online]. Available: https://www.pcisecuritystandards.org/document_library

[2] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum," 2016. [Online]. Available: https://bit.ly/3j4wrgG

[3] Bank Indonesia, "Peraturan Bank Indonesia No. 19/10/PBI/2017 tentang Penerapan Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme bagi Penyelenggara Jasa Sistem Pembayaran Selain Bank dan Penyelenggara Kegiatan Usaha Penukaran Valuta Asing Bukan Bank," 2017. [Online]. Available: https://www.bi.go.id/id/publikasi/peraturan/Pages/pbi_191017.aspx

[4] S. Yulianto, C. Lim, and B. Soewito, "Information security maturity model: A best practice driven approach to PCI DSS compliance," in *2016 IEEE Region 10 Symposium (TENSYMP)*. Bali, Indonesia: IEEE, May 9–11, 2016, pp. 65–70.

[5] S. Thakar and T. Ramos, *PCI compliance for dummies*. John Wiley and Sons, 2011.

[6] J. Liu, Y. Xiao, H. Chen, S. Ozdemir, S. Dodle, and V. Singh, "A survey of payment card industry data security standard," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 3, pp. 287–303, 2010.

[7] Bank Indonesia, "Peraturan Bank Indonesia nomor 18/40/PBI/2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran," 2016. [Online]. Available: https://www.bi.go.id/id/publikasi/peraturan/Documents/PBI_184016.pdf

[8] PCI Security Standards Council, "About us." [Online]. Available: https://www.pcisecuritystandards.org/about_us/

[9] ——, "Maintaining payment security." [Online]. Available: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

[10] ——, "PCI DSS quick reference guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1," 2018. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

[11] R. Umar, I. Riadi, and E. Handoyo, "Analisis keamanan sistem informasi berdasarkan framework COBIT 5 menggunakan Capability Maturity Model Integration (CMMI)," *Jurnal Sistem Informasi Bisnis*, vol. 1, pp. 47–53, 2019.

[12] O. M. Al-Matari, I. M. Helal, S. A. Mazen, and S. Elhennawy, "Adopting security maturity model to the organizations' capability model," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 193–199, 2021.

[13] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," *Future Internet*, vol. 12, no. 9, pp. 1–21, 2020.

[14] A. Aliyu, L. Maglaras, Y. He, I. Yevseyeva, E. Boiten, A. Cook, and H. Janicke, "A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom," *Applied Sciences*, vol. 10, no. 10, pp. 1–15, 2020.

[15] M. F. Saleh, "Information security maturity model," *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 3, pp. 316–337, 2011.

[16] L. Elluri, A. Nagar, and K. P. Joshi, "An integrated knowledge graph to automate GDPR and PCI DSS compliance," in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018, pp. 1266–1271.

[17] R. H. Diputra, "Analisis manajemen risiko pada sistem "bring your own device" menggunakan metode cybersecurity framework NIST: Studi kasus di PT XYZ," mathesis, Magister Sistem Informasi, Universitas Bina Nusantara, 2018.

## APPENDIX

The Appendix can be seen in the next pages.

Cite this article as: K. Razikin and A. Widodo, "General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance", CommIT (Communication & Information Technology) Journal 15(2), 91–104, 2021.

TABLE A1
DIRECT OBSERVATIONS.

| PCI-DSS Goal | PCI-DSS Requirement | General Cybersecurity Requirement | Observation Result |
|---|---|---|---|
| G1: Build and Maintain a Secure Network | R1: Install and maintain a firewall configuration to protect cardholder data | ID 1: Asset Management | The company has used firewalls and implemented rules including:<br>1. Access list source of any destination and any action deny to protect incoming traffic from unknown sources<br>2. Only open the ports needed according to the business justification table<br>3. Update the firmware regularly<br>4. Do a firewall review twice in 1 year<br>The company has created High Level Diagram (HLD) and Detail Level Diagram (DLD) infrastructure topologies<br>The company uses IPS devices to detect a series of external networks |
| | | PR 9.1: Monitoring Infrastructure | The company applies CCTV surveillance for the frontend and backend of the data center<br>The company closes wireless access to the PCI infrastructure |
| | | PR 9.2: Segregation System | The company implements separated production systems and operational systems with two separated firewalls |
| | R2: Do not use vendor-supplied defaults for system passwords and other security parameters | PR 10.3: System Security | The company has changed all the default passwords contained in the system from network devices or supporting applications<br>The company has created and implemented a password policy<br>The company has integrated each user and password in the central user management using radius and Lightweight Directory Access Protocol (LDAP) |
| G2: Protect Cardholder Data | R3: Protect stored cardholder data | PR 11.2: Data Classification | Not Applicable: The company does not store cardholder data on the system |
| | R4: Encrypt transmission of cardholder data across open, public networks | PR 11.1: Encryption | The company applies a masked data format according to ISO 8583 standards<br>The company uses a dedicated encryption machine (HSM) to encrypt data<br>The company applies a standard encryption method with a minimum of 3DES double-length key<br>The company uses a private communication line for each cardholder data transmission from end to end |
| G3: Maintain a Vulnerability Management Program | R5: Use and regularly update antivirus software or programs | ID 5.1: Anti Virus Management | The company has used antivirus with a license and has a centralized antivirus management<br>The company schedules the antivirus database scanning and updating activities on the antivirus management system |
| | | PR 10.2: Management Patch | The company regularly updates the operating system and antivirus applications<br>The changes made to the system are regulated in the change management policy |
| | R6: Develop and maintain secure systems and applications | PR 10.1: Segmentation Network | The company implements network segmentation in the form of VLANs for each function of the infrastructure system (DMZCDE, DMZnonCDE, Internal, and InternalCDE) |
| | | PR 10.3: System Security | For each operating system and supporting application, a hardening process has been carried out according to the CIS benchmark standard |
| | | PR 10.4: Application Security | The company uses a secure protocol by installing a Secure Socket Layer (SSL) certificate |
| G4: Implement Strong Access Control Measures | R7: Restrict access to cardholder data by business need-to-know | PR 8: Identity Management and Control Access | Not applicable: The company does not do application development. The application used can be obtained from the vendor |
| | | PR 9.2: Segregation System | The company implements a standard for writing a username and password, which is integrated with the Radius and Lightweight Directory Access Protocol (LDAP) server as centralized user management combined with the 2 Factor Authentication (2FA) method following the established policy |

| PCI-DSS Goal | PCI-DSS Requirement | General Cybersecurity Requirement | Observation Result |
|---|---|---|---|
| G5: Regularly Monitor and Test Networks | R8: Assign a unique ID to each person with computer access | PR 7: Management Policy and Procedure | The company makes several policies to be implemented to all employees and vendors, including:<br>1. Technology usage policy<br>2. Incident management policy<br>3. Information security policy<br>4. Access control policy<br>5. Secure procedure of credit card data deletion<br>6. Backup procedure<br>7. Inspection for tamper terminal<br>8. Data retention retrieval and secure disposal policy<br>9. Media disposal procedure<br>10. Physical security policy<br>11. Physical access procedure<br>12. Operational security procedure<br>13. Change management procedure |
| | | PR 8: Identity Management and Control Access | The company implements a standard for writing a username and password that is integrated with the Radius server as centralized user management combined with the 2 Factor Authentication (2FA) method following the established policy<br>The company has determined each user access according to responsibility |
| | R9: Restrict physical access to cardholder data | PR 7: Management Policy and Procedure | The company applies the technology usage policy, information security policy, physical access procedure, and physical security policy |
| | | PR 9: Physical Environment Security | The company applies a unique ID to each employee in accessing the computer data center with the following format: Username + Password + OTP<br>The company implements biometric authentication for every employee in accessing the data center computer with the following format: Fingerprint + PIN<br>The company implements a door alarm security system that reads if the data center door is open in more than 1 minute |
| | R10: Track and monitor all access to network resources and cardholder data | ID 4.1: Logging Management | The company implements a centralized logging system for every device in the datacentre based on Host Intrusion Detection System (HIDS) and File Integrity Manager (FIM)<br>The company uses internal NTP as a time centralization for each server and network device |
| | | PR 9.1: Monitoring Infrastructure | The company implements a network and monitoring system to monitor network and server conditions in the data center |
| | R11: Regularly test security systems and processes | ID 4.1: Logging Management | For logging management, companies use HIDS with a retention time of a year |
| | | ID 6.1: Security Assessment | The company has conducted Internal Vulnerability Assessment (IVA) regularly four times a year<br>The company has carried out an External Vulnerability Assessment (EVA) regularly four times a year<br>The company performs Wifi scanning regularly twice a year<br>The company carries out internal and external penetration testing four times a year |
| | | ID 6.2: Compliance Checking | The company uses the Qualified Security Assessor (QSA) vendor to carry out compliance checking activities periodically four times a year |
| | | PR 10.2: Management Patch | The company implements a change management policy for the changes made to the environment |

| PCI-DSS Goal | PCI-DSS Requirement | General Cybersecurity Requirement | Observation Result |
|---|---|---|---|
| G6: Maintain an Information Security Policy | R12: Maintain a policy that addresses information security for employees and contractors | PR 7: Management Policy and Procedure | Patch updates to the system are carried out regularly based on the vulnerability exposure updates |
| | | PR 12.1: Security awareness training Program | The company enters into a cooperation agreement for each vendor or merchant following applicable legal rules |
| | | PR 12.2: Tracking People | The company held IT security awareness training for employees and vendors once a year |
| | | PR 13: Change Management | The company does new employee checking by checking the track record in the one last year by attaching a police clearance certificate (Surat Keterangan Catatan Kepolisian - SKCK) |
| | | R 14: Incident Management | The company implements a change management policy for any changes and activities carried out on systems and infrastructure |
| | | | The company implements a centralized logging system for each device in the datacentre based on the Host Intrusion Detection System (HIDS) and File Integrity Manager (FIM) |