Moving Towards PCI DSS 3.0 Compliance: A Case Study of Credit Card Data Security Audit in an Online Payment Company

Muhammad R. Shihab, and Febriana Misdianti
Faculty of Computer Science
Universitas Indonesia

***Abstract*— E-commerce industry in Indonesia has grown rapidly since 2012. This development is also in line with the number of transactions that uses credit cards. Unfortunately, this phenomenon is followed by credit card frauds as well. Therefore, there is an urge for a standard to be used as a main reference in protecting the security of information.**

Visa and MasterCard have issued an international standard to ensure the security of credit card data, namely, PCI DSS. It emphasizes the importance of protecting cardholder information in one's daily business processes. On December 2013, the latest version of this standard was released, and brought about difficulties, even to those organizations that are already compliant to previous versions of the same standard.

The aim of this research is to be able to identify the changes brought about by the latest PCI DSS, namely, version 3.0. Furthermore, this research is intended to implement that very standard to measure an organization's compliance level. This research uses a case study approach in Indonesia largest company in online payment services. The results of this research are the summation of 182 new controls that are simplified for use by organizations that have complied with PCI DSS 2.0 and are preparing for PCI DSS 3.0. Additionally, we found that Company X, the object of our case study, is compliant towards 77.43% of PCI DSS 3.0 requirements.

Payment card industry data security standard is considered at its earlier stages. We believe that this research is one of the first in observing the changes brought about by PCI DSS 3.0 as well as in implementing it to measure an organization's compliance level.

I. INTRODUCTION

THE e-commerce market in Indonesia was merely $4 million in 2012, doubled by 2013, is expected to reach $18 million by 2015 and $25 million at the end of 2016 [1]. Such rapid development is followed by an increase of more than 30% in credit card payments [2]. However, payment system security industry isn't following this growth in the same pace. Visa and MasterCard noted that Indonesia seeds second in countries with the highest case of credit card fraud [3]. Bank Indonesia recorded more than 22,000 cases of credit card fraud in 2012. Disturbingly, it shows a 15% increase from the previous year [3].

Numerous credit card frauds happen due to a variety of causes, such as human factor or technology factor. 54% of credit card fraud occurs in a transaction with CNP (Card Not Present) method [4]. This method is usually used in online transactions. Therefore it is necessary to ensure the safety of a merchant's payment system.

One imperative step is to create a security standard. Visa and MasterCard have taken an early start by formulating Payment Card Industry - Data Security Standard (PCI DSS), a security standard to be implemented by all merchants that provide payment with credit cards. PCI DSS 1.0 was first published in 2005 and has undergone several improvements. The latest version was released in December 2013, and is commonly known as PCI DSS 3.0 [5]. PCI DSS 3.0 carries many differences that may baffle even those organizations who are already PCI DSS 2.0 compliant. Many hesitate to conduct an internal audit or continue to implement the new controls [4].

Company X is Indonesia's most respected and largest company within the field of online payments with more than 20 billion Rupiah worth of transactions in 2013. By the end of 2014, Company X targets to achieve 90 billion rupiah of transaction volume [6]. In early 2013, Company X has passed PCI DSS 2.0 audit.

This research aims to discover new controls in PCI DSS 3.0 and use those controls to audit an organization that is already compliant with PCI DSS 2.0, in this case is Company X. This research will also identify recommendations for each control that are not yet fulfilled. We believe that this research is one of the earliest of its kind, and will be useful to other organizations upon preparation to implement PCI DSS 3.0 as their security standard.

II. LITERATURE STUDY

This section describes the theories we used in conducting this research, such as understanding the theoretical basis of information security, audit, credit card data fraud, PCI DSS, compliance with PCI DSS, as well as the flow of credit card transactions.

 978-1-4799-8075-8/14/$31.00

A. Information Security

Based on the definition from Cherdantseva and Hilton, information security refers to the measures of digital privacy protection, implemented to prevent unauthorized accesses to computers, databases, and web sites [7]. Currently, data or information security has become the top priority for many organizations [7][8]. Furthermore, ISO 27000 framework explains information security as safeguarding information from all possible threats in an attempt to ensure business continuity, reduce business risk, and maximize or accelerate return on investment and business opportunities [9].

B. Information Security Audit

Audit is defined as an activity that is planned, documented, and carried out by expert personnel to determine the adequacy and adherence of an organization to a procedure or standard documents by investigating, examining, or evaluating the evidences objectively [10]. Additionally, audit is categorized into three types, which are financial audit, operational audit, and information technology audit. Information technology audit is a process of gathering and evaluating evidence to determine the security of a computer system owned by an organization that has been designed to maintain data integrity, security of assets, enabling the achievement of organizational goals effectively, as well as the efficiency of resource uses [11].

C. Payment Gateway

Payment gateway is a service provider that authorizes credit card payments for e-businesses, online retailers, bricks and clicks, or even traditional brick and mortar stores. It protects credit card information by encrypting them to ensure such information is delivered securely from the cardholder to the merchant and from the merchant to the payment processor [12].

D. Transaction with Credit Card

In conducting transactions using credit cards, there are four main processes consisting of authorization, batching, clearing, and funding. Authorization is the process to ensure that the perpetrator of the transaction is a legitimate cardholder. Furthermore, the processes of are batching, clearing, and funding are performed in order to make deposits and bill the right amount of money in the transaction.

E. PCI DSS 3.0

PCI DSS was developed to facilitate the measurement of credit card data security globally. PCI DSS provides a basis of technical and operational requirements designed to protect credit card data. PCI DSS can be used for all those connected with the credit card payment process, which are merchants, processors, acquirers, and service providers, as well as other parties who store, process and transmit data or sensitive authentication data (SAD) [13].

PCI DSS consists of a set of minimum requirements for cardholder data protection. Therefore, additional controls, laws or regulations may be needed locally or regionally for the prevention of additional risk. PCI DSS does not replace local or regional laws, regulations, or other legal requirements [13].

PCI DSS 3.0 document were issued in November 2013, but it should be widely implemented by November 2015. Currently, not a single organization in Indonesia complies with the latest PCI DSS 3.0 standard yet. PCI DSS version 2.0 was revised to version 3.0 because the earlier received numerous criticisms about the ambiguity in many of the audit points. Moreover, PCI DSS 3.0 was added with additional information, elaborating the instructions for each control. This was done to facilitate and guide auditors in conducting the assessment process in a more precise manner [5].

There are 12 main requirements of PCI DSS 3.0:

1. *Install and maintain a firewall configuration to protect cardholder data.*
   Firewall is a device that controls traffic between the internal network and external network. More than that, firewall also controls traffic in and out of sensitive areas within the internal network. It is a key protection mechanism for all network computers. Therefore, the firewall must be included into a PCI DSS audit scope as the first requirement [5].
2. *Do not use vendor-supplied defaults for system passwords and other security parameters*.
   Intruders (external and internal) often use vendor default passwords or other vendor default settings to enter the system. Passwords and settings are well known by hacker communities and are easily obtained from public information [5].
3. *Protect stored cardholder data.*
   Protection methods such as encryption, cutting, masking, and hashing are needed to protect data cardholder. If a smuggler managed to open the security control and gain access to the encrypted data, the data can not be read without the related cryptographic key [5].
4. *Encrypt transmission of cardholder data across open, public networks.*
   Sensitive information that can be accessed by intruders easily must be encrypted during transmission. Wireless network configuration errors and weaknesses in the regulation of encryption or authentication protocol can cause persons to gain access to the data cardholder environment [5].
5. *Protect all systems against malware and regularly update anti-virus software or programs.*
   Malicious software (malware) which consists of viruses, worms, and trojans can enter the network during the business activity and lead to attacks on

 978-1-4799-8075-8/14/$31.00

the system. Therefore, antivirus should be used on all systems as protection against malware threats [5].

6. *Develop and maintain secure systems and applications.*
   Intruder may use security vulnerabilities to gain access to the system. Most of these vulnerabilities can be fixed with a security patch provided by the vendor. Therefore, security patches need to be installed to manage the security of the system [5].
7. *Restrict access to cardholder data by business need to know.*
   Systems and processes have to restrict access based on the business needs and in accordance with job responsibilities to ensure critical data can only be accessed authorized persons [5].
8. *Identify and authenticate access to system components.*
   Unique identification should be given to each employee. It is to ensure that each individual can be held liable for any actions. The effectiveness of password can be determined by the design and implementation of the authentication system. [5]
9. *Restrict physical access to cardholder data.*
   All physical access to data or systems that store data of cardholders should be limited, because it serves as an opportunity for individuals to access devices or data, and delete systems or hardcopies [5].
10. *Track and monitor all access to network resources and cardholder data.*
    Recording mechanism and the ability to track user activities are critical to preventing, detecting, or minimizing the impact of data theft. The existence of logs in all environments enables the company to conduct a thorough tracking, warning, and analysis in the event of a fault [5].
11. *Regularly test security systems and processes.*
    Vulnerabilities are always found by both intruders and researchers. In addition, new vulnerabilities are often introduced by new software. Therefore, system components, processes, and software needs to be checked periodically to ensure security controls are still implemented and adapt to a changing environment [5].
12. *Maintain a policy that addresses information security for all personnel.*
    Strong security policies will provide assurance to the entire entity and inform personnel about what is expected of them. All personnel must know and understand the sensitivity of every data and have a responsibility to protect the data [5].

Previous versions PCI DSS standard has been modified based on inputs from industry partners [14]. Some of the reasons that drive PCI DSS standards change include the lack of knowledge and awareness, weak authentication method, third-party security challenges, weak self-detection against malware, and inconsistency in assessment

The core of the 12 security requirements remain the same, but the new version of the PCI DSS will provide some additional sub-requirements that were found previously lacking. According to [15], the changes in PCI DSS 3.0 are categorized as follows:

- *Clarification*: Provide clarification on the intent of the requirements. Ensure that short words in standard describe the requirement's intended meaning.
- *Additional Guidance*: Explanation, definition, or instruction to improve comprehension or provide further information or guidance on a particular topic.
- *Evolving Requirement*: Changes to ensure that standards are always updated in accordance with emerging threats and changes in the market.

III. Research Methodology

This research uses a qualitative approach, in order to increase the understanding of the problem and to be able to analyze deeper and more comprehensively [16]. Additionally, qualitative approach is used because the data collected is descriptive in manner, such as through interviews and observations. We did not modify any data sources, information, and audit evidence obtained from the company as suggested by [11]. Qualitative research approach suited to obtain information regarding the level of credit card data security that is stored or managed [16]. Thus, we feel that we were able to get a comprehensive and complete data analysis in accordance with the actual conditions in Company X. In conducting this research, we chose a case study approach by using PCI DSS 3.0 as research instrument and Company X as our research object.

In this research, data collection techniques used include interviews, observations of the area, and observations of documents related to the security of credit card data in Company X [16]. Meanwhile, the techniques of data analysis are as follows:

1. Forming transcripts of data collection.
2. Matching the compliance of Company X with the controls of PCI DSS 3.0.
3. Formulating recommendations for each control that has not been fulfilled.

 978-1-4799-8075-8/14/$31.00

TABLE I
SUMMARY OF COMPANY XYZ COMPLIANCE
TO PCI DSS 3.0

No	Requirements	Total Control	Percentage
1	Install and maintain a firewall configuration to protect cardholder data	11/11	100%
2	Do not use vendor-supplied defaults for system passwords and other security parameters	15/15	100%
3	Protect stored cardholder data	17/27	63%
4	Encrypt transmission of cardholder data across open, public network	2/2	100%
5	Protect all systems against malware and regularly update anti-virus software or program	7/7	100%
6	Develop and maintain secure systems and applications	14/17	82%
7	Restrict access to cardholder data by business need to know	0/5	0%
8	Identify and authenticate access to system components	12/14	86%
9	Restrict physical access to cardholder data	23/25	92%
10	Track and monitor all access to network resources and cardholder data	3/12	25%
11	Regularly test security systems and processes	19/19	100%
12	Maintain a policy that addresses information security for all personnel	3/10	40%

IV. ORGANIZATION PROFILE

Company XYZ is a company with services in online payments, providing merchant services to help customers enable online payment, by the use of credit cards, mobile banking, and e-wallet. Company X is in cooperation with the largest banks in Indonesia. Currently Company X has been providing online payment services for more than 100 merchants throughout Indonesia.

Company X is led by a CEO who directly oversees eight divisions. One of these divisions focuses on IT security and compliance. This division oversees several compliance officers who are responsible to ensure the compliance towards known regulations, such as PCI DSS.

V. ANALYSIS AND AUDIT RESULTS

This section will explain the audit process as well as the results.

A. Audit Plan

Prior to performing the audit, we conducted an audit plan consisting of three major steps, as follows:

1. The first step is to identify new requirements in PCI DSS version 3.0. We found 99 new points, consisting of 49 sub-requirements, and 50 sub-sub-requirements. When comparing these 99 points to PCI DSS 2.0 standard, we found 80 points that can be categorized clarifications, 18 points as evolving requirements, and 1 point as additional guidance [15]. We also verified that no requirements duplication occurred in these 99 points. Each sub-requirements and sub-sub requirements have multiple controls. Thus, the total of new controls in PCI DSS 3.0 when compared to PCI DSS 2.0 is 182 controls.
2. In the second step, we eliminated PCI DSS 2.0 controls that have no change at all. Therefore we simplified PCI DSS 3.0 framework which initially has 77 sub-requirements and 163 sub-sub-requirements into 49 sub-requirements and 50 sub-sub-requirements. The output of this process is a new document of PCI DSS 3.0 which contains 182 new controls only. This document will be very beneficial for organizations that have complied with PCI DSS 2.0 and are preparing for PCI DSS 3.0 compliance.
3. Finally, we devised testing procedures for each control, gathered from other literatures. This step is necessary because we felt many testing procedures have ambiguity in meaning. By adding this process, auditors will be facilitated to have more comprehension on the audit controls and testing procedures required.

B. Audit Scope

Audit scope is used to provide a focus for conducting this research. The audit in this research is

Company X. Audit framework used in this research is PCI DSS 3.0, limited to only new or changed controls from PCI DSS 2.0. There are 99 requirements and 182 controls obtained from the audit planning process as explained in the previous section. We discarded 18 controls that either require additional technology to test, or are not in accordance with Company X's business processes. Thus, the total controls used to perform the audit in this research are 164 controls.

C. Data Collection Process

The methods used for data collection process are interview, site observations, and document observations. We interviewed five individuals in this research. Two are from the engineering department and three others are compliance officers. Two researchers were involved in the data collection process. We refrained from occupying research assistant at this step as an effort to better ensure the reliability of the data collected. Furthermore, a thorough data validation process against those interviewed was also conducted.

 978-1-4799-8075-8/14/$31.00

D. Results of Credit Card Data Security Audit at Company X

Generally, we found Company X to have understood the importance of maintaining the security of customers' credit card data. Company X has implemented many main points of PCI DSS 3.0. In addition, we also have identified areas for improvements for Company X in order to meet the requirements of PCI DSS 3.0.

Overall, Company X is compliant towards 77.43% of PCI DSS 3.0 requirements. Table I presents a summary of the Company X's compliance towards the PCI DSS 3.0.

VI. RECOMMENDATIONS

This section will elaborate recommendations for Company X that can serve as inputs to improve their customer credit card data security. Recommendations are given based on our findings, current condition of Company X, and in accordance with the requirements of PCI DSS 3.0.

A. General Recommendations

- Company XYZ needs to perform knowledge sharing of PCI DSS 3.0 to all employees. This is imperative because the compliance of PCI DSS 3.0 needs to involve all elements of the company.
- Company X ought to make the requirements of PCI DSS 3.0 as business-as-usual. Thus, monitoring of cardholder data security and preparing for the audit will be easier.
- Company X must implement strict access controls to limit any access to cardholder data environment. Currently the implementation of access control in Company X is still very weak, both in the production environment and the development environment.
- The roles of a compliance officer that monitors cardholder data security is quite large, which includes collecting logs and scanning the various components of the system, making the required reports, monitoring any changes in system components, firewalls, routers, applications, and so forth. Meanwhile, the compliance officer's position also doubles as an engineer. This situation is not optimal for work due to excessive workload. Therefore, we recommend that Company X should:
    - Discharge compliance officers from their double duties, allowing them to focus more on monitoring cardholder data security.
    - Add new employees as compliance officers, to reduce their soaring work load.

B. Specific Recommendations

Specific recommendations are recommendations that need to be implemented by Company X in order to qualify for specific testing requirements. These recommendations have more details for each PCI DSS 3.0 requirements. This section gives recommendations for all controls are yet to be complied by Company X.

- *Requirement 3 (Protect stored cardholder data)*
  Company X is compliant to 17 of 27 controls. To comply with all controls in this requirement, Company X need to:
  1. Develop policies and procedures to not save SAD (Sensitive Authentication Data) after the authorization process.
  2. Apply all points mentioned in the key management and card data encryption policy.
  3. Prepare a procedure document to generate key-encrypting key and data-encrypting key as well as implementation of that procedure.
  4. Develop key distribution and key generation procedure.
  5. Change the key each time the crypto period has expired.
- *Requirement 6 (Develop and maintain secure systems and applications)*
  Company X is compliant to 14 of 17 controls. To comply with all controls in this requirement, Company X need to:
  1. Create policy and procedure documents that govern the implementation of access control in order to separate development and production environments. Those documents have to mention explicitly that there is segregation of duties in development and production environment.
  2. Provide secure coding training techniques to the developer and make documentation of such training
- *Requirement 7 (Restrict access to cardholder data by business need to know)*
  Company X is compliant to 0 of 5 controls. As can be seen, the implementation of access control in Company X is very weak. It affects the compliance status in requirement 7 as well. To comply with all controls in this requirement, Company X need to:
  1. Company X should create a policy document that identifies the definition of required access for each role, the limitation of access to each of them, and also implement them in daily business operations
- *Requirement 8 (Identify and authenticate access to system components)*
  Company X is compliant to 17 of 27 controls. The lack of Company X in fulfilling this requirement is that the company has not been handling the user authentication for remote access.
  To comply with all controls in this requirement, Company X need to:
  1. Implement two levels of authentication, especially for remote access from outside network
- *Requirement 9 (Restrict physical access to cardholder data)*
  Company X is compliant to 23 of 25 controls.

 978-1-4799-8075-8/14/$31.00

To comply with all controls in this requirement, Company X need to:

1. Provide training for personnel, so that they know the suspicious trials of destruction or replacement of devices.

- *Requirement 10 (Track and monitor all access to network resources and cardholder data)*
  Company X is compliant to 3 of 12 controls. This is due to a recently implemented in which audit logs are yet to be activated. To comply with all controls in this requirement, Company X need to:
  1. Enable audit trail for all individuals' accesses.
  2. Create a document that records all the privileges on the system, create a log for users' identification, authentication, and for all alterations, additions and deletions of account.
- *Requirement 12 (Maintain a policy that addresses information security for all personnel)*
  Company X is compliant to 3 of 12 controls. To comply with all controls in this requirement, Company X need to:
  1. Develop a policy document that defines a convention for labeling or naming inventory.
  2. Prohibit the copying, transferring, or saving cardholder data to local hard drives and removable electronic media when accessing data via remote access technology.
  3. Enforce Automatic disconnect to a session of remote access, if the user is inactive for fifteen minutes.
  4. Make a written agreement for every customer, acknowledging that Company X will monitor all PCI DSS requirements to secure cardholder data.

VII. CONCLUSION

This research shows that the evolving PCI DSS standard carries many changes. When compared to its predecessor, PCI DSS 3.0 has 182 new controls. Having understood the risks of credit card transactions, compliance towards the recent PCSI DSS 3.0 standard is imperative for those in the payment gateway industry.

Company X has a compliance rate of 77.43%. That value is limited to the 164 controls that are used. In addition, the company can implement the recommendations given as initial steps in meeting the PCI DSS 3.0 compliance.

The results in this research can be used as a reference for similar cases related to credit card data security in payment gateway companies. We suggest the future study of PCI DSS to be more quantitative, so that it can measure the severity level of the research object.

REFERENCES

[1] S. Sugden. (2013, Jun.) e27 Website. [Online]. "http://e27.co/indonesian-e-commerce-market-size-to-double-in-2013-to-us-8b/"

[2] T. P. Bhatla and V. Prabhu, "Understanding Credit Card Frauds," Jun. 2003.

[3] Y. P. Hendi, "A Better Credit Card Fraud Prevention Strategy for Indonesia," *Journal of Money Laundering Control*, vol. 15, no. 3, pp. 267-293, Aug. 2012.

[4] R. Docksey, "PCI DSS - Closing the Loop on 'Card Not Present' Fraud," in *IET*, UK, 2013, p. 27.

[5] PCI SSC. (2013, Nov.) PCI Security Standard Council. [Online]. "https://www.pcisecuritystandards.org/security_standards/documents.php?agreements=pcidss&association=pcidss"

[6] Veritrans, DailySocial. (2012, Aug.) DailySocial Website. [Online]. "http://api.dailysocial.net/en/wp-content/uploads/2012/08/eCommerce-in-Indonesia.pdf"

[7] Y. Cherdantseva and J. Hilton, "Information Security and Information Assurance. The Discussion about the Meaning, Scope and Goals," in *Organizational, Legal, and Technological Dimensions of Information System Administrator*. London: IGI Global Publishing, 2013.

[8] ISACA. (2014, Jun.) ISACA.org. [Online]. "http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Information-Security-Management-Audit-Assurance-Program.aspx"

[9] ISO/IEC 27000:2009, "Information technology - Security techniques - Information security management systems - Overview and vocabulary," 2009.

[10] D. H. Stamatis, *Six Sigma and Beyond: The Implementation Process Volume VII*. Edinburgh: CRC Press, 2002.

[11] S. Robinson and S. R. Robinson, *Principles and Practice of Information Security*. New York: Prentice Hal, 2007.

[12] Bank Card USA. (2014, Jul.) bankcardusa.com. [Online]. "http://www.bankcardusa.com/payment-gateway/"

[13] J. Hizver and T.-c. Chiueh, "Automated Discovery of Credit Card Data Flow for PCI DSS Compliance ," in *30th IEEE International Symposium on Reliable Distributed Systems*, Stony Brook, 2011, pp. 51-58.

[14] PCI SSC. (2013, Nov.) PCI Security Standar Council. [Online]. "https://www.pcisecuritystandards.org/documents/DSS_and_PA-DSS_Change_Highlights.pdf"

[15] PCI SSC. (2013, Nov.) PCI Security Standar Council. [Online]. "https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf"

[16] Qualitative Research Consultant Association, *What is Qualitative Research*. Philadephia: QRCA Press, 2014.