Risk Management of Credit Card Payment Gateway using Octave Allegro Methodology At Electronic Payment Provider Institution

Nilo Legowo , Kemas Airlangga Saputra

Abstract*: The use of internet technology is growing very fast which is driving the development of businesses in Indonesia, one of which is in the eCommerce sector. To support payment transactions conducted by e-commerce, in conducting this business, it is necessary to collaborate with business partner engaged in the payment gateways sector. Company partner engaged in the payment gateways sector to provide solutions to electronic financial transactions where one product is a credit card payment gateways. The purpose of this research is to make a risk assessment and risk management for audit certification credit card payment gateway Company. Risk assessment can help to know what are the risks that may occur, how big the impact of these risks, as well as recommendations related control measures must be carried out if the impact of these risks occur. This research using OCTAVE Allegro methodology to identify and evaluate information security risks credit card payment gateway. This research is qualitative research consisting of observation, conducting group discussion with the respondents. The respondend of this research are VP Development and Service Provisioning, VP Operation and Infrastructure, Manager Front End 1, Manager Back End 2, and Senior Programmer. Results of this research are 9 critical information assets in credit card payment gateway in COMPANY, such as : Card Holder Data & Customer Credential, Data Center, Physical Devices, Logical Storage, Logical Network, Supporting Software, Core Application, Encryption Key, and Human Resources. There are 21 risks that may occur during in credit card payment gateway. From 21 risks that were identified, obtained 15 risks are defer, 3 risks to be acceptable, and 3 risks should be mitigate.

***Keywords* : Risk Management, OCTAVE Allegro, Credit Card Payment Gateway.**

I. INTRODUCTION

The growth of ecommerce companies in Indonesia is so fast and is supported by a large number of millennial ages, so many people buy products online. and in making payment transactions using a credit card as a choice in making payments when transaction shopping online. can be demonstrated in 2016 the technology of financial transactions developed rapidly in Indonesia along with the development of financial technology. That makes, financial transactions shift from traditional cash transaction methods such as to online payment methods. Indonesian online payment methods such as escrow systems, virtual accounts, and credit cards instead of existing cards.

Many companies develop credit card payment gateways products because they see opportunities for the development of the credit card payment sector, including the increasing number of business startups in Indonesia that have sprung up with the majority in the eCommerce sector, so it becomes an opportunity to sell or offer credit card payment methods. by companies to startups in the eCommerce sector.

Based on the regulation from Bank Indonesia, all companies that conduct credit card payment gateways business are required to apply risk management in their IT systems

Company has already credit card payment gateway system, where system offered to provide comfort and security to customer, where keep verifying prudential aspects and protection aspects on consumer for application products. As stated in BI regulation clause, that the organizer final settlement provide IT and system in APMK (Card-Based Payment Instrument) must apply risk management in use IT which has reliability and security system based on result IT audit from an independent auditor and has required certification by the principal (Visa or Master Card) [1].

Now company has 2 certification such as ISO 27001:2013 (Information Security Management) v3.1 and PCI DSS (Payment Card Industry Data Security Standard) from TUV Rheinland Cert Gmbh but for credit card payment gateways just in scope of PCI certification v3.1 DSS because this is a requirement from BI to organize credit card payment gateway system. Currenty, the company requires of risk management that can be used by both certifications, where risk management is made using guidelines refer on requirement ISO 27001: 2013 [10] and PCI DSS v3.1 [13].

Because of various risk possibility happens on system, company feels it is necessary need strong identification and mitigation for serious threat on system and made control to risk. That information security is a priority, a threat to the security of the data on credit card payment gateways like corrupt or affect, directly or indirectly, such as hacking, viruses/worms, denial of service and spamming.

Manuscript published on November 30, 2019.
* Correspondence Author

Nilo Legowo *, Information Systems Management Department, Binus Graduate Program-Master of Information Systems Management, Bina Nusantara University,Jakarta Indonesia 11480,

Kemas Airlangga Saputra, Information Systems Management Department, Binus Graduate Program-Master of Information Systems Management, Bina Nusantara University,Jakarta Indonesia 11480,.

Therefore it is necessary for the implementation of risk management system credit card payment gateways.

There are several types of frameworks that can be used to conduct a risk assessment. In accordance with the risk management recommendations in clause 12.2 P.C.I. D.S.S. regarding risk assessment and management, where written the recommended risk management is OCTAVE, NIST SP 800-30, and ISO 27005 [13] with various considerations available in this study the framework used is OCTAVE Allegro.

The OCTAVE method (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is one method that can be used by companies as a framework for assessing a risk to information security [11]. OCTAVE is not a guideline or standard like ISO / EIC but a method as an orderly arrangement of parts or steps to achieve a financial, routine and systematic procedure to achieve something.

The purpose of this study is to apply overall risk management to credit card payment gateways in companies and conduct risk assessments using the OCTAVE Allegro framework. Implement the existing guidelines in Bank Indonesia, ISO 27001: 2013, and PCI DSS v3.1 regulations in the steps of the risk management framework that are created as controls for risks in credit card payment gateways if risks occur.

II. LITERATUR REVIEW

2.1 Information Security

Information security is the protection of information and critical characteristics it has (confidentiality, integrity, and availability), including the system and hardware that uses, stores and transmits information, through application policies, training and information security awareness programs, and technology [17]. Losses related to information security will continue to occur and their impact will destroy the organization [15]. Organizations need to identify and implement appropriate controls to ensure adequate information security [14].

Information security controls help organizations to provide the level of security the organization needs for their information [9]. Effective information security can be achieved through joint efforts from the information system owner, user, customer, security personnel, and other stakeholders responsible[4]. From the above it can be concluded that information security depends on information security controls applied by the company.

The influence of information owners and maintainers in using information and maintaining information also contributes to information security. And the impact of the unavailability of adequate information security controls, can provide losses that can continue to occur if the steps for implementing controls are not carried out [2].

2.2 Vulnerability

vulnerability is a particular way in which agents from threats can enter to attack information assets [17].

2.3 Threat

Threat is an indication of the possibility of an unexpected occurrence. Threats referring to situations (or scenarios) where a person can carry out unexpected actions (for example an attacker initiating denial of service against a company email server) or natural events can cause undesired results (for example fires that damage a company's information system hardware). A threat is created when someone exploits a vulnerability from a system [2].

2.4 Risk

Describes risk as a quantitative measurement of potential damage caused by threats, security loopholes, or from an event (having evil intentions or not) that affect a collection of information technology assets owned by the company. Exposure to risk (ie, being the subject of an event that creates a risk) causes potential loss, and risk is a measure of the "average" (typical) loss that can be expected from that exposure. Risk therefore, is a quantitative measure of damage that can occur to certain assets even after a number of information security precautions have been used by the organization [12].

2.5 Risk management

Risk management according to Carol Woody is an iterative process that addresses the analysis, planning, implementation, control and supervision of security policies [18]. The stages in conducting risk management for software development projects generally consist of 6 stages namely Identify, Analyze, Plan, Track, Control, Communicate. [19].

Describes risk as a possibility of damage or loss. This refers to situations where someone can do something that is not desirable or natural events can cause undesirable results, which results in negative impacts [3].

Describes risk as a function of the possibility of a threat that is associated with a potential security gap, and the impact resulting from the adverse event on the organization [7].

Payment Gateway Service is a 3rd party service that connects merchants with banks. With the availability of these services, merchants can provide online payment services on their online shopping website, by connecting their website to the payment gateway service using the service from the Application Program Interface (API). Payment gateway service is very needed, because of the high initial cost and maintenance costs to connect with the bank, besides that, a system that can connect bank accounts from customers and merchants is also needed [8]. Figure a relationships on the Internet payment system can see Fig.1. [5].

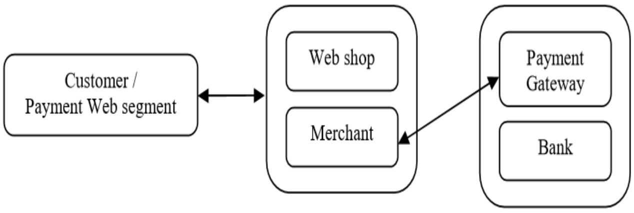

Fig.1. Relationships on the Internet Payment System [5]

Payment Gateways Transaction

The following are the stages (see figure 2.2) that occur from beginning to end when purchasing goods / services online [8]:

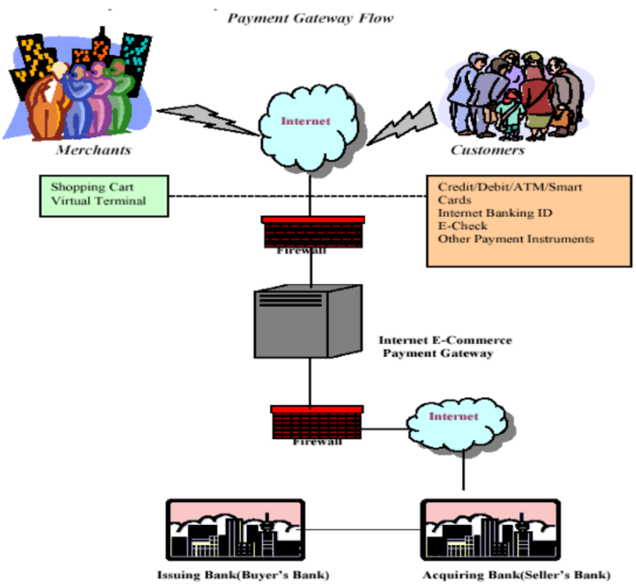
Payment Gateway Flow
Merchants
Internet
Customers
Shopping Cart
Virtual Terminal
Credit/Debit/ATM/Smart Cards
Internet Banking ID
E-Check
Other Payment Instruments
Firewall
Internet E-Commerce Payment Gateway
Firewall
Internet
Issuing Bank(Buyer's Bank)
Acquiring Bank(Seller's Bank)

Fig.2. Payment Gateway Flow [8]

III. METHODOLOGY

This research method uses literature study to get the releated and supporting the writing of this article. Literature study materials obtained from journals, articles, books, and other reference that supports the processing and analysis of data. Additionally, literature study on previous research is conducted to obtain the required information. This research is a qualitative research consisting of conducting group discussion to the respondents and some influence from previous studies. The methodology using *OCTAVE Allegro* framework to perform risk assessment on the risk of information security while ISO 27001:2013 and PCI DSS v3.1 clause as risk management recommendation and policy.

3.1 Octave Allegro

The method used in this research is *OCTAVE Allegro* because that can be used by companies as a framework for assessing a risk to information security, whereas standards such as ISO 27001:2013 are a set of rules widely recognized or involved (mainly because of excellence) that controls how people develop and manage materials, products, services, technologies, tasks, processes, and systems [11]. The difference between the risk management framework and standardization, is that the framework is a solution not as a method to regulate and communicate their risks. Standardization models such as ISO 27001:2013 are often not appropriate for managing information security risks but rather for information security [6].

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a methodology used to identify and evaluate information security risks. *OCTAVE Allegro* aims to assess the operational risk environment of a broad organization with the aim of producing better results without the need for extensive knowledge to conduct risk assessments [16].

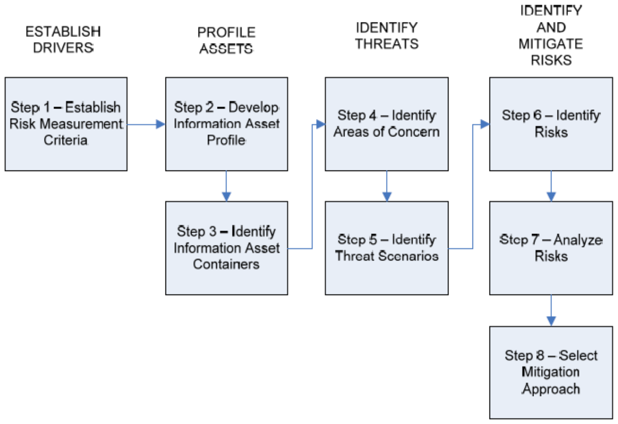
ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify Risks
Step 7 – Analyze Risks
Step 8 – Select Mitigation Approach

Fig.3. Picture I Step OCTAVE Allegro [17]

IV. RESULT AND DISCUSSION

There are 8 steps in OCTAVE Allegro. The first thing to do is doing a group discussion to the parties responsible and deal directly related to both systems, such as : VP Development and Service Provisioning, VP Operation and Infrastructure, Manager Front End 1, Manager Back End 2, and Senior Programmer. Group discussion conducted to Determine The Impact of Risk Criteria, Critical Information Assets, Risk Containers, An Area of Concern, and The Consequences of Those Risks.

4.1 Determination of Risk Measurement Criteria

The first thing to do is doing group discussion with *VP Development and Service Provisioning* and *VP Operation and Infrastructure*. In the group discussion process, the respondent filling risk measurement criteria worksheet and the impact area prioritization worksheet that has been provided by *OCTAVE Allegro*. From the group discussion results can be determined criteria for risk measurement.

There are two (2) activities at this stage, determination of the impact area and determination the priorities. There are five (5) Impact area selected : *Reputation and Customer Trust*; *Financial*; *Productivity; Safety and Health;* and *Fines and Criminal Penalties*.

There are three (3) level of impact of risk that is used in determining the impact area refers to *OCTAVE Allegro* framework, such as : *High*, *Medium*, and *Low*.

Impact areas of customer reputation and trust can be seen in detail in table I.

Table-I: Impact areas (reputation and customer trust)

Reputation and Customer Trust			
Impact Area	***Low***	***Medium***	***High***
Reputation	Reputation is slightly affected, there is no or need a small business effort to improve reputation	Reputation badly affected, and a business with a cost that is needed to improve reputation	Reputation is badly affected, and a business with a high cost for repair or almost impossible repaired
Customer Losses	Less than 2% customer reduction due to loss of confidence in the product	2% to 10% customer reduction due to loss of confidence in the product	More than 10% customer reduction due to loss of confidence in the product

The financial impact area there are 3 points to be used as a measurement, namely profit loss, operational costs, and one-time financial loss. The impact of the financial area can be seen in more detail in table II.

Table-II: Impact area (Financial)

Financial			
Impact Area	***Low***	***Medium***	***High***
Profit Loss	Profit loss < 0.05% per month from target revenue	Profit loss 0.05% to 1% per month from target revenue	Profit loss of more than 1% per month from the revenue target
Operational Costs	An increase of less than 2% in annual operating costs	An increase of 2% to 10% in annual operational costs	An increase of more than 10% in annual operating costs
One-Time Financial Loss	Less than Rp. 25,000,000,	Ranges between Rp. 25,000,000 - up to Rp. 50,000,000,	More than Rp. 50,000,000

the impact area of productivity there are 2 points that are used as a reference measurement, namely handling service disruptions and programmer turn over. Currently there are 4 programmers who handle credit card payment gateways, with the advancement of the payment method business, the likelihood of the temptation of competitors to inhouse programmers is increasing. Impact of productivity area can be seen in more detail in table III.

Table-III: *Impact area* (produktivity)

Produktivity			
Impact Area	***Low***	***Medium***	***High***
Disruption Handling Services	Can not service the transaction process for < 30 minutes	Can not service the service transaction process for 30 minutes to 60 minutes	Can not service the service transaction process for >60 minutes
Turn Over Programmer	*Turn over programmer* for one year <25%	*Turn over programmer* for one year 25% to 50%	*Turn over programmer* for one year > 50%

In the impact area of fines and legal sanctions there are 2 points to be used as a measurement reference, namely legal administration and acquirer cashback.

The impact of the penalty area and legal sanctions can be seen in more detail in Table IV.

Table- IV: Impact area (fines and legal sanctions)

Fines and Legal Sanctions			
Impact Area	***Low***	***Medium***	***High***
Legal Administration	Violations of articles relating to the implementation of credit card payment gateways.	Errors in the implementation of government regulations in the operational activities of credit card payment gateways resulting in a warning from the regulator (BI)	Failure to comply with government regulation which resulted in the revocation of the operator's permit by the regulator (BI).
Cashback Acquirer	Returns demand <2% per month of total transactions	Returns are equal to 2% or> 2% per month of total transactions so that you get a temporary suspend	Returns equal to 2% or> 2% per month of total transactions as much as 3 times so that the acquirer is revoked

At the impact of the safety and health area there is only 1 point to be used as a reference measurement, namely occupational health and safety. Because it can indirectly influence due to increased employee working hours. The impact of the area of safety and health can be seen in more detail in Table V.

Table -V: Impact area (Safety and health)

Safety and Health			
Impact Area	***Low***	***Medium***	***High***
Health & Safety (K3)	Employee health problems can be cured within 2 days due to the effect of increasing employee working hours Employee	health problems and can be cured with care due to the effect of increased employee working hours	Serious employee health problems that can lead to disability or even death

4.1.1 Determining Priority Scale of Impact Area

After all impact areas have been determined, the next activity is setting priorities for impact area. The most important impact area will have the higher priority value. *VP Development and Service Provisioning* and *VP Operation and Infrastructure* determining the priority scale impact area.

Table -VI: Priority scale for *impact areas*

Priorty	*Impact Areas*
5	Financial
4	Fines and Criminal Penalties
3	Reputation and Customer Trust
2	Productivity
1	Safety and Health

From table I, it can be seen that the *Financial* aspect has the highest priority for Company. This is because company ensure the failure of the transaction is only 1% every Month to Customers. Second priority is *Fines and Criminal Penalties* aspect because it is related permits from *Regulations and Acquirer*. According to everyone API credit card fraud of more than $ 11 billion per year, the percentage of lost income for fraud increased from 0.51% in 2013 and 0.68% in 2014, the biggest loss occurred on non-card transactions present of web, telephone, or mail order transactions (everyoneapi.com). in this case the company guarantees transaction failure of only 1% per month to the customer. The second one that has priority is a fine and legal sanction because if the permit from the regulator and acquirer is automatically revoked Company will not be able to sell payment gateways products.

4.2 Profile Development Information Assets

In this step, we determinated of the critical information asset. Assets information that selected is related to information in *Credit Card Payment Gateway System* owned by company to achieve the vision and mission of the company.

After gathered all asset informations, we discussion with *Manager Front End 1, Manager Back End 2,* and *Senior Programmer* in group discussion. The result group discussion can be determine critical information assets in company. Result group discussion there are 9 critical assets information in *Credit Card Payment Gateways System*.

Determination of any information assets that are critical for the company refers to risk measurement criteria that can cause a large impact if the following things occur (Software Engineering Institute, 2007):

- The information assets are accessed by people who do not have permission.
- The information assets are modified by people who do not have authority.
- The information assets are lost or damaged.
- Access to information assets is damaged or disturbed.

The company already has information about their critical information assets. This information is in the "Risk Assessment Analyst Table" document. Information assets that are determined as critical information assets will be recorded on the critical information asset worksheet provided by OCTAVE Allegro. The following is a list of critical information assets owned by the company related to the operation of credit card payment gateway transactions:

- Information Card Holder Data & Customer Credential
- Data Center Information
- Physical Devices Information (Servers, Network, Storage, Crypto Engine, etc)
- Logical Storage Information
- Logical Network Information
- Supporting Software Information (OS, Platform, etc)
- Core Application Information
- Encryption Key Information
- Human Resources Information

After all critical information assets on the system are obtained, the next step is to complete the information assets profiling worksheet provided by OCTAVE Allegro. Filling is done by group discussion with Front End 1 Manager, Back End 2 Manager, and Senior Programmer to discuss and fill out information asset profiling worksheet based on 9 information assets above.

4.3 Identification of Information Asset Containers

At this stage, identification of information asset containers is carried out using information asset risk environment map worksheet. There are 3 categories of container information assets located, namely:

a. Technical (Technical) Hardware, software, or systems that are under company control (internal) or that are outside the control of the company (external).

b. Physical (Physical) Physical location or document that is under the control of the company (internal), or that is outside the control of the company (external).

c. People Anyone who knows information that is under the control of the company (internal), or who is outside the control of the company (external).

4.4 Identification Area of Concern

In this step, we doing group discussion with *Manager Front End 1, Manager Back End 2,* and *Senior Programmer*. Group discussion results can be determined *Area of Concern* for 9 critical assets informastion. *Areas of Concern* will be documented with reference to *The Information Asset Risk Worksheet OCTAVE Allegro*. The results of group discussion can be seen in Table VII.

Table-VII: Area of concern for information Assets

Information Assets	No	*Area of Concern*
Card Holder Data & Customer Credential	1	*Stealing Credit Card Data*
	2	*Stealing Username* and *Password Customer*
Data Center	1	*Data Center Facility not Available*
	2	*Stealing Access Data Center*
Physical Devices	1	*Device Component Failure*
	2	*Unauthorized Physical Access to Devices*
	3	*Unauthorized Remote Access*
	4	*Stealing HSM Physical Key & Card*
Logical Storage	1	*Unauthorized Access to Logical Unit Number*
Logical Network	1	*Network Attack*
	2	*Unauthorized Access*
Supporting Software	1	*Unauthorized Access OS*
	2	*Unauthorized Access Platform*
	3	*Unauthorized Access Primary Database*
	4	*Unauthorized Access Database Backup*
Core Application	1	*Unauthorized Access to Application*
	2	*Hacking*
	3	*Unauthorized Access to Source Code*
Encryption Key	1	*Unauthorized Access to Key Storage*
Human Resources	1	*Unweel Condition Programmer*
	2	*Unweel Condition Operation Officer*

4.5. Identification of Threat Scenarios

At this stage, the area of attention is expanded into a threat scenario that details further the characteristics of the threat. Activities that must be carried out at this stage are as follows:

a. Complete information asset risk worksheet for each identified threat scenario.

b. Determine the probability in the description of the threat scenario that has been made in the information asset risk worksheet.

At this stage there is a group discussion at company with Manager Front End 1, Manager Back End 2, and Senior Programmer. The discussion was conducted to determine the threat scenario and probability of the threat scenario.

The probability level refers to the OCTAVE Allegro framework, namely there are 3 levels of probability of low, medium, and high. In addition, the results obtained are threat scenarios for each area of concern to each critical information asset.

4.6. Risk Identification

At this stage a group discussion was held in the company with Front End 1 Manager, Back End 2 Manager, and Senior Programmer to get the risk of each area of concern to each critical information asset. This stage aims to determine how threat scenarios that have been recorded in each information asset risk worksheet can have an impact on the company.

Risk is derived from a combination of threats and consequences that result.

4.7. Risk Analysis

In this step, we doing calculation of *Relative Risk Score* to analyze the risks and help company determined strategy decisions to face the risks. Step risk identification and risk analysis has a close relationship, in every area of concern on any information asset that has been defined. The risk having consequences that will give impact on the impact area, the impact on the impact area will be given an impact value accordance the criteria assess of risk measurement. Each value of the impact have the weight as seen in Table VIII.

Table -VIII: Calculating impact area score

Impact Areas	Priority	*Low (1)*	*Medium (2)*	*High (3)*
Financial	5	5	10	15
Fines and Criminal Penalties	4	4	8	12
Reputation and Customer Trust	3	3	6	9
Productivity	2	2	4	6
Safety and Health	1	1	2	3

The risk analysis process to obtain the relative value of risk is carried out through a group discussion to determine the impact value for each risk based on the consequences produced.

Table – IX: Risk analysis at *card holder data & customer credential* (i)

Information Asset		*Card Holder Data & Customer Credential*			
No	*Area of Concern*	Consequences	*Severity*		
			Impact Areas	Nilai	*Skor*
1	Credit Card Data Theft	- Customer credit card data can be disseminated by irresponsible parties - Loss of company reputation due to loss of important data - Losses obtained by customers who are victims of data theft	Financial	*High*	15
			Fines and Legal Sanctions	*Medium*	8
			Customer Reputation and Trust	*High*	9
			Produktivity	*Medium*	4
			Safety and Health	*Low*	1
			Nilai Relatif Risiko		37

4.8. Selection of Control Mitigation & Recommendation Approaches

The mitigation approach is a way for an organization to overcome risks. OCTAVE Allegro provides 4 options for dealing with risk, namely [16] :

a. Accept; A decision made during a risk analysis not to take action to overcome a risk and accept the consequences that have been stated. Risks received must have a low impact on the organization.

b. Mitigate (Mitigation / Reducing) ; A decision made during a risk analysis to overcome risks by developing and implementing controls to counter threats or minimize the resulting impact, or both. Reduced risk is a risk that usually has a medium to high impact on the organization.

c. Defer (Suspending); A situation where risks are not received or mitigated based on the organization's desire to gather additional information and carry out additional analysis. Deferred risks need to be monitored and re-evaluated. Suspended risks are generally not a threat to the organization or do not significantly impact the organization if it occurs.

d. Transfer (Divert); A decision made during a risk analysis to overcome the risk by transferring the risk to a third party.

At this stage sequencing is carried out for each risk that has been identified based on the relative value of the risk, ranging from the highest to the lowest. After that, grouping each risk is based on the relative value of the risk and the probability of the occurrence of the risk. Risk grouping can help in decision making on mitigation approaches for these risks. The mitigation approach for each risk group provided by OCTAVE Allegro can be seen in Table X.

Table – X: Mitigation approach

Pool	*Mitigation Approach*
Pool 1	Mitigation
Pool 2	Mitigation atau *Defer*
Pool 3	*Defer* or Accepted
Pool 4	Accepted

Source : [16]

The next step grouping risk and mitigation approach shaped in the form of relative risk matrix in the form of relative risk matrix based on the relative and probabilities. To be able to apply relative risk matrix, *OCTAVE Allegro* already own a framework itself. So we just put some of the previous points into the table relative matrix. Seen below the Table XI Relative Risk Matrix.

Tabel -XI: Relative risk matrix

Probabilities	*Relative Risk Matrix*		
	30 To 45	16 To 29	0 To 15
High	*Pool 1*	*Pool 2*	*Pool 2*
Medium	*Pool 2*	*Pool 2*	*Pool 3*
Low	*Pool 3*	*Pool 3*	*Pool 4*

Source : [16]

From the results of grouping for each risk in the operational activities of credit card payment gateways in the company, 21 risks were identified, 15 risks were deferred, 3 (three) risks to be received, and 3 risks that need to be mitigated. And in the table added recommendations for control of the Area of Concern by implementing clauses in ISO 27001: 2013 and PCI DSS v3.1.

Table -XII: Pendekatan mitigasi pada *card holder data & customer credential*

Aset Information		*Card Holder Data & Customer Credential*		
No	***Area of Concern***	**Mitigati on Risk**	**Container**	Control Recommendations
1	Credit Card Data Theft	*Defer*	*Eksternal*	ISO 27001 : **(A.10.1.1)**Policy on the Use of Cryptographic Control PCI DSS: (**Requirement 3**) Protect card holder's stored data **(Requirement 4)** Encrypt the card holder's data contained in the network (**Requirement 7**) Limit access to cardholder data **(Requirement 9**) Limiting physical access to cardholder data
2	Customer Username and Password Theft	Mitigati on	*Eksternal*	ISO 27001 : (A.9.2.5) Checking User Access Rights (A.9.4.1) Information Access Restrictions (A.10.1.1) Policy on the Use of Cryptographic Control PCI DSS: **(Requirement 7**) Limit access to cardholder data (**Requirement 9**) Limiting physical access to data cardholder

4.9. Risk of the highest score

Of the 21 risks that have the highest score are Unauthorized Access to Source Code and Hacking on Core Application critical assets with a value of '44' so that there is need for activities other than control recommendations according to ISO 27001 and PCI DSS clauses, the control recommendations are:

- Unauthorized Access to Source Code
  - Protect the source code from unauthorized changes using the system repository.
  - Provides backup of source code in the offline repository
  - Perform functional tests before live production.
- Hacking
  - Perform assessment and review vulnerabilities for each system component periodically (if there is an update of the source code).
  - Perform periodic applications.
  - Provides regular data backup every day to minimize data loss.

V. CONCLUSION

Based on the results of discussions, studies, and analysis of operational risk management Credit Card Payment Gateways in company, we concluded that :

- There are 9 critical asset information in Credit Card Payment Gateways System at company : *(1) Card Holder Data & Customer Credential; (2) Data Center; (3) Physical Devices; (4) Logical Storage; (5) Logical Network; (6) Supporting Software; (7) Core Aplication; (8) Encryption Key; (9) Human Resources*.
- From 9 information assets that has been identified, 21 risks that may occur during credit card payment gateways. Risk that have the highest score and almost chalky happened is unauthorized access to source code and hacking for transaction Credit Card Payment Gateway.

From 21 risks that were identified, obtained 13 risks are defer, 3 risks to be acceptable, 3 risk should be mitigate and 2 risks transferred to third party *(outsource)*

REFERENCES

1. Bank Indonesia, "Peraturan Bank Indonesia No. 14/2/PBI/2012 Penyelenggaraan Kegiatan APMK", Bank Indonesia, 2012.
2. Caralli, Richard A, et al. "*Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process*" U.S : Carnegie Mellon University. 2007.
3. Christopher Alberts, A. D. "Managing Information Security Risks : The OCTAVE Approach*,"* Addison Wesley, 2002.
4. Conner, B., Noonan, T., & Holleyman II, R., "Information Security Governance : Toward a Framework for Action," (Business Software Alliance). 2004.
5. Đurić, Z., Marić, O., and Gašević, D. "Internet Payment System: A New Payment System for Internet Transactions," Journal of Universal Computer Science, vol. 13, no. 4, 2007, pp 479-503.
6. Filipe N. R Macedo, "Models for Assessing Information Security Risk. Instituto Superior Tecnico", 2009.
7. Gary Stoneburner, A. G., "Risk Management Guide for Information Technology Systems*,"* Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, 2002.
8. Gulati, V. P., and Srivastava, S., "The Empowered Internet Payment Gateway," Tata Consultancy Services Limited, 1, 2007, pp 98-107.
9. Haar Van de, H., & von Solms, R., "Deriving Information Security Control Profiles for an Organization. Computers & Security," 22 (3), April 2003, pp. 233 – 244.
10. ISO & EIC, *"ISO/IEC 27001:*2013 Information Security Management Systems Requirements", ISO & EIC, 2016.
11. Kiran, K. V. D., et al, "Performance And Analysis Of Risk Assessment Methodologies In Information System", International Journal of Computer Trends and Technology Vol. 4 Issue 10, 2013.
12. Kouns Jake, D. M., "Information Technology Risk Management In Enterprise Environments," New Jersey : John Wiley & Sons, 2010.
13. PCI Security Standards Council, "PCI-DSS Requirements and Security Assessment Procedures", PCI Security Standards Council II, 2016.
14. Saint-Germain, R., "Information security management best practice based on ISO/IEC 17799" The Information Management Journal. Vol. August 2005, pp. 60-66.
15. Schwartz, M. "Computer Security : Planning to Protect Corporate Assets*,"* Journal of Business Strategy. Vol. 11(1), 1990, pp. 38-41.
16. Software Engineering Institute, "Introducing OCTAVE Allegro : Improving The Information Security Risk Assessment Process*,*" Hanscom AFB: Cameige Mellon University, 2007.
17. Whitman Michael E. and Mattord Herbert J. "Management of Information Security,"3rd Edition. Thomson-Course Technology, 2010.
18. Woody, C."Applying OCTAVE: Practitioners Report" Hanscom AFB:Technical Note CMU/SEI-2006-TN-010 Carneige Mellon University. May 2006.
19. Higuera, R. P., & Haimes, Y. Y. "*Software Risk Management"* Pittsburgh : Software Engineering Institute, 1996.

AUTHORS PROFILE

Nilo Legowo, Associate Professor in Computer Science at Bina Nusantara University completed his undergraduate education at Surabaya State University in Education in 1989 and continued his Masters degree in Informatics Engineering at the STTIBI graduated in 1997, and at In 2014, he entered the Doctoral Program in Management Research at Binus University graduated 2018. Being a lecturer since 1997 began teaching in various Private Universities in Jakarta in the fields of Computer Science and Information Systems.

Since 2009, he has joined faculty member at the Computer Science Department of Bina Nusantara University as a Subject Content Coordinator (SCC) in the field of Software Engineering. Since 2011 he has been assigned as Deputy Head of Department to manage the Postgraduate Program in Information Systems Management.

Kemas Airlangga Saputra, born in 1986, have passion in IT especially Online Payment System. Completed his undergraduate education at Binus University's Information Technology Faculty of Computer Science in 2008, and completed his education at Binus University Information Systems Management Postgraduate Program in 2017.Currently works in Payment Gateway Service Provider Company as a Lead IT Security Application. Has 7 years experience as a Programmer with various language (C, Delphi, C++, PHP, J2ME, etc) since 2009, 2 years experience in IT Fraud as a Fraud Analyst, and 1 year experience in IT Security as Vulnerability Tester.