International Journal of Psychosocial Rehabilitation, Vol. 24, Issue 7, 2020
ISSN: 1475-7192

Risk Mitigation Plan in API Integration Using NIST SP 800 - 37

[1]Rangga Octavian Pratama[1], Prawita Oktovini Sihotang[2], Widia Rismadewi[3], Asep Rifki Pauji[4], Falahah[5]

Abstract – *Integrating the backend system or external system in recent business system is a must. Complexity in operational system makes company or organization should have a good plan in integration. The best and easy way in integration is using application programming interface (API) that can help us integrating the system without doing lots of modification. But, integrating the API or the system using API can lead into some risky situation, such as data format problem, security, or non-standard API development issue. The risk issue need to encounter by preparing proper mitigation plan. It can be done by implementing framework for risk management or assessment such as explained on NIST SP 800-37 documents. On this research, we implement the risk assessment on integration problem at PT.X, which provide online services and needs to process data from customer, sales, and financial information. The data analysis from risk assessment shows that there are three top risks need to resolve which are accountability, hesitating over API utilization, and lack of Security. Based on this result, we also propose some mitigation plan to reduce the impact, such as establish roles and responsibility for API development and maintenance, socialized and promote API utilization, and increase the security capability.*

[2]***Keywords:*** *Risk, NIST 800-37, intergation, API, mitigation*

I. INTRODUCTION

Risk management is a necessary fundamental need. In risk management is a complex activity and involves all components of an organization. This is due to the global era, the business is faced with an environment with very high uncertainty and complexity. Based on a survey conducted by one of the auditor company KPMG against 1500 members of the Audit committee in 34 countries, it was found that 43 percent of correspondents acknowledged how difficult it is to monitor the major risks faced by Company. One of the main risks in question is the risk of information technology (IT) and cyber risk.

PT X is a company that assists online entrepreneurs in handling its business in terms of over-sales, stock arrangement to complete accounting needs. This company can also help integrate with various online shop so it is very helpful in running the business online or offline. In running its business, PT X prioritizes to entrepreneurs who focus on online business so that with the interaction between PT X and online businesses does not need to calculate the accounting records and reporting as already Automatically made with the same sales occurrence.

Engaged in accounting information system software involving customer data, sales data, and customer financial report data requires that the company has a strong security and integrated IT system. Business processes running at PT X pose critical risks that can cause barriers to the company. Risk management of IT systems. In this case, in integrating another

[2] Information System Department, Widyatama University, Bandung, Indonesia
pratama.octavian@widyatama.ac.id[1], prawita.oktovini@widyatama.ac.id[2], widia.rismadewi@widyatama.ac.id[3], rifki.pauji@widyatama.ac.id[4], falahah@widyatama.ac.id[5]

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

platform with PT X using the API (Application Programing Interface) in other words the possible risk of data provided by other platforms can interfere with the integration System associated with PT X. This is a problem for PT X in maintaining the data quality and the security of the systems created.

The NIST SP 800-37 standard is used as a reference in conducting the management of an information security risk, which aims to anticipate the risk of making losses not happening to the organization. Risks can be identified, assessed and reduced risk impact to an acceptable level of the organization. NIST SP 800-37 was chosen as a reference for risk management in the use of systems and information technology at PT X.

II. LITERATURE REVIEW

A. Risk Management

Risk is the possibility of unintended consequences that can cause losses, such as loss, disaster, and injury (Darmawi, 2014). According to (Pinontoan, 2010) risk is the negative impact or result of decisions taken in life.According to Gondodiyoto (2007), risk is an opportunity, the negative impact of implementing vulnerability, considering the probability and impact of risk. Companies can minimize risk by anticipating control, but not completely avoiding exposure, even with a maximum control structure.

According to Idroes (2008), risk is a hazard, threat or possible action that has an opposite effect to the goal to be achieved. In the risk there is no method that can guarantee the adverse effects can be avoided, but the risk can be minimized so that the consequences of the risk does not cause large losses. From various definitions of risk it can be concluded that risk is a threat from actions that arise from deviations that cause harm.

Risk management according to Kasidi (2014) is an effort aimed at reducing the possibility of losses caused by the risks faced. Risk management is the process of identifying, managing risks, and forming strategies to be managed through existing resources. The strategy used is to transfer risk with other parties, avoid risk, reduce the adverse effects of risk, and accept all consequences of the risk. Risk management enables IT managers to balance operational and economic costs of protection measures and achieve benefits in mission capabilities by protecting IT systems and data that can support the organization's mission. It can be concluded that risk management is an effort made to reduce or eliminate the risks faced (Stoneburner, Goguen, & Feringa, 2002).

B. NIST 800 - 37

NIST SP 800-30 is a standard document developed by the National Institute of Standards and Technology of special publications containing the continuation of legal responsibility under the Computer Security Act of 1987 and the law Information Technology management reform year 1996. NIST SP 800-30 There are three stages of the process namely risk assessment, risk mitigation and risk evaluation.

According to (Wolingpirayat, 2007) NIST issued a recommendation through a special 800-30 publication on the Risk Management Guide for Information System / Technology. There are three processes in risk management issued by NIST SP 800-30, namely the risk assessment, risk mitigation and risk evaluation. ·

Risk Assessment

Risk assessment is the first step in the risk management methodology issued by NIST to define potential threats and risks associated with the use of information technology. There are 9 (nine) steps to fulfill, namely:

1. System Characterization
2. Threat Identification
3. Vulnerability Identification
4. Control Analysis

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

5. Likelihood Determination
6. Impact Analysis
7. Risk Determination
8. Control Recommendations
9. Results Documentation

All of the above steps are taken to see the characteristics and threats as well as the impact that will occur. The risk determination itself is divided into 3 levels, High, medium and low. Still each level has its own score, for the probability that it has a level of 1.0 for the high scoring limit is 0.5 and a low of 0.1. While the value for impact is 100 where the high value is 50 and the low value is 10.

Risk Mitigation

Risk Mitigation is the second stage of the NIST risk management process by prioritizing, evaluating and implementing recommendations from risk reduction controls from the risk assessment stage. Activities in the mitigation phase are:

1. Prioritize Action
2. Evaluate Recommended Control
3. Conduct Cost Benefit Analysis
4. Select Control
5. Assign Responsibility
6. Develop Safeguard Implementation Plan
7. Implement Selected Control

Risk Evaluation

Risk evaluation activity is the last stage of the activity after the risk mitigation process, in general the network implemented in the organization will experience changes or development of hardware components, software development and applications by versions that are more up to date and newer.

C. Rest API

API (Application Programming Interface) is a small module that has certain function. API is a software module that can be accessed by people who need it in a way that has been determined by the service. The API consists of various elements such as functions, protocols, and other tools that allow developers to create applications. Focused representation of functions declared in the API to provide specific services. If in one module has multiple APIs, this has become common because each API is intended for specific uses of the related module (Rama and Avinash, 2015). The purpose of using the API is to speed up the development process by providing functions separately so that developers do not need to create similar features. APIs that work at the operating system level help applications communicate with the base layer and with each other following a series of protocols and specifications.

Web API program interface from the system that can be used via methods and headers on standard HTTP protocol. Web APIs can be accessed from various HTTP clients such as browsers and mobile devices. Web API also has the advantage of using infrastructure that is also used by the web, especially for the use of caching and concurrency (Miller et al, 2014).

D. Web Service

According to Michael, S. I. and Purba, J., (2007), Web services are computing that can be accessed through Internet and intranet networks with certain protocol standards in the platform and an independent programming language interface.

Web services objectives are used as a facility that provides services (in the form of information or data) or as a communication bridge between programs, so that it can connect applications contained on the same network as the application on different networks. WEB services are built on the well-known protocols that also have several independent platforms, such as HTTP, XML, UDDI, and WSDL. One type of Web service is REST.

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

III. METHODOLOGY

The methodology on conducting this research consists of 5 phases that we adopt from NIST SP 800-37, which are: Identify Risk Register, Risk analysis, risk priorities, Risk mitigation and Risk Plan.

A. Risk Register

Risk Register or risk list can be examined by the project manager as a management tool to assess the risk management process in the project. The risk Register is used to identify, assess and manage risk to the review process. The goal risk Register or list of risks records the details of all the risks that have been shared with their analysis and plans for how the risks will be treated.

It is the responsibility of the project manager to ensure that the risk register is updated every time it is used. Using or updating a risk list is usually delegated to the project control function. This is the risk that has been managed, avoided or no longer relevant to be removed from the risk register. Plans to face such risks can also be removed from the risk register.

Risk Register will be distributed to the stakeholders or parties who have a direct relationship with this project in order to continue to be monitored what possible risks will occur and find the right solution.

Risk Register is already the responsibility of the Project Manager. From existing risk updates, to anything that needs to be done to reduce the risk. Risk has been resolved solution, can be eliminated from the risk register. On this research we use the risk register that identified by axway and concepta, that is specific for API integration and API security, as follow:

1. Bad coding
2. Inadequate validation
3. Hesitating over API utilization
4. Accountability
5. Risk of xml
6. API incompetence
7. Lack of security
8. Going overboard with control
9. Term of services
10. Unsatisfactory security
11. API Evolution
12. Developer responsibility
13. There are no restrictions for end-users
14. Inadequate coding
15. Certificate validation issues

B. Risk Analysis

Risk analysis is the step to determine the level of risk. It can be done by identifying and analyzing potential problems that could negatively impact the organization in order to avoid or mitigate such risks.

We can use risk mapping to determine the risk level by separating low risk to a high risk then provide evaluation data at once with risk correction.

Risk analysis considers the source of risk, the consequences and possibilities of the consequences that may be missed in the future, a factor that affects possibilities and consequences as may be identified. Risks can also be analyzed by combining the approximate consequences and possibilities of existing control contexts.

C. Risk Priority

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

The next step in determining the problem that must be resolved, namely to find the risk priority where this step is enabled to find the priorities that will be done first in creating a risk plan. Risk priority aims to sort out which problems can be solved in advance and which risk level should be prioritized in the integration of API. This benefit at risk priority is in solving problems we know which to do first and important problems will be more quickly resolved.

D. Risk Mitigations

Risk Mitigation is a planned and ongoing process that is used to control, evaluate, and prevent the risks that occur. Risk Mitigation is done to minimize the risk level so that it is not affected by the resources and running business processes, so the risk is not happening again. In taking a decision, reduce the risk by using the relevant data.

Risk Mitigation is used for the preparation of mitigation plans. Companies need to get information on the risks that will be encountered, in the process of risk mitigation, the company devise a series of plans to minimize exposure to risk.

E. Risk Plan

Risk plan is a document that aims to make an estimate of the impact of risk that has occurred so if the risk arises and there is no way out then the road will be taken the risk plan. With the risk plan, all existing problems have been made of repair documents as well as the exit so that will be used as consideration in taking the next step.

IV. FINDING AND DISCUSSION

A. System and Risk Overview

The system we choose as an object for this research is a system for facilitating online commerce. The system will connecting three subsystem as the backend, which are: marketplace, inventory and distribution system. Integration on this system requires 5 API that will be connecting three system as described in table I.

Table 1. API Support for Integration

API-code	**Description**	**System Connected**		
		Market place	**Inventory**	**Distribution**
API-01	Check order	√	√	
API-02	Confirm order delivery		√	√
API-03	Confirm payment	√		√
API-04	Update stock	√	√	
API-05	Confirm shipping		√	√

Figure 1 and 2 below show the API that ready to implement. The others still on development process.

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

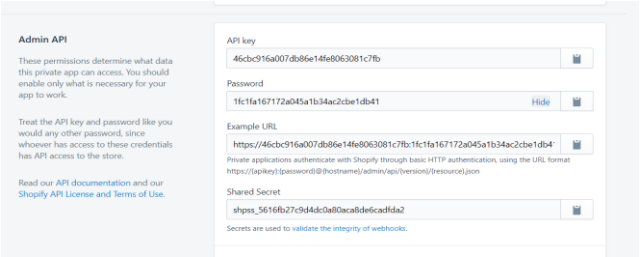

Figure 1 Shopify Code API

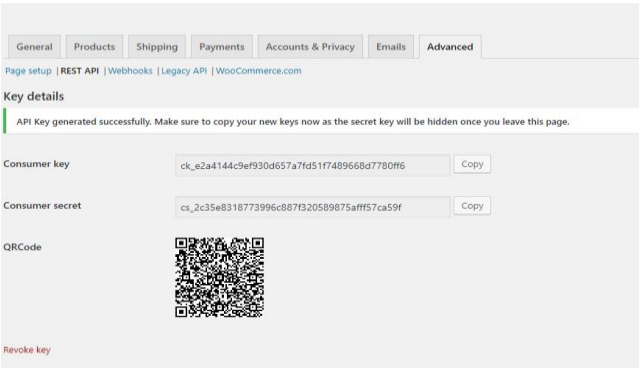

Figure 2 WoCommerce Code API

We also need to map the risk register into affected API. It will help us to prioritize the existing risk and preparing specific course action in certain API. List of affected API is shown in table II.

There is some problem for existing API operational such as:

1. A system disconnect occurred
2. Difficulty completing orders, because the system is unstable
3. Changes to API specifications in a short amount of time, without confirmation
4. The difference that makes the system and user API
5. Trouble for monitoring API activities

Table II. Impact of Risk on API

Risk Register	**Affected API**				
	1	2	3	4	5
Accountability	√	√	√	√	√
Hesitating over API utilization			√		√
Lack of security	√		√		√
Developer responsibility	√	√	√	√	√
Bad coding	√			√	√
Inadequate validation	√	√	√	√	√
Risk of XML			√	√	√
API incompetence	√		√		√

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

Going overboard with control			√	√	√
Term of services		√		√	√
Unsatisfactory security		√		√	
API Evolution	√	√	√	√	√
There are no restrictions for end-users		√	√		√
Inadequate coding	√	√		√	
Certificate validation issues	√		√		

B. Risk Analysis

In this research, we assess the risk of the system and analysis the result. the system that has been running in the integration using the API. We will use the combination between impact and probability and multiply the number to identify the score for each risk register. Probability represent the tendency that risk condition would be exist. Impact show the impact of the risk if it happens. Probability and Impact is expressed using percentage to show that more bigger the value, more higher the probability or impact of the event. After calculate the score, we can also adjust the level of the risk as high, medium and low. On this research we choose the limit of high is above 0.7, medium between 0.7-0.5 and low when the score is below 0.5. Table III show the result.

B. Result and Discussion

As we can see from table III, we can identify 3 highest score for risk, which are:

1. Accountability, score: 0.84
2. Hesitating over API utilization, score: 0.68
3. Lack of Security, score: 0.6

Accountability is the condition when we have to define the stakeholder who has accountability for keeping the API running well. The impact of accountability failure can be critical because without clear accountability, it is hard for organization to fix the problem on API system. The next score is hesitating over API utilization, show that in an organization, sometimes its happen that some business function or unit refuse API utilization. The lack of security on the API would affect the system significantly because it can lead of data or information leak.

Table III. Probability and Impact Analysis

Risk	Probability	Impact	Score	Level
Accountability	90%	90%	0,81	High
Hesitating over api utilization	80%	85%	0,68	Medium
Lack of security	80%	75%	0,6	Medium
Developer responsibility	80%	75%	0,6	Medium
Bad coding	50%	90%	0,45	Low
Inadequate validation	30%	50%	0,15	Low

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

Risk of xml	60%	70%	0,42	Low
API incompetence	50%	50%	0,25	Low
Going overboard with control	20%	30%	0,06	Low
Term of services	90%	30%	0,27	Low
Unsatisfactory security	70%	70%	0,42	Low
API Evolution	40%	60%	0,24	Low
There are no restrictions for end-users	10%	30%	0,03	Low
Inadequate coding	30%	30%	0,09	Low
Certificate validation issues	10%	10%	0,01	Low

In order to mitigate the risk above, we propose some approach as bellow:

1. The company must compile a series of plans on the handling and accountability related API implemented. Increase in accountability rules.
2. The company requires the socialization related to the use of API.
3. Increased security in the API as a risk control on the lack of security in the company.

From research that has been discovered and conducted, problems that have become a big constraint in integration using the API is that includes business processes already done. The API plays an important role for companies who want to connect with other parties and want to contribute to the marketplace. The integration used here uses the basic complex programming so that there are many shortcomings in a website.

In this case, this research has a distinction with other research. In this research, it is more important to risk the worst possible on a website that want to use the integration phase using API Code. It is certainly very risky when in relation to sales as well as distribution of sales of products carried out between markeplace. With the API can facilitate an expansi merketplace.

V. CONCLUSION

Based on the research identification that has been conducted and analysed in the previous chapter, here are some of the inferred:

1) Based on Risk Assesment that has been implemented, we can be identified that the risk that is the biggest obstacle in building an integration in the marketplace is Acoountabilty, Hesitating over API Utilization, and Lack of Security.

2) Risk scores show that greatest risk level is the value of 0.81, 0.68 and 0.60 according to the calculation of the risk register above.

3) with the Risk Plan, the risk can be handled with some documents that have been created and can be handled according to the analysts using NIST 800-37.

After dealing with this research, in addressing the system API should pay attention to some technical in the creation of programs and things to be considered in the integration so that with the risk register the risk of failure to connect Or even the error will not occur.

REFERENCES

[1] Darmawi, H., 2014. *Manajemen Risiko.* Jakarta: Bumi Aksara.

[2] Gondodiyoto, Sanyoto. (2007). Audit Sistem Informasi Pendekatan COBIT.

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019

[3] Idroes, F. N. (2008). Manajemen Risiko Perbankan: Pemahaman Pendektan 3

[4] Internet Banking And Commerce

[5] Jakarta: Penerbit Mitra Wacana.

[6] Kasidi, 2014. *Manajemen Risiko.* Bogor: Ghalia IndonesiaMedia. Pilar Kesepakatan Bassel II Terkait Aplikasi Regulasi dan Pelaksanaannya di Indonesia. Jakarta: Rajawali Pers

[7] Pinontoan, J. H. (2010). Manajemen Risiko TI Konsep-konsep. Majalah PC

[8] Stoneburner, G., Goguen, A. & Feringa, A., 2002. *Risk Management Guide for Information Technology Systems Recommendation of the National Institute of Standards and Technology Special Publication 800-30*.

[9] Wolingpirayat, J.2007. *E-payment Strategies of Bank Card Innovation*. Journal of Internet Banking And Commerce

[10] Yu, D., Ebadi, A.G., Jermsittiparsert, K., Jabarullah, N., Vasiljeva, M.V., & Nojavan, S. (2019) Risk-constrained Stochastic Optimization of a Concentrating Solar Power Plant, *IEEE Transactions on Sustainable Energy*, https://doi.org/ 10.1109/TSTE.2019.2927735.

[11] Michael, S.; Purba, J., 2007, Membongkar Teknologi Pemrograman *Web service*, Gava Media, Yogyakarta

Received: 10 Nov 2018 | Revised: 20 Dec 2018 | Accepted: 02 Jan 2019