Risk Analysis in the Application of Financcore Information Systems Using FMEA Method

Y S Triana 1, R A M Pangabean 2

1,2Information System, Faculty of Computer Science, Universitas Mercu Buana, Jl. Meruya Selatan no 1, Jakarta, Indonesia

email: yaya.sudarya@mercubuana.ac.id1, 41815120166@student.mercubuana.ac.id2

Abstract. In the banking world maintaining customer data is very important so as not to experience various risks, including leakage of customer data. Leakage of customer data is one of the big risks that may occur in the banking world, whereas customer confidentiality should be guaranteed. Possible risks such as misuse of identity or theft of transaction data by unauthorized parties. This will certainly harm both the customer and the bank. So that customer data is not leaked, lost or misused, it is necessary to have a regulation or verification system of customer data that can be reviewed for security and use. The solution that can be done to prevent this event is to use the FMEA methods that can be used to reduce errors and system failures. Information system security has a positive and very significant effect on decision making, therefore it is necessary to have an information system risk analysis that supports it comprehensively so that it can help in decision making.

Keywords: Data Leakage, FMEA, Security of IS.

1. Introduction
As a multi finance company, PT. XYZ Finance provides a variety of applications to support smooth operations while meeting the needs of consumers and corporate partners. On the other hand, system security and the company's data base are also important issues of concern to the company. From the system side, the company implemented an antivirus application to safeguard data security from tampering / virus applications and implemented a hardening policy for each personal computer (PC) and server. At present, the company has implemented a Mobile Device Management system to maintain the security of a centrally controlled system. The company also implements backup systems on a daily, weekly and monthly basis, to maintain the security of historical data on the loan system from disasters, both natural disasters and disruption of system damage [1].

But it was not enough there, PT. XYZ Finance also realizes that financial institutions are a trust-based business. In digital networks like today, data is usually sent by copying it from one place to another, the problem is how to verify that the data and information received from the network are original and up to date [2]. Data and information also need to be well guarded by the company so as not to cause
data leakage in the future. Data leakage that occurred in a finance company is a major disaster that can affect all operational aspects. However, on the one hand, data security is not only the responsibility of the company, but also the customer / consumer. For this reason, every community, especially customers, must be more careful and aware of the value of their personal data by not spreading data to other parties.

Customer losses arising from corporate system errors, the company will replace all losses suffered by customers. Beyond the company's commitment to bear all losses suffered by customers in the event of undesirable things, on the one hand the company also takes preventive measures to tighten the security system. This is done because the company realizes that there is a great trust that customers entrust to them and also as a company business in preventing the emergence of greater risk.

Financore is a financing application that displays data and information related to consumer credit at PT. XYZ Finance which is useful in supporting the vehicle loan financing process, both when applying for credit, installment periods to closing installments. Financore is one of the many applications provided by PT. XYZ Finance in meeting company needs for corporate business processes.

During the use and implementation of the information system, it is possible to create various risks that can threaten the sustainability of business processes. Management of the possibility of the emergence of various risks is something that needs to be considered [3]. There are several ways that can be taken to prevent this, and PT. XYZ Finance has implemented the company's operational standards in terms of implementing information systems prevention. However, these methods require active collaboration on the part of the company using appropriate and appropriate methods. Based on the problem above, we need a method that can help in measuring the level of security and evaluation of information system security, in addition to reducing the occurrence of errors and system failures.

In this study, a problem formulation was raised regarding the steps in analyzing the risk management and security of information systems in the finance company. The method used in this study is to use the method of Operational Critical Threat, Asset and Failure Mode and Effect Analysis (FMEA). The purpose of using the FMEA method is to rank the chances of a system failure or the level of risk caused.

Previous research related to FMEA was carried out by Alvina Hendika Putri and Yupie Kusumawati in 2017 entitled "Critical Asset Risk Mitigation Strategy for Information Technology Using Octave and FMEA Methods" which raised the topic of problems related to hacker attacks that disrupted network systems. The results of the study are based on the number of risk assessment results that the highest risk is found at high RPN level [4]. Other related research was carried out by Melita Dyah Purwitasari et al in 2017 with the title "Analysis and Mitigation of IT Asset Risks Using FMEA Frameworks" which raised the topic of issues related to the risk of information technology assets at the Health Polytechnic of the Ministry of Health Semarang which gives a large impact to the organization which can disrupt the organization's work systems and operations against environmental aspects. The results of this study using the FMEA method of risk control measures to rank very high and high risk which have a standardized focus on the Information Security Management System (ISMS) so that risk can minimized or even eliminated [5].

To be able to minimize risks efficiently and effectively requires the involvement and supervision of all stakeholders in the preparation of policy implementation by applying a framework that is appropriate to the need to solve problems more quickly, such as the application of the Operational Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) and Failure Mode and Failure Mode and Failure Mode methods. Effect Analysis (FMEA).
in the digital era, technology and information systems have become very important things in an organization [6-7]. The advantage of this study is the lack of risk calculation research on data leakage and security carried out in the financial and banking sector which is very useful for the sustainability of the financial and banking business, especially in Indonesia. This study will produce information system security that is able to have a positive and significant influence on decision-making by management, for a supporting and comprehensive information system risk analysis.

2. Methods

2.1 Failure Mode Effect Analysis (FMEA) Method

FMEA (Failure Mode Effect Analysis) is a method used to evaluate the occurrence of a failure of a system, design, process or service to make the handling steps. To carry out the risk assessment process the FMEA (Failure Mode and Effect Analysis) method is used to produce an RPN (Risk Priority Number). RPN is obtained based on the multiplication of 3 risk assessment factor variables, including Severity (magnitude of failure impact), Occurrence (intensity of failure), and Detection (control ability) [3]. The following is a flowchart of the stages of the FMEA process.

The FMEA method is used to provide ranking or rate values that have been identified by the octave method. The FMEA method is used to rank the chances of a system failure or the level of risk caused.

In FMEA the RPN value is a calculation process that is used to determine the level of each risk. Obtained based on 3 factors that have been explained previously namely Severity, Occurrence and Detection. The RPN value can be shown using the following formula:

\[
RPN = S \times O \times D
\]  

\(O = \text{Occurrence}\) 
\(D = \text{Detection}\)

The RPN value for each failure ranges between 1 and 1000. Acceptance limits are set for the RPN score based on previous research. RPNs of more than 300 are considered unsafe [8]. After carrying out the calculation process, the next step is to determine the level of risk based on the value of the RPN. The scale will later be used for the risk assessment process to find out which risk is highest. That way the company will be able to determine the highest-value risk prevention measures. The RPN scale will be illustrated in the following table.

| RPN     | Level Risk  |
|---------|-------------|
| >=200   | Very High   |
| 120 – 199 | High       |
| 80 – 119 | Medium      |
| 20 – 79  | Low         |
| 0 – 19   | Very Low    |
Risk assessment needs to be done based on 3 factors, namely Severity, Occurrence, and Detection, in order to be able to rank priorities for the occurrence of a risk. Then it will be able to generate a Risk Priority Number.

1. Severity
Severity is the initial stage in analyzing a risk by ranking based on how big the impact of an event can affect the output process. The scale is given from 1 to 10, where the value of 10 is the worst value.

| Rank | Effect                      | Severity                                             |
|------|-----------------------------|-------------------------------------------------------|
| 10   | Dangerous without warning   | System failure will have dangerous effects without warning. |
| 9    | Dangerous with warning      | A system failure will have a dangerous effect with prior warning. |
| 8    | Very high                  | All support systems will not function.                |
| 7    | High                       | The system can operate but not optimally.             |
| 6    | Moderate                   | The system can operate but not optimally.             |
| 5    | Low                        | The system is operational and safe but has decreased performance. |
| 4    | Very low                   | The system experiences a gradual decline in performance. |
| 3    | Small                      | Little effect on system performance.                  |
| 2    | Very small                 | Negligible effect on system performance.              |
| 1    | There is no effect          | The effect of failure will not occur on the system.   |

2. Occurrence
Is a situation where the cause of the risk will occur and cause failure during the asset component is used.
The scale is given from 1 to 10.

| Rank | Effect                                      | Occurrence                                         |
|------|---------------------------------------------|-----------------------------------------------------|
| 10   | Very high: Failure is almost inevitable.    | The possibility of failure occurs once a day.       |
| 9    | Very high: Failure is almost inevitable.    | The possibility of failure occurs 5 times in         |
8. **Height:**
Failure occasionally occurs.

The possibility of failure occurs once a week

7

6

5

4

3

2

1

**Medium:**
Failures occur occasionally but not in large numbers.

The probability of failure occurs 2 times in 1 week

The probability of failure occurs 5 times in 1 month

The probability of failure occurs 3 times in 1 month

The probability of failure occurs 2 times in 1 month

**Low:**
Failures that occur are relatively small.

Very rarely:

Failures that occur are relatively small and rare.

Remote:

Failure never occurs.

The probability of failure occurs once a month

The probability of failure occurs once every 3 months

Remote:

Failure never occurs. Chances of failure occur once every 6 months

---

3. Detection

Is a measurement of the ability to control a failure that can later occur. Where the value of detection is adjusted to the control carried out by the company. The scale index of detection is 1-10.

| Rank | Effect                          | Detection                                                                 |
|------|---------------------------------|---------------------------------------------------------------------------|
| 10   | Almost impossible               | There is currently no control capability that can detect failure.          |
| 9    | Very rare                       | Current control capabilities are very difficult to detect the cause of failure |
| 8    | Rare                            | Current control capabilities are difficult to detect the cause of failure   |
| 7    | Very low                        | The current control capability to detect the cause of failure is very low   |
| 6    | Low                             | The current control ability to detect causes of failure is low.            |
| 5    | Moderate                        | Current control capability to detect causes of failure is moderate         |
| 4    | Somewhat high                   | Current control capability to detect causes of failure is moderate to high. |
| 3    | Height                          | Current control capability to detect causes of failure is high.            |
2 Very high. The current control capability to detect the cause of failure is very high.
1 Almost certain Current controllability can almost certainly detect causes and prevent failures

2.2 The purpose of FMEA
This study tries to further explore the use of the FMEA method in the field of information technology, especially information systems. The information system here is quite interesting to discuss because it is not physical, and its security can be very important. Information security can be defined as protection from unauthorized access in the form of use, destruction or alteration of data and information systems. Nowadays the role of information security has become more important because many people, businesses and government institutions have stored data in digital form using various types of technology [9].

There are several objectives that need to be achieved in FMEA (Failure Mode Effect Analysis) including:
1. Identify and predict failures that might occur.
2. Evaluate the impact of a failure that occurs on the system.
3. Give priority levels of risks that occur in order to facilitate the process of improvement based on the ranking process priorities.
4. Plan and take corrective actions to prevent and reduce the potential for system failure.
5. Documenting the entire process carried out.

Benefits of FMEA
There are benefits to be gained in applying the FMEA method in risk management in an organization, namely:
1. Reducing the occurrence of problems in the system.
2. Estimating actions that can reduce the occurrence of risk.
3. Save costs for system development.

2.3 Risks
Risk is something that leads to uncertainty over the occurrence of an event during a certain time interval where the event causes a loss whether it is a small loss or a large loss. This uncertainty can affect the achievement of the objectives of each organization or agency dealing with risk. Therefore, it is necessary to conduct a risk analysis to identify, measure, and then develop strategies as a basis for building a complete risk management system. In this context risk is always associated with negative consequences but facing or taking risks can also produce positive impacts. Another possibility of risk can lead to consequences that cannot be ascertained [10].

2.4 Risks Management
Risk management is a system of monitoring and protecting risks on assets, profits and finances of a business entity or from the occurrence of a loss due to the risk. Where is the risk management process that includes identification, evaluation and control of risks that can threaten the continuity of the company's business or activities? Risk management refers to the culture, processes and structures that are geared towards managing uncertainty. Risk management is a process of identifying, measuring risk, and forming a strategy to manage it through the available resources. Risk management aims to manage this risk so that it can obtain optimal results. The risk management process includes five activities, namely communication and consultation; define context; risk assessment; risk treatment; as well as monitoring and review. The risk management
process can be shown in the figure below [11]. In this case risk management will involve processes, methods and techniques that help IT managers maximize the probability and consequences of positive events and minimize the probability and consequences of opposite events.

2.5 Information System Risk Management

Information system risk management is the application of risk management in the context of information systems to manage IS risk. IS risk management can be considered as a component of a broader risk management system. Information Systems Risk Management is a process of identifying vulnerabilities and threats to information resources used by an organization and carried out by IT managers to achieve business goals, reduce risks, and balance expenses in achieving profits and protecting information. Therefore, it is necessary to evaluate the Information System risk management to determine the level of risk management capability that has been achieved, so as to increase the company's ability to manage every risk [12].

2.6 Information System Security

Information system security is an important thing that every company needs to pay attention to, information leaks and system failures can cause losses. Information security includes a mechanism to control access and use of databases at the object level, information security on users, where the user has a certain access. Given the importance of information in multi-finance companies, information must be protected or secured by all company personnel. All existing company information must have proper backup and recovery in place [13].

XYZ Finance realizes that in carrying out its business activities, the company is always faced with inherent risks in business activities and banking operations. In order to control these risks, the company implements an integrated risk management system that covers all aspects of risk faced by XYZ Finance. Basic Risk Management Policy aims to ensure the risks faced by the company can be identified, measured, controlled and reported properly. To support the implementation of effective risk management, the company continues to develop a risk management infrastructure by referring to applicable regulations and international best practices.

3. The Results

3.1 Information System Development

The business process of developing information systems is managing and exercising control for system security, both in terms of hardware, software, servers, networks and other support systems in the company to maintain its security, maintenance, maintenance and development so that business processes in the company goes well.

3.2 Analysis and Discussion

1. Organizational Perspective
   In an organization, there is a process carried out to find out about information, namely critical asset data, critical asset security needs, critical asset threats and applied security.

2. Data Components of Information System Critical Assets
   The information system asset component becomes an important thing for companies and government agencies to support business processes. The following is a list of critical system asset components owned by the company.

3. Data Identification of Critical Assets Component Information System
   Furthermore, an identification of information security needs is carried out on the critical asset components of the Information System owned by the company by including the CIA Triad (Confidentiality, Integrity, and Availability).

4. Risk Events Against Critical Asset Components of Information Systems
The following is an identification of risk events and causes that can occur in each critical asset component of the Information System.

5. Security That Has Been Implemented
   Based on the results of interviews with the company that it has taken several security measures to safeguard the critical assets component of SI owned by the agency from threats that will occur and can hinder the ongoing business process.

3.3 The following are security measures taken by the data management and information division of XYZ Finance:

1. CCTV installation
   The installation of CCTV security in the server room has been implemented by the organization so that activities and events that occur in the room will be controlled and recorded.

2. Data Backup
   The organization always backs up important data, be it server data or important data in the company to prevent the risk of data loss and data theft.

3. Using a Licensed OS
   The agency has used a licensed OS so that performance is more optimal and prevent interference from occurring at any time, however, the OS is licensed only for certain components, not all components use the licensed OS.

4. Installation of Fingerprint in the server room
   The agency has implemented a fingerprint system with a server for server security so that not all parties can enter the server room and only certain parties can enter the server room.

5. Granting access rights on the server
   The agency has provided protection by providing limited access rights on each server. So only those who have access rights can manage the server.

3.4 Security Weaknesses of SI Components in the Company
   A weakness was found in the organization in securing the critical assets component of SI owned. In accordance with the results of the interview these weaknesses are:

1. Only certain computers use a licensed antivirus
2. Still using a third party
3. Human resource capacity is lacking in handling IS problems
4. Server room that is not specific because it is still in the repair stage

3.5 Technology Perspective
   In the technology perspective, there are several processes that have been carried out to find out related information about the key components of the company that support business processes.

3.6 Identification of Key Components
   A key component is a component that can support the main business processes in an organization. Based on the critical asset components, the information system obtained will be processed and searched for what components of the information system assets are included in the key components.

3.7 Vulnerability Evaluation of Key Components
   After obtaining data related to key components based on the critical assets component of SI, a vulnerability evaluation of the key components owned by the Company will be conducted.

3.8 Development Strategy and Plan
   At this stage, a plan will be made to develop a security protection against the company's critical SI assets by conducting an analysis and risk measurement. So that an appropriate risk mitigation plan will be obtained.
3.9 Measurement of Risk
After identifying the risk, the next step is to measure the risk by giving a value or weight to each risk using the FMEA method. Which will produce a list of risk priorities.

3.10 Risk Ranking
Risk levels are grouped based on the risk measurement results that have been added up in the previous stage. The level of risk priority ranking that occurs in the critical SI asset component in the company is based on the risk ranking level.

The results obtained from the ranking table above are that there are 4 risks with a low level and 14 risks with a very low level. Although these risks are low and very low, risk mitigation steps are still being taken to handle any risks that occur and minimize losses for the Company.

4. Conclusion
The conclusions obtained based on the results of research that has been carried out in the data and information management division related to risk analysis and management of the critical asset components of the information system are:
1. Based on the results of risk identification, there are several causes of risk that may make business processes not run smoothly, but the most common causes are:
   - Control and maintenance of SI has not been carried out regularly.
   - Hacker attacks that disrupt websites and networks.
   - Do not have information security management standards
2. Ranking Based on FMEA
   Based on the ranking table using FMEA, the RPN is obtained based on the multiplication of 3 risk assessment factor variables including Severity (magnitude of impact), Occurrence (intensity of failure), and Detection (control ability). The results of the RPN ranking are ranked based on the level of risk, namely from Very High, High, Medium, Low and Very Low. So, there are 18 risks including 4 risks with a low level and 14 risks with a very low level these risks are:

   Based on the risk level table, the risk events that occur are still at a very low risk level (Very Low), because risk events do not always occur frequently and do not hamper business processes that occur but controls related to information technology are still not effective and efficient and placement related to assets - SI assets are still not safe.

5. References
[1] PT XYZ Finance Profile/Financial Report: Annual Report PT XYZ Finance 2018 24 October 2019
[2] Susilo F A and Yaya S T 2018 Digital supply chain development in blockchain technology using Rijndael algorithm 256 IOP Conference Series: Materials Science and Engineering 453
[3] Matondang N Ikna N I and Anita M 2018 Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ) Jurnal RESTI Vol 2 No 1 pp 282 – 287
[4] Putri Alvina H Yupie K 2017 Strategi Mitigasi Risiko Aset Kritis Teknologi Informasi Menggunakan Metode OCTAVE Dan FMEA Techno Com Vol 16 No 4
[5] Purwitasari Melita D and Wellia S S 2017 Analisis dan Mitigasi Risiko Aset TI Menggunakan Framework OCTAVE dan FMEA Fakultas Ilmu Komputer Universitas Dian Nuswantor Semarang
[6] Yaya S T Astari T 2019 Enhance Interval Width of Crime Forecasting with ARIMA Model- Fuzzy Alpha Cut Jurnal TELKOMNIKA 17(3) 1193-1201
[7] Astari R Raziv H D Yaya S T 2019 Security risk analysis of bring your own device (BYOD) system in manufacturing company at Tangerang Jurnal TELKOMNIKA 17(2) 753-762
[8] Rezaei Fatemeh Masoud Ferdosi and M Yarmohammadian 2018 Revised Risk Priority Number in Failure Mode and Effects Analysis Model from the Perspective of Healthcare System International Journal of Preventive Medicine Wolters Kluwer Medknow
[9] Budiarto R 2017 Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA dan ISO 27001 Pada Organisasi XYZ Journal of Computer Engineering System and Science Vol 2 No 7
[10] Husein Gilang M and Radiant V I 2015 Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika (JATEL) Jurnal Teknik Informatika dan Sistem Informasi Vol 1 No 2
[11] Mahardika Krisdana B Agustinus F W and Ariya D C 2019 Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 : 2018 Jurnal Sebatik 1410-3737
[12] Firdaus Nurfitri Z and Suprapto 2018 Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik) Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. Vol 2 No 1 page: 91-100.
[13] Afandi Herman and Abdi D 2015 Audit Keamanan Informasi Menggunakan ISO 27002 Pada Data Center PT. Gigapatra Multimedia Jurnal TIM Darmajaya. Vol 1 No 2