ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse93952020.pdf
https://doi.org/10.30534/ijatcse/2020/93952020

Information System Security Risk Management E-Learning Using FMEA in University

Abram Leonard[1], Nurmaryo Anggito[2], Friska Sialagan[3], Jarot S. Suroso[4]
[1] Information Systems Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Indonesia, Abram.Hasibuan@binus.ac.id,
[2] Information Systems Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Indonesia, Nurmaryo.Anggito001@binus.ac.id,
[3] Information Systems Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Indonesia, Friska.Sialagan@binus.ac.id,
[4] Information Systems Management Department, BINUS Graduate Program – Master of Information System Management, Bina Nusantara University, Indonesia, Jsembodo@binus.edu,

ABSTRACT

The security of information systems in the learning process during the Covid-19 pandemic is very important for educational institutions today, which are based on government regulations that require learning to be done online. In order to prevent the transmission of covid-19, people are advised to stay at home, but the learning process must continue. In the process of learning system risk is a point that must be considered. In online learning, information system security risk management can use the FMEA platform to analyze data security and minimize risks that occur.

Key words: E-learning, FMEA, Information System Security

1. INTRODUCTION

The use of information systems in educational institutions in the current pandemic era is required to be able to adapt teaching and learning activities with new methods. Teaching and learning activities can be carried out by learning online / online. This is done to reduce the risk of transmission, spread and the potential for the formation of the Covid-19 cluster in educational institutions, especially universities. With this online teaching process, a platform system is needed to support this activity.[1]

Several universities in this era began to look at developing online teaching, where this type of teaching is the most widely used since some teachers started putting their courses online, in order to absorb students' attention with teaching materials that are in line with the courses offered. on campus[2].

According to "XL Axiata", customer traffic carrying out learning activities from home increased by 10-15 percent in the third week of March 2020. Access to WFH (Work from Home) and SFH (School from Home) applications increased by 48 percent. The increase in traffic was caused by changes in the way you work and study using the online / remote system from home due to the COVID-19 pandemic. Almost all regions experienced an increase of about 10-15 percent.[3]

In an effort to improve student performance and ability to develop, feedback on the system they have is needed. This data is collected from the activities used (activity data in an online learning environment) such as chat, forums, videos etc. [4]. Various data above allows for access by unauthorized parties and can be misused by the wrong party.

Teaching and learning activities using the E-Learning system are something new for some universities, so they do not yet have an adequate E-Learning system. The college must develop an E-Learning system that suits the needs of a time like this. In addition, in the development and use of the E-Learning system, there are certain risks, plus minimal experience in using the system.

This study aims to find any risks that have the potential to interfere with the teaching and learning process using the E-Learning system. This research is also intended to assist universities to manage existing risks using the FMEA (Failure mode and effect analysis) method.

2. THEORY

2.1 Risk

Risk is generally viewed as something negative, such as loss, danger, and other consequences. This loss is a form of uncertainty that should be understood and managed effectively by the organization as part of a strategy so that it can be added value and support the achievement of organizational goals. [5]

A risk, as explained in the previous section, is an uncertain condition or event which if it occurs can have a

negative or positive impact. Risk occurs cumulatively and can affect an objective. The concept of risk can determine the level of risk (level of risk). Based on the variables used, probability and impact, the level of risk can be classified as follows:[6]

1. Low Probability Low Impact = Low Risk, this risk is a risk that has the smallest level of influence compared to other risks, so in certain policies this risk can be ignored.
2. Low Probability High Impact = Moderate Risk, Risk is a risk that has an intermediate position, where this risk must be monitored and requires treatment, with handling depending on the impact given.
3. High Probability Low Impact = Moderate Risk, Risk with medium influence. Unlike the low probability high impact impact, this risk only needs to be monitored.
4. High Probability High Impact = High Risk. The risk that has the highest effect when compared to other risks. This risk is the most dangerous risk and one that must be treated promptly

According to Suganda (2015) risks can be grouped into six types, namely:

1. Pure risk is a risk where possible has a loss, but possibly no gain, one example is fire and accidents.
2. Speculative risk is the risk where we expect losses as well as gains. This risk usually exists in the business world.
3. Status risks arise from certain equilibrium conditions such as risks arising from natural conditions. These risk characteristics have practically no effect over time.
4. Dynamic risk arises from changes in certain conditions such as changes in technology, changes in social conditions.
5. Objective risk is a risk based on objective parameter observations.
6. Subjective risk is a risk based on a person's perception of risk.

Risk management is a series of processes in identifying risks, conducting risk assessments, and developing a series of actions to reduce these risks to a level acceptable to the organization.[7]

2.2 Information Security

The term information security is used to describe the protection of hardware, data, software, infrastructure, and information from misuse by unauthorized parties. [8]

Information security threats are people, organizations, mechanisms, or events that have the potential to compromise company information resources. Information security threats can be internal and external, including company employees, temporary workers, consultants, contractors, business partners. Based on a survey conducted by the computer security institute, it found that 49 respondents faced security incidents caused by the wrong actions of users.[8]

2.3 Information Security Management System

Information Security Management System is a way to protect and manage information based on a systematic business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security [9].

The Information Security Management System aims to minimize the level of risk arising from the exchange, processing, storage, traffic and disposal of data and information. [10]

2.4 FMEA (failure Mode Effect Analysis)

FMEA is an analytical method to find errors that have the potential to occur in the future. FMEA is systematic and can improve operational performance in the production cycle and reduce the level of risk received. FMEA has been in use since about 40 years ago, but its widespread spread began around the 1990s. Its spread stems from the use of the "QS-9000" by the US automotive industry in the 1990s. "QS-9000" is an international quality standardization system developed by the "International Automotive Task Force (IATF) in 1996".[11]

3. METHODOLOGY

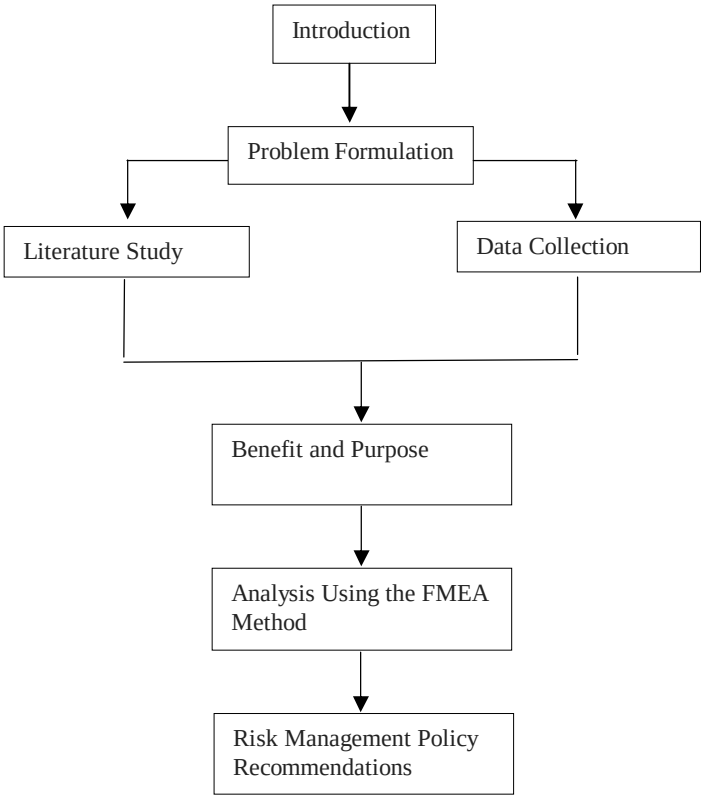

Figure 1: Framework used

1. Introduction
   In this stage it is used to define the background of the research, by looking at the current conditions of online teaching and learning.
2. Problem Formulation
   The next step after analyzing from the introduction is to identify the problems that will be discussed later, so that the research does not get off track.
3. Literature Study
   In the literature study, namely the process of studying literature related to risk management. Done to produce a basic reference that can be used in research.
4. Data Collection
   In data collection, researchers collected data by conducting group discussions, mentoring lecturers, and collecting data from higher education institutions.
5. Purpose and Benefit
   In this stage, namely determining the goals and benefits to be achieved from the research to be carried out.
6. Analysis using FMEA method.
   The analysis using the FMEA method consists of ten stages.

According to Chrysler (1995), FMEA can be done by:

- Recognizing and evaluating the potential failure of a product and its effects
- Identify actions that can eliminate or reduce the chance of potential failure to occur
- Recording process so that documents need to be updated regularly so that they can be used to prevent and anticipate failures. [12]

FMEA (Failure mode and effect analysis) stages:

- Step 1 Review the process and product
- Step 2 Think and look for models that have the potential to fail.
- Step 3 Describe the effects of the failed model.
- Step 4 Determine the severity of the effects.
- Step 5 Determine the rank of each failure model.
- Step 6 Determine the tracking rating for each failure model.
- Step 7 Calculate the risk priority level of each failure model.
- Step 8 Prioritize the failure model that must be implemented.
- Step 9 Take steps to reduce or eliminate high risk failure models.
- Step 10 Calculate the RPN value when the failure model is reduced or eliminated.

* RPN (Risk Priority Number) = measuring tool when determining risk to assess critical failure models or should be prioritized.

Severity * Occurence = Criticallity

Severity * Occurence * Detection = RPN

Below is the FMEA (Failure mode and effect analysis) worksheet used.

Failure Mode and Effects Analysis Worksheet

Process or Product: _____ FMEA Number: _____
FMEA Team: _____ FMEA Date (Original) _____
Team Leader: _____ (Revised) _____
Page: 1 of 1

	FMEA Process										Action Results				
Line	Component and Function	Potential Failure Mode	Potential Effect(s) of Failure	Severity	Potential Cause(s) of Failure	Occurrence	Current Controls, Prevention	Current Controls, Detection	Detection	RPN	Recommended Action	Responsibility and Target Completion Date	Action Taken	Severity	Occurrence	Detection	RPN
1																	
2																	
3																	
4																	
5																	
6																	
7																	
8																	
9																	
10																	

Figure 2: FMEA Worksheet

7. Risk Management Policy Recommendations
   At the end of this research will produce results in the form of an approach that can be used to reduce risks in the learning process by using the FMEA method.

4. DISCUSSION

FMEA is generally used in the early stages of production of a product, it aims to reduce costs by identifying products and processes so that they are easy to modify at the beginning.

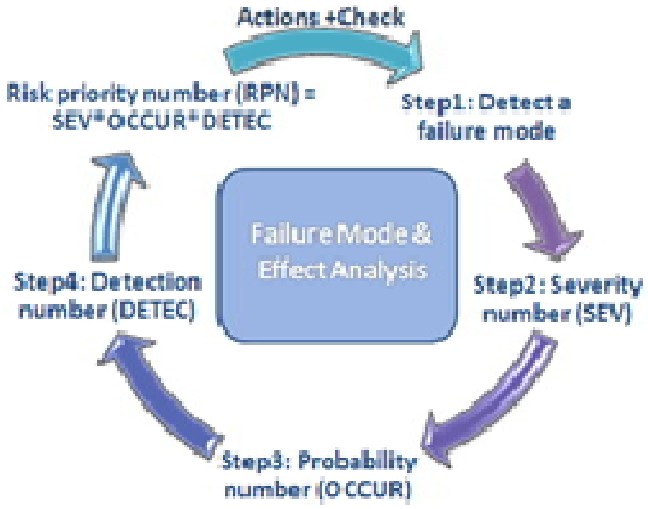

Figure 3: General FMEA stages

In the picture above, there are general FMEA stages and will be explained in detail below using the 10 FMEA steps that occur during the online learning process in tertiary institutions:

1. Write down all the main steps in the process that outline the learning process.

2. List potential errors (failure mode) for each step of the process by analyzing and finding the points of error that may occur at each stage of the process.
3. List the effects of the failure modes listed earlier. If something goes wrong, estimate the effect the process owner (you) will have on your customers.
4. Make a rating, which effect is the largest to the smallest. Give a number 1 for the least effect, and 10 for the biggest effect and make sure the team understands and approves the rating before you start. Enter a number in the 'SEV' (severity) column.
5. Identify the cause of the failure mode (error) causing this effect. Make a rating like you did for the effect list above identifying which causes are most likely and which are least likely. Give the number 1 for the lowest probability and 10 for the highest probability. Enter in the column "OCC" (occurence).
6. Identify the controls in place to detect error issues on your list, and rate them according to their effectiveness in detecting and preventing errors. A value of 1 means that you have practically perfect control, and a number 10 means that you have no control over failure, or have control but are very weak. Enter in the 'DET' (detection) column. If any SOPs are identified, write down the SOP number.
7. Multiply the numbers in the severity (SEV), occurrence (OCC), and detection (DET) columns and enter the results in the 'risk priority number' (RPN) column. This column will generate numbers that will help your team to prioritize focus. If, for example, you have points of severity 10 (greatest effect), occurrence 10 (occurs all the time), and detection 10 (undetected), the RPN value will be 1000. This means the condition is very serious.
8. Sort the value on the RPN and identify the most critical and urgent issues to be addressed immediately, where the team must prioritize focus.
9. Define specific actions to be taken and delegate them to the person responsible for the area. Don't forget to set a deadline date, when this action should start / finish.
10. After the action is performed, recalculate the occurrence and detection values. In most cases, the severity does not need to be changed unless the customer decides that it is not an important issue.

5. CONCLUSION

By using the FMEA (Failure mode and effect analysis) framework, it really helps universities to analyze the level of security of information systems in the learning process in the network using 10 stages and MFEA (Failure mode and effect analysis) worksheets. Thus the prevention of information system security risks can be done to minimize the risks that will occur in the future and this greatly helps universities in carrying out their business processes and is an asset going forward. Learning that is carried out online is a learning technique that benefits both parties between universities and students who have limitations both in terms of time and distance that make it impossible to do face-to-face learning when the Covid-19 pandemic has ended.

REFERENCES

[1] S. Arsendy, G. A. Sukoco, and R. E. Purba, “Riset dampak COVID-19: potret gap akses online ‘Belajar dari Rumah’ dari 4 provinsi,” *https:/Theconversation.com*, 2020. .

[2] S. Ouhrir, S. Lotfi, and M. Talbi, “of Advanced Science and Students ’ Views on E-learning and Knowledge of Learning Platforms : Case of a Professional License at the Higher Normal School of Casablanca,” vol. 8, no. 5, 2019.

[3] C. RIZKIA, “XL Axiata Catat Kenaikan Trafik Data Selama WFH dan SFH,” 2020. .

[4] Z. Lahbi and M. Sabbane, “U-Edu: Multimodal learning activities analytics model for learner feedback in ubiquitous education system,” *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 5, pp. 2551–2555, 2019.

[5] G. Soputan, B. Sompie, and R. Mandagi, “Manajemen Risiko Kesehatan Dan Keselamatan Kerja (K3) (Study Kasus Pada Pembangunan Gedung Sma Eben Haezar),” *J. Ilm. Media Eng.*, vol. 4, no. 4, p. 99095, 2014.

[6] A. Lokobal, D. Pascasarjana, T. Sipil, and U. Sam, “Pelaksana Konstruksi dI Provinsi PAPUA (Study Kasus di Kabupaten Sarmi),” *J. Ilm. Media Eng.*, vol. 4, no. 2, pp. 109–118, 2014.

[7] G. Stoneburner, a. Goguen, and a. Feringa, *Risk Management Guide for Information Technology Systems*, vol. 800–30. 2002.

[8] M. Junior, “Sistem Informasi Manajemen Jilid 1,” p. 330, 2001.

[9] I. Desy, B. C. Hidayanto, and H. M. Astuti, “Penilaian Risiko Keamanan Informasi Menggunakan Metode Failure Mode and Effects Analysis di Divisi TI PT. Bank XYZ Surabaya,” *Semin. Nas. Sist. Inf. Indones.*, no. September, pp. 467–472, 2014.

[10] “About ISMS-AC,” 2009. .

[11] M. A. Bennett, R. McDermott, and M. Beauregard, *The Basics of FMEA*. 2017.

[12] F. Kustiyaningsih, “Penentuan prioritas penanganan kecelakaan kerja di pt ge lighting indonesia dengan metode failure mode and effect analysis (fmea),” *Skripsi. Univ. Sebel. MARET*, 2011.