

IT Risk Identification and Evaluation: a Case Study on XYZ University

Daniel Albertivan^{#1}, Hendryantono Limantara^{#2}, Reza Annisa Rachmadiati^{#3}, Adik Wedsa Pamungkas^{#4}, Nico Surantha^{#5}

[#]Computer Science Department, Binus Graduate Program-Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia.
E-mail: ¹daniel.albertivan@binus.ac.id; ²hendrayantono.limantara@binus.ac.id; ³reza.rachmadiati@binus.ac.id, ⁴adik.pamungkas@binus.ac.id; ⁵nico.surantha@binus.ac.id

Abstract— The purpose of this paper is to demonstrate that Failure Mode Effect Analysis (FMEA) can be applied to the educational field to identify various failure modes and its potential failure effect that could occur in anytime. FMEA is widely used in a design, a manufacturing or assembly process, or a product and service for identifying all possible failures. Risk identification is part of risk management. Therefore it is a critical first step of it. This paper is a case study on XYZ University which trying to implement risk management which only focused on how to identify the risk using FMEA. FMEA needs some parameters to be defined which are severity values, the likelihood of occurrence, and detection. Risk Priority Number (RPN) is a matrix that indicates potential risk calculated by multiplying the three components, and it used to classify which should be taken care of first based on the highest RPN value. Filtering the ticketing system and mapped the incidents that happened to the current business process is how the data collected, also the interview to end user for validation. The result of this paper is astonishing because it is different from the initial expectation that business process like LMS or network facility will get the highest RPN value, but after doing all the process, it is found that telecommunication is at the top. Surely this provides a new perspective to risk management to be slicker in handling potential one.

Keywords—educational; Failure Mode Effect Analysis; FMEA; risk; risk management.

I. INTRODUCTION

The risk is a situation involving exposure to danger or harm. In an organization, the risk is a part of doing business; it is a challenge for every company. Risks can have consequences in financial, reputation, development and performance itself [1]. If an organization pays much attention to manage the risk effectively, it will help organizations to perform well in an uncertain environment. It is not only talking about the negative impact on an organization but also a positive impact. A positive risk, if managed well, can turn into an opportunity for the organization [2].

Risk management is a combination of science and art of identifying, analyzing, and responding to an uncertain condition. In terms of project management, the risk will remain in the life of a project and until the project is to meet the project objectives. Risk management will help the project manager and team to achieve the goals by improving the process of determining project scope, developing realistic estimation and with the selection of good projects [3]. Failure in managing risk can harm the organization as well as the client involved with the project. Davy Corporation, the project completed two years behind

schedule and poor management of project risk was damaged not only Davy, but also the clients, and Trafalgar House who bought Davy Corporation [4]. Risk management approaches nowadays become more complex because it integrates many additional risk domains [5], but this paper only involves both Information Technology (IT) and Business domain. It was proven to increase the chance of business sustainability, enhance the business process, and value added. The study shows that the framework of organizing detailed information efficiently is useful to help risk assessment process and assists in making the decision C level [6], [7].

The objective of this paper is to present the use of Failure Mode Effect Analysis (FMEA) to define and identify the risk specifically related to network infrastructure, how to convert the collected data into useful information to identify and evaluate three factors of FMEA. The aim is resulting in a Risk Priority Number (RPN) which acts as an indicator for determining proper action by resulting a table of risk severity, hence the most critical risk will be prioritized and could be mitigated.

II. MATERIAL AND METHOD

A. Material

1) Failure Modes and Effect Analysis

Failure Modes and Effect Analysis (FMEA) is a methodology designed by U.S Military in the 1940s, to identify any potential failure modes before the problem happened and used to assess the risks of a product or a process [8]. FMEA was first developed in the 1960s by the aerospace industry as a formal design methodology in order to fulfill the reliability and safety requirements [9]. Nowadays it has been spread to other industries, such as oil and gas, and automotive. FMEA was built to identify and prioritize all the possibility of imperfection in products or process. It also can be defined as a set of procedure to examine any potential failure in a system and determine the impact to the whole system and classify each potential failure according to its how severe it will affect [10]. FMEA has some components to be calculated:

- Severity (S): is a numerical estimate of how severe end user will be affected because of the failure event, it is a 10-point scale, ten is the highest.
- Occurrence (O) or likelihood, is a numerical estimate likelihood of a failure mode will occur during production. It is a 10-point scale, ten is the highest.
- Detection (D) or can be termed as effectiveness, is a numerical estimate of how effective the control that has been made to detect the root cause or failure mode before it is happening or to prevent it from happening. It is a 10-point scale; ten is the highest.

Risk Priority Number can figure out the seriousness of potential risk indicated the larger RPN values. If the RPN is identical, the Severity (S) multiply by Occurrence (O) = $S \times O$ should be considered because the occurrence plays more role after the severity in risk management [11].

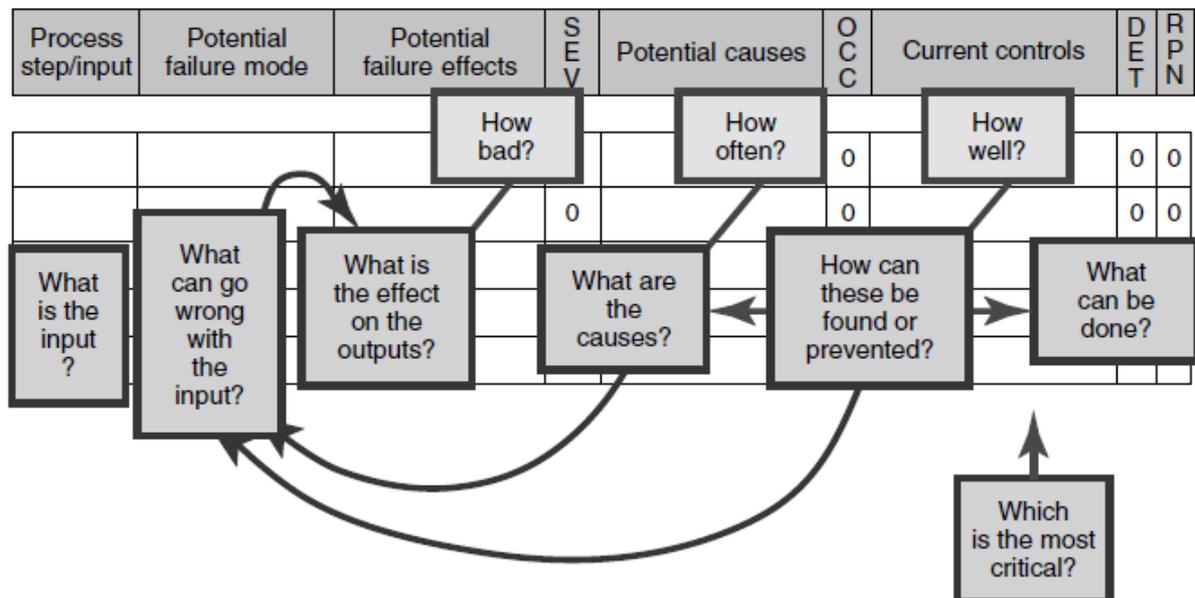


Fig.1 FMEA table and rating chart [12]

2) Project Risk Management

Project risk management is part of the Project Management Book of Knowledge (PMBOK) which are generally accepted as the greatest practice within project management [13]. The main objective of risk management implementation is to increase the chance or likelihood of definite risk, can be addressed as an opportunity and reduce the likelihood of negative risk in a project [14]. Regardless of the positive or negative it will be, the application of identifying risks has a positive effect because the organization has information to know what potential of failures they will face and assess and prepared some precaution before the events of failure are happening and impact more damage to the organization [15].

The handling of risk in a project using risk management becomes the most critical part of predicting what may occur in the future [16]. Deciding how to achieve better risk

management is very important. Risk management process has several steps [17], here are a modified process which focused on how to identify the potential one as follow:

B. Case Study

XYZ University is a private university in Indonesia which part of AB Group. XYZ University has more than 30.000 students active all over Indonesia. In the year 2017, AB Group started a project to build another campus. The bridging campus was built to accommodate the interest of prospective students as a temporary campus before the main building is built. There, all the operational activities such as learning activities and office activities are carried out. Although classified as a bridging campus, there are many things to be considered regarding IT infrastructure, such as the network infrastructure as the primary concern in this

paper. The employees in bridging campus need to access some applications located in the head office in Jakarta, also synchronizing the data with the head office, they need to communicate with the head office daily. This paper could be a guide to the XYZ University to identify what risk will be

likely to occur and what should be the main concern while maintaining existing infrastructure and also knowing the maturity of the current business process as important factor to be considered [18], [19].

TABLE I
PROJECT RISK MANAGEMENT PROCESS

Project Risk Management Process	Description
Identify Risks	This is a critical step. It produces a potential risk register which may occur in every field of works. This step should identify the risks that may occur in all areas also the impact on the current system.
Analyze and Evaluate Risks	After the risk register is produced, the next step is to analyze and evaluate. FMEA is used to analyze each of identified risk based on failure mode or in this paper is the reason for outages. It also helps to evaluate the level of risk based on the severity, likelihood, and detection. Not all risk has the same level of losses. Evaluating the severity and likelihood of occurrence will provide a new perspective on potential risk so that consideration in making decisions will make it more reasonable.
Risk Mitigation	Once the risk has analyzed and evaluated, for reducing the impact or likelihood of occurrence in acceptance level, a strategy in responding to the risk is needed. The strategy is known as mitigation risk. In handling risk mitigation there are some options such assume or accept, avoid, control, transfer, watch or monitor.
Risk Monitoring	The purpose of this step is for tracking and ascertaining whether the organization followed policies. Although strategies in managing risk were once decided within the organization monitoring risk is about assessing whether the strategies still effective or not.

C. Related Work

A study in risk management has been widely researched with various model from identity, handle, and mitigation to monitoring. Also, to compete with a competitor, the company needs to keep up the quality and reliability of the product while continuing in identified and manage the risk that occurred.

Risk mitigation plan should facilitate the process of identification circumferential opportunities and risks itself [20]. Risk mitigation can be conducted by reviewing and identifying risk mitigation activities, technology, technique, procedure, people, process and method used in IT Governance [21]. Most of the existing models and framework of mitigating risks cannot support IT Governance to mitigate risks. Thus, risk mitigation components and metrics are important and should be considered when mitigating risks [22].

FMEA also used to analyze the current state of services within an acute care healthcare organization, and it is recommended to use FMEA before implementation of any new service as one of an effective method for yielding highest quality [23].

However, identified and assess risk much easier task than to suggest a proper mitigation plan because handling risk needs to be ready in advance, so the risk will not become bigger when it appeared. So once determined risk by its priority, handling and mitigation strategies need to be determined too for each risk factor [24]. Torabi and Giahi also using FMEA to enhance risk assessment which becomes the main parts of a business continuity management system [25]. FMEA is also studied by Tejaskumar S.Parsana dan Mihi T. Patel to improve the quality and efficiency of Manufacturing Industry. The prevention action also proposed according to risk prioritization [26].

Enterprise risk management (ERM) used by xyz university

is a systematic and integrated approach to managing all forms of risks that may confront directly or indirectly. It focused on the whole enterprise as a big picture. However, FMEA can help current system to be assessed the possible ways in which failure might occur, assess the impact of the failure and understand what preventive action can be taken before such failures occurring [27].

D. Methodology

The data was collected from the ticketing system and interview user for validation. The classification of risk is according IT service catalogs which provided by IT division. All the incidents are mapped to the service catalogs in brainstorming way involving all risk-related team to ensure the validity. The data shows that the main business process related to IT infrastructure and services at XYZ University are as follows:

1. Attendance system is required to record all attendance of employees. The system is using SAP. Each employee can do attendance at any site of XYZ University. Attendance can be done via fingerprint or the web-based on SAP Portal.
2. Learning Management System (LMS) for Regular Program Student is an information system for a regular student, used by the lecturer and student to support academic learning. This system is used by the entire regular program student, both Bachelor, and master degree and in all majors. Attendance, discussion forum, course material, information regarding financial status can be accessed through the LMS.
3. Financial System is using SAP web-based application and has several functions to accommodate the task of finance officer such as purchase request, leave request, medical billing, and budgeting.
4. Learning Management System (LMS) for Online Program Student is an information system for students who prefer online program classes of how classes are conducted every day, used by the lecturer and student to support the

academic learning. This system is used by the entire online program student, a bachelor degree and master degree and for all majors. Attendance, discussion forum, course material, information regarding financial status can be accessed through the LMS.

5. Email acts as a communication medium between internal parties and external parties. The purpose of using official email is to build a professional image to external parties. Email is divided into two, for student/lecturer and the employees. Because of a great number of students, so email for students and lecturers are using office 365 which integrated with LMS as a single sign-on. Meanwhile, the email server for employees is using the on-premises exchange server because the number of employees is not as many as students.

6. Video conference is a service supported by IT division in order to accommodate the needs of online meeting, distance learning in a different location, and for the student of the online program. It is using many platforms, such as Cisco WebEx, Skype for business, Cisco Telepresence, Cisco Jabber. Cisco Webex is used to support online classes. Cisco telepresence is used for meetings between different campus locations. Skype for business and cisco jabber are used for meeting with external parties. Video conference is also held for meetings with other universities both at home and abroad.

7. Telecommunication is required to save the cost by using a telephone, so the communication between employees in a different location can be done with lower cost and quickly. This service also provides communication with external parties, using the billing system. The service is vital for marketing staff because of daily task communicate with external parties. This plays a vital part in customer services to help customers efficiently and ensures they are satisfied

8. Online Admission acts as a virtual representative where prospective students can do online registration.

9. Network facilities are provided to facilitate employees so that they can access the internal system. Wired typically used by an employee while lecturer and student use wireless. Both of them have different rules, but both can access the internal system corresponding to their regulation.

In this paper, the author modified some name of the column table of RPN, which are potential failure mode as RFO and potential failure effect as impact. The name changed because it is more reasonable to be used in the educational field.

Severity criteria are determined by assessing the risk impact which can disturb the business process wholly, or it only affects some individual in a division. The frequency of occurrence is determined by how often the same incident is happening. These incidents are recorded, by calculating these records, it will bring out frequency level of the likelihood for an incident will happen. Detection describes the perspective of the university, if the incident is happening, how bad it will affect the quality of services, is the service still useable or it is unusable and also it measures how effective current design control works. The author used the model of table based on Tejaskumar's work as follow [23]:

TABLE II
TABLE OF SEVERITY

Effect	Criteria	Rank
Hazardous Without Warning	Business Loss	10
Hazardous With Warning	Some business processes in some divisions will be affected	9
Very High	Business processes will be affected	8
High	One business process will be affected in one division	7
Moderate	One business process will be affected in one division	6
Low	Affected some people in some divisions	5
Very Low	Affected some people in a division	4
Minor	Affected only one people in the division	3
Very Minor	Affected only one people, will not affect his task	2
None	No Effect	1

Table 2 shows the criteria of severity used to specify the impact of a potential risk that may occur to the current business process which has been explained. The criteria cover from how failure affected to no people, affected some people till the loss of ability in running the existing business process resulting in a business loss.

Next step is to define the table of occurrence which shows as follow:

TABLE III
TABLE OF OCCURRENCE

Effect	Frequency of Occurrence	Rank
Very High	Several times a day	10
	Once a day	9
High	Three times a week	8
	Two times a week	7
Moderate	One time a week	6
	The specific event will occur	5
Low	In some events will occur	4
	Once a month	3
None	Unpredictable	2
	Once a year	1

Table of occurrence consists of the period in which an incident may occur. This period is measured by looking at the existing ticketing system, in which when sorted by time and mapped to recurring incidents and it created a specific pattern of the period. The criteria cover from it only occurred once a year or occur at an unpredictable moment to several times a day which disturb for most of the people. The result is shown in Table 3.

The next step is to determine the detection of the current condition. Detection relatively measures the ability to design control to detect or prevent a potential cause or reason for outages that might happen. In this paper, the author put the pre-incident response which can be a picture as a detection

control which has been done by the university to prevent bad things happen.

TABLE IV
TABLE OF DETECTION

Detection	Criteria of Detection	Rank
Very High	No design control	10
	Unproven design control	9
High	Design control have poor chance of detection	8
	Design controls are likely to miss the problem	7
Moderate	Design controls may miss the problem	6
	Design controls have an even chance of working	5
Low	Design controls are moderately effective	4
	High probability of detection	3
None	Very High probability of detection	2
	Controls will almost certainly, detect	1

The data that previously discussed can be used to calculate The Risk Priority Number (RPN) by multiplying three elements which are Severity, Occurrence, and Detection. The formula is:

$$RPN = Severity \times Occurrence \times Detection$$

RPN can help the risk-related team to identify potential risks to make a plan that should be taken, either mitigate, eliminate or transfer it to professional companies.

According to the interview, communication via phone has become very important for daily activity. It is considered more efficient than the email. Besides, it can shorten the time when critical conditions occur and also when students or parents want to get some information right away. For some people, it is essential to keep the line of communication always available especially if associated with phone service.

The Marketing team needs good and reliable telecommunication service so they can do a telemarketing approach to the prospective students. It will increase the effectiveness and efficiency also the chance number of student intakes. Personal approach and more trusted relationships can be built through the telecommunication way. Although their many methods to get connected with the customers, such as using instant messenger, we believe that good communication begins with warm personal communication over the phone.

Also, the Learning Management System (LMS) acts as a bridge between university and students, any information related to courses, exams or financial status can be accessed here. LMS plays huge role in the learning process because whenever there is a failure it will impact learning process that day, and it is everlasting for several days which disrupted the learning activity such as upload and download

learning materials or accessing the forum. LMS is often get disrupted during the score announcement, during the announcement of new classes schedule and also at the end of the due date of project submission. Therefore, the anticipation that has been done is added to the server's capacity and use load balancing techniques to distribute the workload across many servers. An explanation of why there are two LMS because they run different systems, maintained by different teams and have different functions, so it requires two different systems running simultaneously.

Most of the services are related to a network infrastructure which becomes an essential part of current services. However, the discussion is about how to break down all potential failure of a product, process or systems. Identify the actions needed that could eliminate or reduce the chance of potential failures and document the process.

Table 5 shows the matrix calculation of RPN. Weights should be incorporated into each identified business process so that the RPN score will appear after the process of multiplication is performed. Small RPN is always better than high RPN. It is recommended to begin an action with high RPN and working in descending order the objective is to reduce one or more potential risk that make up the RPN. The use of a Pareto chart is giving the picture the most important areas to be solved as soon as possible as the RPN score is calculated.

It is explained earlier that to get the weight of each column of severity, occurrence, and detection is through brainstorming and consideration of team-related risks. Reason for Outages (RFO) is determined using the records of incidents. It classified something that already happened before, or it can be something that acts as an agent of failure in the future in the main business process. The column can be assigned what can happen in the event of failure and the impact on the ongoing business process. The data in this column is taken from previous incidents and added with the result of the discussion on the broader impact if the failure occurs. Pre-incident responses are precautions that have been thought and done and are running to date to minimize the effects that will occur in the event of a failure or can be said to be current control. In the FMEA in this paper added this column to facilitate the determination of the score of each column. Risk Managers and the team discussed every criterion in the RPN matrix. The result of the brainstorming to fill the weight of each criterion of RPN is as follows:

III. RESULTS AND DISCUSSION

Table 5 shows the FMEA process where the objective is to produces RPN scores. It scales from 1 to 1000. Each variable has a scale from 1 to 10. When all each of it is filled in then we multiply it. From table 5, we create a Pareto Chart to identify which service needs to be prioritized based on the Pareto Principle [28].

TABLE V
PROCESS FAILURE MODE AND EFFECT ANALYSIS

No	Services	RFO	Impact	Severity	Occurrence	Detection	Pre-Incident Response	RP N
1	Attendance	Hardware Failure	Over time & Attendance Calculated need to be done manually	5	2	3	Multiply Attendance Spot	30
		Network Failure					Backup Connection	
		Server Down						
		Unregistered User						
2	LMS Regular Student	Application Error	Student and lecturer cannot access the course material, schedule, attendance is done manually and user satisfaction decreased	8	8	7	Increase the number of servers and server capacity	448
		Server Down					Implement load balancer server	
		Server Slow						
		Unregistered User						
		Network Failure						
3	Finance System	Application Error	Employees cannot access the financial system, procurement, and human capital	6	2	7	Make backup data of server finance	84
		Server Down						
		Server Slow						
		Unregistered User						
		Network Failure						
4	LMS Online Student	Application Error	Student and lecturer cannot access the course material schedule, attendance system running manual and user satisfaction decreased	8	6	9	Increase the number of servers and server capacity	432
		Server Down						
		Server Slow						
		Unregistered User						
		Network Failure						
5	Email	Server Down	Student, Lecturer, and employees cannot send and receive email	8	2	7	Separating the email server of student and lecturer to cloud service	122
		Unregistered User						
		Network Failure						
		Storage Full						
		Spam Indication						
6	Video Conference	Network Failure	Online learning, online meetings, and activities that require video conference cannot be done	6	4	5	Make a redundancy of Internet Link	120
		Internet Down						
7	Telecommunication	Network Failure	Communication becomes ineffective, bring down the number of student intake, reduced customer satisfaction, and increased communication costs	9	9	9	Make a redundancy of Internet Link to each site	729
		PABX Server Down						
		Device Broken						
8	Online Admission	Server Down	A student cannot register online and bring down the number of student intake	7	4	7	Backup database server	196
		Network Failure						
		Unregistered User						
		Application Error						
9	Network Facility	Internet Down	All activities that require the network would be disrupted	9	2	8	Make a redundancy of Internet Link to each site	144
		Network Failure						
		Hotspot issue						
		Unregistered User						

ACKNOWLEDGMENT

We would like to acknowledge the support from Bina Nusantara University for making this work under the Bina Nusantara Graduate Program, Magister of Information Technology.

REFERENCES

- [1] Antonio, B., & Gaudenzi, B. (2013). Risk Management. <https://doi.org/10.1007/978-88-470-2531-8>.
- [2] Wickboldt, J. A., Bianchin, L. A., Lunardi, R. C., Granville, L. Z., Gaspary, L. P., & Bartolini, C. (2011). A framework for risk assessment based on an analysis of historical information of workflow execution in IT systems. *Computer Networks*, 55(13), 2954–2975. <https://doi.org/10.1016/j.comnet.2011.05.025>.
- [3] Zou, P. X. W., Wang, S., & Fang, D. (2008). A life-cycle risk management framework for PPP infrastructure projects. *Journal of Financial Management of Property and Construction*, 13(2), 123–142. <https://doi.org/10.1108/13664380810898131>.
- [4] Fontaine, M. (2015). Project Risk Management. *Enterprise Risk Management: A Common Framework for the Entire Organization*. Elsevier Inc. <https://doi.org/10.1016/B978-0-12-800633-7.00004-3>.
- [5] Huth, M., Vishik, C., & Masucci, R. (2016). From Risk Management to Risk Engineering: Challenges in Future ICT Systems. *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber-Physical Systems*. Elsevier Inc. <https://doi.org/10.1016/B978-0-12-803773-7.00008-5>.
- [6] Ko, D. G., & Kirsch, L. J. (2017). The hybrid IT project manager: One foot each in the IT and business domains. *International Journal of Project Management*, 35(3), 307–319. <https://doi.org/10.1016/j.ijproman.2017.01.013>.
- [7] Liu, S. (2016). How the user liaison's understanding of development processes moderates the effects of user-related and project management risks on IT project performance. *Information and Management*, 53(1), 122–134. <https://doi.org/10.1016/j.im.2015.09.004>.
- [8] Lipol, L., & Haq, J. (2011). Risk analysis method: FMEA/FMECA in the organizations. *IJESEAS International Journal of Basic & Applied Sciences*, 11(05), 74–82.
- [9] Santos, F. R. S. dos. (2008). Fmea and Pmbok Applied To Project Risk Management. *JISTEM Journal of Information Systems and Technology Management*, 5(2), 347–364. <https://doi.org/10.4301/S1807-17752008000200008>.
- [10] Shinde, R. R., & Morey, R. B. (2015). Failure Mode Effect Analysis-Case Study for Bush Manufacturing process. *IJESEAS International Journal of Scientific Engineering & Applied Sciences*, 1(4), 283-294.
- [11] Thakore, R., Dave, R., & Parsana, T. (2015). Research Article A Case Study: A Process FMEA Tool to Enhance Quality and Efficiency of Bearing Manufacturing Industry, 3, 413–418. <https://doi.org/10.9756/BIJEMS.10350>.
- [12] Kritzinger, D. (2017). Failure Modes and Effects Analysis. *Aircraft System Safety*, 101–132. <https://doi.org/10.1016/B978-0-08-100889-8.00005-2>.
- [13] Jamali, G., & Oveisi, M. (2016). A Study on Project Management Based on PMBOK and PRINCE2. *Modern Applied Science*, 10(6), 142. <https://doi.org/10.5539/mas.v10n6p142>.
- [14] Schwalbe, K. *Information Technology Project Management, Revised 6e.*, Course Technology, Cengage Learning, 2011.
- [15] PMI. (2013). *A Guide to the Project Management Body of Knowledge. Project Management Institute (Vol. 5)*. <https://doi.org/10.1002/pmj.20125>.
- [16] Rodríguez, A., Ortega, F., & Concepción, R. (2017). An intuitionistic method for the selection of a risk management approach to information technology projects. *Information Sciences*, 375, 202–218. <https://doi.org/10.1016/j.ins.2016.09.053>.

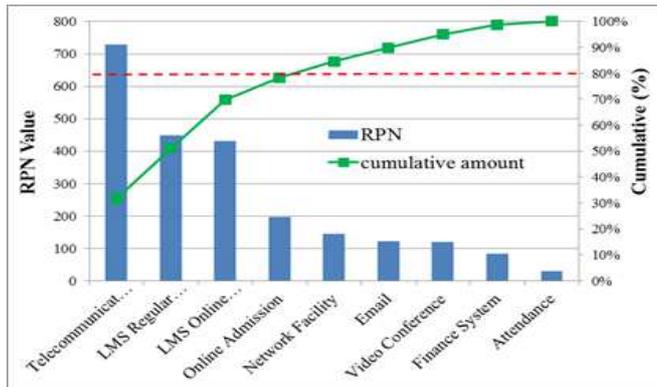


Fig. 2 Pareto chart of risk priority number

The left vertical axis of the Pareto chart represents RPN values. Vertical bars represent each service and the left has the highest RPN values. The cumulative line is used to add the percentage from each bar. It determines how much of the total services should be fixed by addressing the highest few in Pareto chart.

We identify services that contribute to 80% of the risk. Figure 2 shows that the telecommunication, LMS regular student, LMS online student, and online admission contribute to the 80% risk of the system. Therefore, we advise prioritizing on that four services to be solved as soon as possible.

IV. CONCLUSIONS

In this paper, the author used FMEA to identify various failure modes and its potential failure effect that could occur in a current business process that applied to an educational field which commonly used to in industrial field to enhance a process or to improve steps of making a product.

This paper reaches deeply to the source of failure by the interview end user and classify every incident reported in the ticketing system which resulting reason for outages and also explains the impact explicitly to the current business process. Although it seems Network facility or LMS will be a prime candidate from the list of risks that exist but using the FMEA give another point of view, new perspective of a current business process which result shows telecommunication is at top priority list. Telecommunication area should take more precaution hence it will not interfere current business process whenever the failure happens. If a catastrophic event occurs, the media coverage may affect the campus's reputation, posing a threat to future admissions and so financial strength. The risks faced by the university are diverse, and the loss potentials are enormous. The risk manager must be vigilant in protecting the organization's assets from both direct and indirect potential losses. By developing and implementing a comprehensive risk management plan, a university will hold a dynamic tool that can serve as a road map for identifying and managing risk exposures.

However, this paper is only focused on the process of risk management which is concentrated in the assessment of risk. Further work should be concentrated on mitigating and monitoring the risk of minimizing potential negative risks and maximizing potential positive risks.

- [17] Ennouri, W. (2015). Risk Management Applying Fmea-Steg Case Study. *Polish Journal of Management Studies*, 11(1), 56–67.
- [18] Rodrigues-da-Silva, L. H., & Crispim, J. A. (2014). The Project Risk Management Process, a Preliminary Study. *Procedia Technology*, 16, 943–949. <https://doi.org/10.1016/j.protcy.2014.10.047>.
- [19] Zeb, J., Froese, T., & Vanier, D. (2013). Infrastructure Management Process Maturity Model: Development and Testing. *Journal of Sustainable Development*, 6(11). <https://doi.org/10.5539/jsd.v6n11p1>.
- [20] Khatavakhotan, A. S., & Ow, S. H. (2012). An innovative model for optimizing software risk mitigation plan: A case study. In 2012 Sixth Asia Modelling Symposium (pp. 220-224). IEEE.
- [21] Tonny, B., Pa, N. C., Nor, R., Nor, H., Jusoh, Y., Information, G., & Systems, T. (2016). Development and Initial Results of a Component Model for Risk Mitigation in IT The Development and Initial Results of a Component Model for Risk Mitigation in IT Governance, (December).
- [22] Jnr, B. A., Pa, N. C., Nor, R., Nor, H., & Josoh, Y. Y. (2016). The Development and Initial Results of a Component Model for Risk Mitigation in IT Governance, 2(2), 1–13.
- [23] Polancich, S., Rue, L., Poe, T., & Miltner, R. (2018). Proactive Risk Mitigation: Using Failure Modes and Effects Analysis for Evaluating Vascular Access. *Journal for Healthcare Quality*, 40(1), 58–65. <https://doi.org/10.1097/JHQ.0000000000000125>.
- [24] Shahzad, B., & Afzal, S. (2010). Risk Mitigation And Management Scheme Based On Risk Priority. *Work*, 10(4), 108–113.
- [25] Torabi, S. A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, 89, 201–218. <https://doi.org/10.1016/j.ssci.2016.06.015>.
- [26] S. Parsana, T., & T. Patel, M. (2014). A Case Study: A Process FMEA Tool to Enhance Quality and Efficiency of Manufacturing Industry. *Bonfring International Journal of Industrial Engineering and Management Science*, 4(3), 145–152. <https://doi.org/10.9756/BIJEMS.10350>.
- [27] Sprcic, D. M., Pecina, E., & Orsag, S. (2017). Enterprise Risk Management Practices in Listed Croatian Companies. *UTMS Journal of Economics*, 8(3), 219–230.
- [28] Cervone, H. F. (2009). Using Pugh matrix analysis in complex decision-making situations. *OCLC Systems & Services*, 25(2), 76–81. <https://doi.org/10.1108/10650750910961875>