Heliyon 6 (2020) e03161

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Research article

The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment

Apol Pribadi Subriadi, Nina Fadilah Najwa *

Department of Information Systems, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia

ARTICLE INFO

Keywords:
Systems engineering
Safety engineering
Information security
Information systems
Information systems management
Information technology
Information management
FMEA improvement
FMEA consistency
IT risk

ABSTRACT

FMEA is as a method for assessing IT risks. This research aimed to examine the consistency of both traditional FMEA and improved FMEA in IT risk assessment. Improved FMEA is the result of a synthesis framework to minimize consistency in traditional FMEA. Two sets of action research cycles (plan, act, observe, reflect) were applied in this research. Action Research 1 was used to examine and prove the consistency of traditional FMEA. On the other hand, Action Research 2 was applied to examine the consistency of improved FMEA. Tests were carried out by two different teams in the same case study. The consistency was observed in the gap of the RPN results in both teams, and the differences result in both action research cycles. Action Research 1 proved that traditional FMEA was not consistent. The gap in the amount of risk at a very high level was four risks. However, Action research 2 had the same amount of risk at a very high level. Based on the correlation test, the consistency of action research 1 was 0.848 (very large correlation), and the action research 2 was 0.937 (near-perfect correlation). The consistency of improved FMEA proved to be more consistent than traditional FMEA. The limitation of this study was memory issues because both action research cycles were carried out by the same team and with similar case studies. Further research is expected to compare traditional FMEA and improved FMEA in different case studies. The theoretical contribution was the improved FMEA synthesis based on limitations of traditional FMEA. The FMEA team may use Improved FMEA Framework.

1. Introduction

Every organization has to maintain its information security from Information Technology (IT) risks. The Information security aspect comprises confidentiality, integrity, and availability (Whitman and Mattord, 2012). IT risk are related to threats and hazards due to extensive use of IT. Moreover, IT risk can cause unexpected damage and loss (Spremic and Popovic, 2008). Risk affect the organization in both financial and non-financial aspects.

IT risks can be measured by various methods: quantitative, qualitative, and semi-quantitative. Methods that are purely qualitative and descriptive tend to produce a more subjective risk assessment. In addition, a quantitative method can eliminate a lot of information and is time-consuming as well as complicated to describe the risks in an organization (Chen, 2015). A semi-quantitative measurement method combines both quantitative and qualitative methods. *Failure Mode and Effect Analysis* (FMEA) is classified as the semi-quantitative method. The Risk Priority Number (RPN) in FMEA supports the quantitative analysis of risk events. This method not only is found the highest risk accurately and quickly but also overcomes the concerns about losing information (Zhao and Bai, 2010). FMEA can evaluate the potential risk critically (Murphy et al., 2011).

FMEA is suitable for assessing IT risk (Najwa and Subriadi, 2018). FMEA provides common structures and languages that can be used in many types of organizations, for example: manufacturing and service industries, profit and non-profit organizations, private and public organizations, and government organizations (McDermott et al., 2009). The difference in measurement using FMEA of IT risks with other FMEAs lies in the risk objects researched. FMEA in IT aspects assesses risks in the information security aspect (confidentiality, integrity, and availability).

FMEA receives many criticisms from several previous studies regarding the consistency of risk assessment. The FMEA weakness points found include difficulties in finding risk potential root causes, evaluating risk factors accurately, defining scale criteria, which are not clear and doubtful, the non-linear 1–10 priority scales, subjectivity/human error, bias, time-consuming, the importance level of parameters which is similar, duplicated RPN duplication, and RPN formulation.

* Corresponding author.
E-mail address: ninafadilahnajwa@gmail.com (N.F. Najwa).

https://doi.org/10.1016/j.heliyon.2020.e03161
Received 10 September 2019; Received in revised form 11 November 2019; Accepted 31 December 2019

The higher the level of organizational dependence on IT, the higher the potential failure and its impact (Najwa and Subriadi, 2018). However, an organization needs proper FMEA and acquires a consistent measurement result. The impact of inconsistent risk assessment results is a critical aspect to be considered by the organization. If FMEA is improperly applied, the organization will perform an incorrect mitigation (Subriadi et al., 2018). This might happen because the high-risk priority requires a higher cost and top priority treatment. On the other hand, the low-risk level requires low budget or can be ignored. The losses that the organization have experienced will be doubled if it was incorrectly measured.

Studies that combine the use of FMEA and information security risks are not that many (Silva et al., 2014). Thus, FMEA in the IT field needs to be explored (Lai and Chin, 2014). This study analyzed the consistency of traditional FMEA and Improved FMEA in IT Risk Assessment. The methodology used was action research (plan, act, observe, reflect), comprising two cycles. Action research 1 examined and proved the traditional FMEA consistency, while action research 2 included a critical analysis, synthesis of improved FMEA, and examination of the improved FMEA consistency. The stages of consistency analysis examined IT risks by two different teams in the same case study. Consistency measurement was based on the results of RPN score from each team. Both action research models presented the comparison of the RPN score from both teams based on the level of risk (very high, high, medium, low and very low). The difference in the amount of risk on each level from the results of both teams indicated that there was an inconsistency issue.

The theoretical contribution of this research is to prove the consistency issue of traditional FMEA in IT risk assessment. This research suggested a model (Improved FMEA) based on literatures and the result of consistency traditional FMEA; then this research also proves the improved FMEA consistency. The result of this research shows the comparison of the consistency of traditional FMEA and improved FMEA. Moreover, the practical contribution this study is to provide the guidance for improved FMEA that can be tested and tried to get more consistent risk measurement results.

2. Literature review

2.1. Failure Mode and Effect Analysis (FMEA)

IT risk management is applied to protect IT assets such as data, hardware, software, personnel, and facility from both whole external threats (i.e., catastrophe) and internal threats (i.e., technical error, sabotage, unauthorized access) (Bandyopadhyay et al., 2011). One method that has been widely used in measuring risks for over 40 years is Failure Mode and Effect Analysis (FMEA). FMEA was generally used by the aviation industry in the midst 1960s and is particularly used in safety or security issues (McDermott et al., 2009). FMEA is growing and can be used in various fields, including Information Technology. The difference in the use of FMEA is based on the risk object to be measured (Lai and Chin, 2014). In addition, the focal point of risk measurement in this research is IT risks. FMEA in the IT field focuses on sensitive data and information security (McDermott et al., 2009). FMEA framework helps managers and technicians to identify potential failure modes, potential causes, and mitigation (Sharma and Sharma, 2010).

FMEA uses Risk Priority Number (RPN) technique as well as linguistic terms to determine the impact of risk (severity), the possibility of risk (occurrence), and risk opportunities (detection). Scale determination does not have a specific procedure, so it can be determined using the customization of the risk team. The most commonly used range of criteria scale is 1–10 scale (van Leeuwen et al., 2009). The RPN value is obtained by multiplying the value of the three parameters. Risks with the highest RPN values are assumed to be important risks and should get high priority handling compared to the risks with low RPN values (Sankar and Prabhu, 2001).

2.2. Related works

The FMEA method applied in risk management bears a consistency issue (Barends et al., 2012; Estorilio and Posso, 2010; Gary Teng et al., 2006; Oldenhof et al., 2011). A research conducted by (Lai and Chin, 2014) proposed Information Security FMEA Circle that modified traditional FMEA methodology. Moreover, another research by (Oldenhof et al., 2011) examined the consistency of FMEA by assessing risks in different teams in a case study. The risk analysis steps are identification of the potential cause, severity, and risk detection in each critical asset. This research proves that the implementation of traditional FMEA is not consistent. Therefore, the result of the research is guidance to examine the consistency of traditional FMEA and Improved FMEA.

A research conducted by (Estorilio and Posso, 2010) criticized the FMEA consistency by fixing each step in FMEA methodology. There are seven factors affecting the irregularity (FMEA Consistency) in the FMEA: knowledge, training, failure history, teamwork and synergy, time requirement, and control. This study provides guidance in synthesizing the improved FMEA framework, which is also supported by the results of a gap analysis of the methodology used by (Oldenhof et al., 2011).

The uncertainty of the RPN value can be analyzed from the uncertainty of risk assessment in each of these parameters: severity, occurrence, and detection (Cameron et al., 2017). The weakness of the RPN is that it did not consider the relative importance of the parameters, there was the duplicate RPN with the different combination, and the underlying risk implications could also be different, it was not easy to assess accurately, and the RPN formula could evaluate (Chai et al., 2016). The FMEA weakness because of the large variety of combinations, so it could cause the duplication of RPN value. Duplicate RPN that had a low or high-risk impact had the same importance level to be targeted for risk mitigation (Banghart, 2014).

The new hybrid FMEA Model, which combines Fuzzy Preference Programming (FPP), Fuzzy Cognitive Maps (FCMs), and Fuzzy Graph-Theoretical Matrix Approach (GTMA), was proposed by (Baykasoğlu and Gölcük, 2017). This research purpose was to help the drawbacks of traditional FMEA and RPN. FPP was used to get the rank of risk causes from incomplete, improper, and reciprocal assessment comparisons. FCMs were to capture the causal dependencies among risk. Then, fuzzy GTMA was to assess the risk priority of failure modes by relating the interaction between risk causes. The limitation of this study was too quantitative, so the detail process and the risk analysis on cases were inadequate. In addition, the results of this study were dependent on the expert's point of view.

According to the results of the literature review conducted by (Liu et al., 2013), FMEA's weakness lies in not having weight values because it has the same important level in each parameter. Previous researches combined Fuzzy and FMEA methods in risk assessment. FMEA is combined with Fuzzy method to overcome the weaknesses of FMEA in the same level problem in each parameter (Liu et al., 2013). Those weaknesses are: (1) it was difficult to define functions that were relevant to risk factors because the language or terms were difficult to understand easily; (2) it required a high cost and long time-consuming in applying fuzzy; (3) a complex calculation by considering a lot of information loss in the risk analysis process. The fuzzy implementation is, in fact, still difficult and required a long time in the risk analysis process.

The number of studies that combines FMEA and information security risks is still limited (Silva et al., 2014). The use of FMEA in the IT field still needs to be explored (Lai and Chin, 2014). The consistency of traditional FMEA in the IT field has been proved by (Subriadi et al., 2018). The results of this study prove the inconsistency problem of traditional FMEA. The final result of this research presented the synthesis FMEA framework based on the case study. However, the research had not yet reached the empirical testing phase and proved the consistency of the synthesis FMEA.

The difference between this research and the others is that this research explored FMEA in the IT field and testing traditional FMEA

consistency issues in accordance with previous researches criticisms. Unlike traditional FMEA consistency testing conducted by (Oldenhof et al., 2011), who conducted risk assessment in the chemistry industry field, this research assessed the IT Risk. This research also provided recommendation solutions based on FMEA weaknesses by developing an improvement framework to improve FMEA. The improved FMEA consistency was tested in the same way as the traditional FMEA consistency methodology. Therefore, it could be seen that the reliability of improved FMEA was more consistent and better than traditional FMEA.

3. Methodology

3.1. Research question and research object

The purpose of this research was to prove the consistency of traditional FMEA and improvedFMEA. FMEA documents used by both teams as instruments for measuring IT risk were similar. The FMEA consistency was observed based on differences in the RPN value obtained. Based on the gap that became the background of research, the research questions are (1) How is the consistency resulted using Traditional FMEA?; (2) What is the result of synthesis FMEA framework to overcome the consistency Traditional FMEA?; (3) How empirical are the results of the Improved FMEA framework synthesis?

The first question was answered by testing the Traditional FMEA framework on two different teams in the same case study (Action Research 1) (Subriadi et al., 2018). The second question was answered by aligning the identified FMEA weakness points, diagnosing the causes, and providing the recommendation for solutions. The result of the alignment was improved FMEA, which was an improved model of traditional FMEA. The third question was answered by testing the Improved FMEA framework on two different teams in the same case study (Action Research 2).

The research object was a ministry of the government in Indonesia that has critical information technology assets. The use of IT in the ministry's government was used to improve performance and service to the citizen.

3.2. Action research cycles

This study was conducted by two action research cycles (Hall and Coats, 2005; Rose et al., 2015). Action Research 1 was to examine the traditional FMEA consistency, and Action Research 2 was to examine the improved FMEA consistency as a recommendation for solutions. There were two teams of FMEA, each comprising three members. The FMEA team was the combination of a section chief, a senior employee, two IT practitioners, and a researcher as the coordinator of FMEA team.

3.3. Action research 1

Action Research 1 had 4 stages. The explanation is as follow:

- *Plan.* Planning was done by designing traditional FMEA risk assessment scenarios, which was conducted by two different teams. The design of a risk assessment scenario consisted of identifying business processes and building an asset-based threat profile, and identifying infrastructure vulnerabilities by following the methodology of Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Alberts and Dorofee, 2002). Scenario analysis in IT risk analysis is by identifying IT risk, making a risk assessment by two teams, prioritizing risks, and comparing the result (gap analysis) (Oldenhof et al., 2011).
- *Act.* Implementating the research scenario with team FMEA.
- *Observe.* Collecting the data during the implementation of the research scenario.
- *Reflect.* Analyzing the gap as the input for the next action research (improved FMEA synthesis).

3.4. Action research 2

Action research 2 had 4 stages. The explanation is as follows:

- *Plan.* The research scenario plan was to synthesize and test improved FMEA. This stage was also included in the scenario to get the conclusion regarding the comparison between the results of traditional FMEA and improved FMEA. The phases of the FMEA framework synthesis followed the methodology developed by (Estorilio and Posso, 2010):
  a) *Critical analysis in each identified process.* The results of this stage are FMEA weaknesses that need to be considered in the FMEA process. Critical analysis was done based on FMEA documents.
  b) *Diagnose the possible caused.* A literature study was conducted regarding the possible causes of these weaknesses. The results of the gap analysis would be an additional reference to strengthen the diagnosis of the causes of these weaknesses.
  c) *Recommendation solution.* Improvements were made by aligning weaknesses identified, possible cause diagnosed, and recommendation solution in accordance with previous research.
  d) *Validation.* At the initial stage, validation and verification of traditional FMEA documents were done by two IT practitioners, then validation of Improved FMEA was done by experts in the field of risk management who already had certification.
- *Act* Implementing what was based on the research scenario.
- *Observe.* Collecting the data during the implementation of the research scenario.
- *Reflect.* Analyzing the result differences obtained from the two teams. This stage was the conclusion from the two action research cycles that have been implemented.

3.5. Traditional FMEA research framework

This research used traditional FMEA framework for Action Research 1. Traditional FMEA comprises five general stages, namely identifying potential failures and impacts, determining severity, determining the frequency of occurrence, detecting failures, and calculating RPN values (Software, 2016; Stamatis, 2003). These general stages are explained in more detail in Figure 1 (McDermott et al., 2009).

The FMEA method is a general framework that can be used to measure various risk objects. This research used the OCTAVE method to identify IT risks. The OCTAVE method was able to define IT risks associated with critical assets in the organization (Alberts and Dorofee, 2002). The initial stage was to identify the business processes and related products (critical assets) with the OCTAVE method. The OCTAVE stage was to build an asset-based threat profile and identify infrastructure vulnerabilities. Brainstorming the failure (risk identification) using the FMEA and OCTAVE methods were aimed to determine the failure that could occur. Stages of risk identification were carried out by identifying threats, vulnerabilities, and attacks (Lai and Chin, 2014). The risk identification result was the FMEA document, which contained a risk register accompanied by an impact and a potential cause. The FMEA document used as a reference was the American Society for Quality (ASQ), which was adapted to ISO 27001(Security, 2008; Stamatis, 2003).

Risk assessment was based on the severity, occurrence, and detection values carried out by the FMEA team. The scale used was the 1–10 scale as the most commonly used. The next step was to calculate and to prioritize the highest urgency risk. Prioritizing risk assessment was based on risk level (very high (VH), high (H), medium (M), low (L), and very low (VL)). The risk level is a reference for the elimination or reduction of the high risk of failure mode. The next step was to calculate the RPN value as reduction or elimination failure modes using Eq. (1). However, this research focuses on the consistency of FMEA as a risk assessment method.

$$RPN = severity\ x\ detection\ x\ occurrence \quad (1)$$

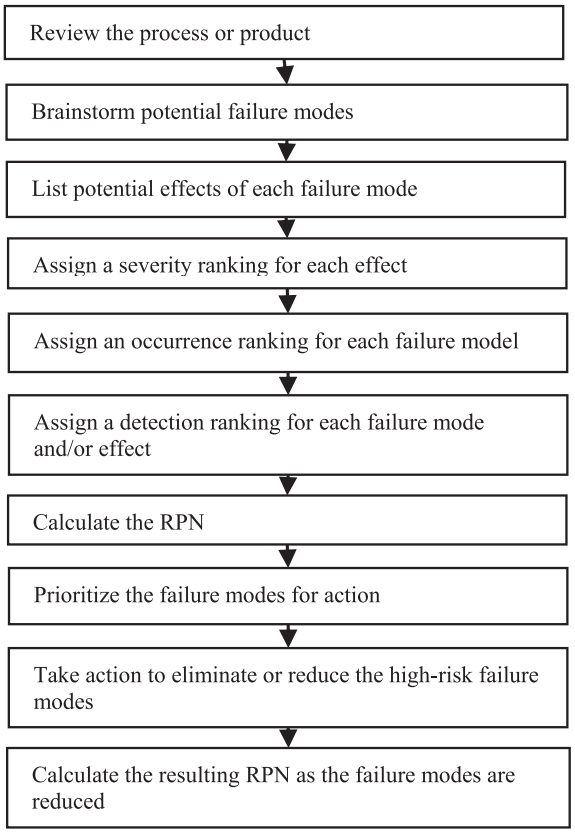

Figure 1. Traditional FMEA.

4. Result and discussion

4.1. Action research 1 (AC1)

4.1.1. Traditional FMEA consistency results

Risk identification results obtained 37 risk registers that have been adapted to the traditional FMEA framework. The research results on the Action Research 1 cycle found that there were differences in RPN between the two teams (Figure 2). Based on the risk assessment by both teams, significant differences in the value of each parameter occurred at the detection, severity, and occurrence. RPN results at a very high level in Team 1 were 3 risks, while 7 risks registered by the Team 2. At the top three, both teams had similarities in defining risk. The other differences were based on the dynamics of giving risk scale for each parameter.

The difference in assigning risk scale to the same type of risk indicated a consistency issue. In the severity parameter (Figure 3), there were some differences, which were a big gap from risk assessment between two teams. At the HW02 Risk ID, Team 1's severity risk scale was 6, while Team 2's was 1. At the HW10 Risk ID, Team 1 determined 7 for severity risk scale, while Team 2 determined 1 for severity risk scale.

The difference in assessing severity scale certainly had a significant effect on the results of risk prioritization. The level of importance of each parameter (severity, occurrence, and detection) was identical (linear). Therefore, if it was multiplied by other values, it would greatly affect the amount of RPN obtained.

The difference in risk assessment between the two teams in the occurrence parameter was not significant (Figure 4). This proved that both teams understood the risk events that occurred in their environment well. The risks in an organization's environment could be predicted based on the level of occurrence by defining a time span scale.

The detection parameter had the highest level of difference compared to other parameters (Figure 5). As one example of the risk with the HW01

Team 1								Team2							
Code	*Event Risk*	*Potential Cause(s) of Failure*	*SEV*	*OCC*	*DET*	*RPN*	*Risk Level*	*Code*	*Event Risk*	*Potential Cause(s) of Failure*	*SEV*	*OCC*	*DET*	*RPN*	*Risk Level*
NT03	Decreased network connectivity	network failure	6	10	10	600	VH	NT03	Decreased network connectivity	network failure	7	10	9	630	VH
HW04	Server down	DDOS attack.	6	9	7	378	VH	HW04	Server down	DDOS attack.	7	9	7	441	VH
NT01	Network disconnect	network failure	6	10	6	360	VH	NT01	Network disconnect	network failure	6	9	7	378	VH
HW05	Server damage	controlling and maintenance are not routine	6	4	6	144	H	DA07	Corrupt Data	network connection is not optimal	9	7	5	315	VH
HW14	network failure	Network infrastructure damage	6	4	6	144	H	HW13	Illegal Information access	access right weak and no passwords	10	10	3	300	VH
HW16	Network device malfunction	Force of nature and animal	6	3	7	126	H	HW16	Network device malfunction	Force of nature and animal	6	7	7	294	VH
HW13	Illegal Information access	The access right is weak and no passwords	10	10	1	100	M	NT02	Network disconnect	network or electricity failure	6	7	6	252	VH
DA03	breaking data/info	sharing password	10	8	1	80	M	HW05	Server damage	controlling and maintenance are not routine	7	4	7	196	H
HW15	network failure	network config manipulation	6	2	6	72	L	DA03	breaking data/info	sharing password	10	9	2	180	H
HW06	Server damage	Force of nature	2	4	8	64	L	DA05	Lost Data	Software and network failure	9	4	3	108	M
HW02	Server burned	Power failure	6	1	10	60	L	HW14	network failure	Network infrastructure damage	6	4	3	72	L
HW03	Server overheat	AC is not working	3	4	5	60	L	DA02	unconfidentiality data	Misuse of access	10	2	3	60	L
HW08	Computer damage	Computer config error	6	2	5	60	L	DA06	Cybercrime (hacker attack)	firewall security	10	3	2	60	L
DA04	Data invalid	Human error (invalid input data)	5	4	3	60	L	DA01	Full Capacity	uncontrol memory capacity	5	5	2	50	L
DA06	Cybercrime (hacker attack)	firewall security	10	2	3	60	L	PP02	Human Failure	Human resource incompetent	4	3	4	48	L
HW18	Printer/scanner damage	controlling and maintenance are not routine	1	6	8	48	L	PP01	Human Failure	Human error (invalid input data) and misuse device	5	3	3	45	L
SW01	Software failure	software out of dates	6	4	2	48	L	SW01	Software failure	software out of dates	5	4	2	40	L
PP01	Human Failure	Human error (invalid input data) and misuse device	4	3	4	48	L	HW18	Printer/scanner damage	*controlling and maintenance are not routine*	1	6	6	36	L
PP02	Human Failure	Human resource incompetent	4	3	4	48	L	HW19	Printer/scanner damage	Force of nature	1	6	6	36	L
SW02	Virus attack	Antivirus is not reliable	6	6	1	36	L	PP03	Fraud or misuse of access rights	There is conflict interest	9	2	2	36	L
NT02	Network disconnect	network or electricity failure	6	6	1	36	L	HW07	Computer damage	Virus attack	7	4	1	28	L
HW01	Server burned	Server overheat	3	1	10	30	L	SW02	Virus attack	Antivirus is not reliable	5	5	1	25	L
DA05	Lost Data	Software and network failure	10	3	1	30	L	DA04	Data invalid	Human error (invalid input data)	4	4	1	16	VL
DA07	Corrupt Data	network connection is not optimal	10	3	1	30	L	NT04	IP Addressing Errors	Human error	4	2	2	16	VL
HW07	Computer damage	Virus attack	7	4	1	28	L	HW03	Server overheat	AC is not working	4	3	1	12	VL
DA01	Full Capacity	uncontrol memory capacity	6	4	1	24	L	HW08	Computer damage	Computer config error	6	2	1	12	VL
DA02	unconfidentiality data	Misuse of access	9	2	1	18	VL	HW15	network failure	network config manipulation	2	2	3	12	VL
HW09	Computer damage	software out of dates	3	1	5	15	VL	HW17	Loss of network device components	Theft	6	2	1	12	VL
HW10	Computer damage	Force of Nature	7	2	1	14	VL	HW09	Computer damage	software out of dates	3	1	3	9	VL
HW17	Loss of network device components	Theft	6	2	1	12	VL	SW03	System failure	Security hole	5	1	1	5	VL
NT04	IP Addressing Errors	Human error	6	2	1	12	VL	HW01	Server burned	Server overheat	4	1	1	4	VL
PP03	Fraud or misuse of access rights	There is conflict interest	8	1	1	8	VL	HW02	Server burned	Power failure	1	1	1	1	VL
SW03	System failure	Security hole	6	1	1	6	VL	HW06	Server damage	Force of nature	1	1	1	1	VL
HW12	Loss PC components	Theft	1	3	1	3	VL	HW10	Computer damage	Force of Nature	1	1	1	1	VL
HW20	Loss printer/scanner	Theft	1	2	1	2	VL	HW11	HW *out of dated*	Technology outdated	1	1	1	1	VL
HW11	HW *out of dated*	Technology outdated	1	1	1	1	VL	HW12	Loss PC components	Theft	1	1	1	1	VL
HW19	Printer/scanner damage	Force of nature	1	1	1	1	VL	HW20	Loss printer/scanner	Theft	1	1	1	1	VL

Figure 2. RPN results of action research 1.

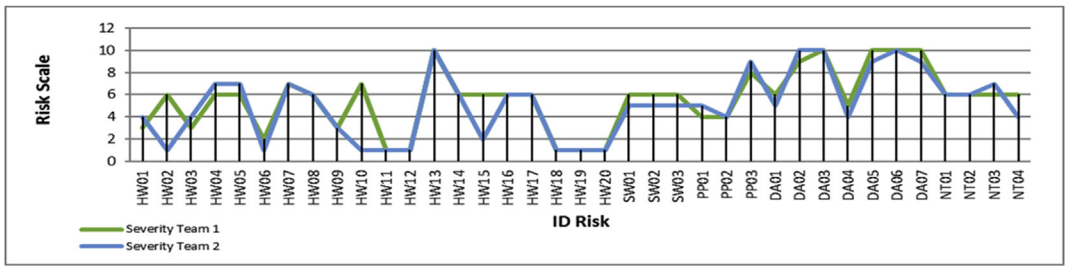

Figure 3. Comparison of risk assessment in Severity parameters (Action Research 1).

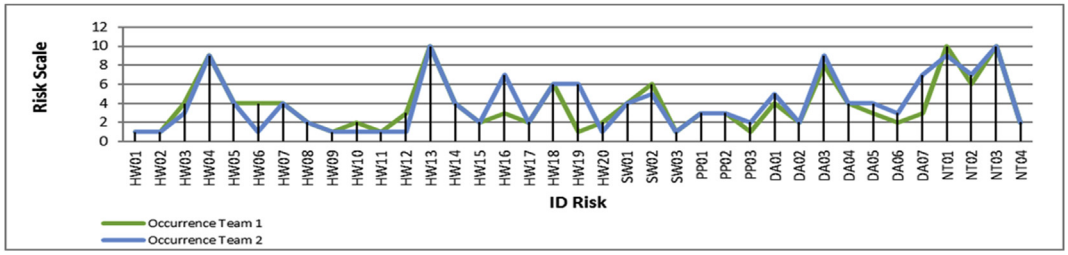

Figure 4. Comparison of risk assessment in Occurrence parameters (Action Research 1).

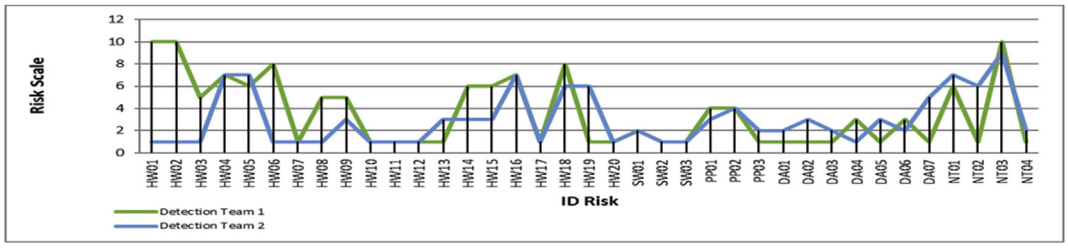

Figure 5. Comparison of risk assessment in Detection parameters (Action Research 1).

and HW 02 Risk IDs, Team 1 determined the detection scale 10, while Team 2 determined detection scale 1. The gap in determining the detection scale by both teams gave a significant difference in the RPN. The consistency of the two teams in assessing the detection parameter was influenced by subjective issues. Subjective issues, that were intended, were only based on experience and knowledge from the informants. Thus, measuring detection parameters required tools such as event monitoring tools. With these tools, teams could provide an assessment in accordance with existing data, and the accuracy of the risk assessment would increase.

4.1.2. Gap analysis of team 1 and team 2

Comparisons were made based on the parameters of differences or factors that had been stated in (Estorilio and Posso, 2010). There are several factors that affect the FMEA irregularity in risk assessment, including in terms of knowledge, risk assessment team, training, failure history, and completion time (Table 1). This research also added a comparison of the parameter scales.

Gap analysis can be defined by determining the difference between current knowledge or practice (current practice) with evidence of best practice (Janneti, 2012). Gaps can occur in the scope of knowledge,

Table 1. Gap analysis.

Factors	The Difference*(Current Practice)*	*What is Best Practice?*
Parameters scale	The gap sequence of the IT risk measurement parameters was detection, severity, and occurrence.	The parameters scale could be limited to save time in assessing risk. It was also more effective in getting reliable measurement results. (Paciarotti, Mazzuto, & D'Ettorre, 2014)
People (FMEA Team)	Each action research assesses by two teams. The team 1 consisted of IT Practitioner, Section Chief, and Coordinators. The team 2 consisted of IT Practitioner, senior employees (operator), and coordinator.	This matter was already suitable for the results of research conducted by (Oldenhof et al., 2011).
Time Completion	The team 1 took a long time to measure risk compared to the team 2.	Risk assessment required estimated time and job division. (McDermott et al., 2009). The risk assessment should be less than 90 min (Estorilio and Posso, 2010).
Training	Each team has got an explanation of how to use the FMEA method. The informant also attends the training which is held once a year.	Provide training on the use of the FMEA method to measure IT risk to the FMEA team (Estorilio and Posso, 2010). All members should know about the IT aspect in the organizations.
Knowledge	The case study had never been to assess an IT risk. The informant's educational background was not from the IT field.	
Failure History	The failure history factor was based on the informant's experience and knowledge.	

skills, or practical. A gap analysis is a technique that can help identifying the current situation with the conditions achieved by completing the gap. Gaps can be complemented with several solutions for existing differences as required or intended conditions. In this case, the gap analysis was the input to continue the cycle of Action Research 2.

4.2. Action research 2 (AC2)

4.2.1. Improved FMEA (planning stages)

Improved FMEA is synthesis based on the literature review according to the weaknesses of traditional FMEA. Improvements were made by aligning the weaknesses, diagnosing of causes, and providing recommendation solution (Table 2). The critical analysis results in the FMEA weakness points for each step of the FMEA process. The FMEA weakness points found are in the form of the difficulties in finding risk potential root causes, difficulties in evaluating risk factor accurately, definition of scale criteria that was not clear and doubtful, non-linear 1–10 priority scales, subjectivity/human error, bias, time-consuming, similar importance level of the parameters, duplicated RPN, and RPN formulation.

The solution recommendations in Table 2 became a reference in synthesizing the improved FMEA model. Improved FMEA in Figure 6 had more detailed stages and included strategies that could minimize the traditional FMEA weaknesses. The Improved FMEA Model consisted of four main stages (determination of risk assessment requirements, risk identification, risk analysis, and evaluation, and recommendation control documentation).

- Identify Context
  This stage determined the risk assessment scope. The target system described and asset identification(Lai and Chin, 2014). The determination of critical assets was categorized based on hardware, software, people, data, and network (Alberts and Dorofee, 2002).
- Identify Business Process
  Business process analysis was carried out to understand the current system performance (McDermott et al., 2009).
- Establish FMEA Team

This stage determined the parties involved in the risk assessment. The following was the procedure for establishing the FMEA team:

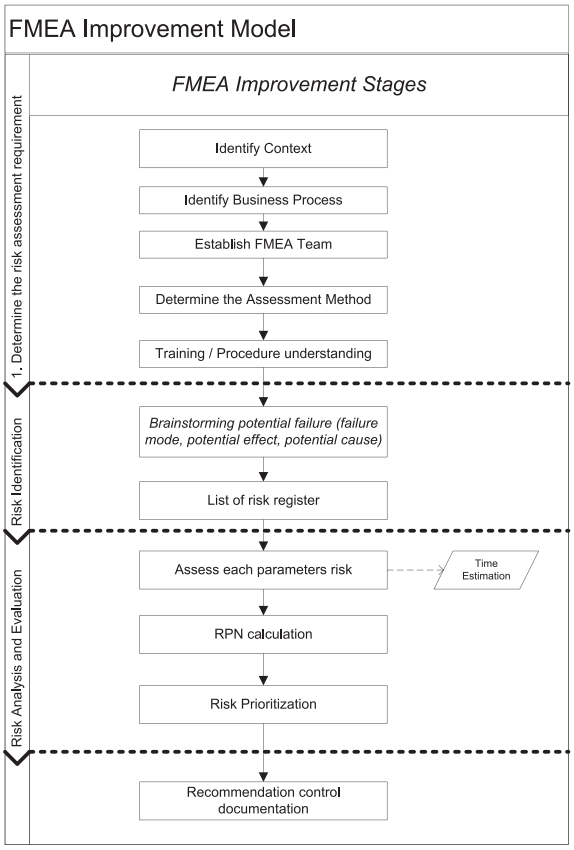

Figure 6. Improved FMEA model.

a Team Size: The number of odd teams helped and facilitated the voting calculation process. A minimum number was 3 people in a team(-Alberts and Dorofee, 2002).

b Team Member: There were at least two expert technicians in the FMEA team to balance significant individual differences in crucial risk decisions (Oldenhof et al., 2011). Each team consists of

Table 2. Alignment of weaknesses, causes, and recommendations.

Weakness	Diagnose the possible caused	Recommendation Solution
The difficulties in finding risk potential root causes	Defining sources of threats that were not appropriate (Cameron et al., 2017; Liu et al., 2013).	Source of threat categories in the risk register (Cameron et al., 2017).
The difficulties in evaluating risk factor accurately	The many variations of scenarios that affect the identical RPN results. (Sawhney et al., 2010)	
Definition of scale criteria was not clear and doubtful	There was no specific procedure for determining the criteria scale (van Leeuwen et al., 2009).	Reduction of the range of the parameter variable (Scale) (Paciarotti et al., 2014). They have categorized the scale of severity risk into 3 risk types, namely service/operational, media attention, and regulation.
The non-linear 1–10 priority scales	The team needs to think longer in determining the right scale because of the many considerations of the right numbers in the 1–10 scale. (Paciarotti et al., 2014; Sankar and Prabhu, 2001).	
Subjectivity/human error, Bias	There was no guidance about team FMEA (Raspotnig and Opdahl, 2013). Knowledge and experience (Banghart, 2014; Gary Teng et al., 2006).	Procedure for establishing a FMEA team (Alberts and Dorofee, 2002; Jain, 2017; McDermott et al., 2009; Oldenhof et al., 2011), Training related to FMEA methods and introduction to IT risks (Estorilio and Posso, 2010).
Time-consuming	There was no time limit on the IT risk assessment (Jain, 2017).	estimated time and division of tasks (McDermott et al., 2009). No more than 90 min (Estorilio and Posso, 2010).
The importance level of parameters was the same	There was no value variable, which was the main key that might be used in the analysis (Liu et al., 2013; Xiao et al., 2011).	Severity and occurrence values were the main keys that might be used in the analysis compared to detection (D) parameters (Xiao et al., 2011).
The RPN formulation	The formula was too simple because it considered the same level of importance. (Sankar and Prabhu, 2001)	
Duplicated/Identic RPN	A large number of variations in RPN values (max = 1000). (Banghart, 2014)	Reduction the range of the parameter variable (Scale) (Paciarotti et al., 2014)

Table 3. Improved FMEA document.

Code	Critical Assets	(impact) Potential Failure Modes (s)	Potential Effect(s) of Failure	SEV	(threat) Potential Cause(s)/ Mechanism (s) of Failure	Source of Threat	OCC	Current Compensanting Controls (Compensate Vulnerability)		RPN
								Preventive Control	Detective Control	
<asset code>	<asset name>	<final impact of failure/risk>	Severity of service/operational, media attention, regulation		Threat	*<people, process, technology>*		Prevention	*Monitoring*	

Significance of italics denotes that the team would choose one of these option (people, process or procedure).

multidisciplinary members so that the team can understand the process analyzed well (Jain, 2017). Other criteria that need to be considered were (Alberts and Dorofee, 2002): (1) people who knew the types of information related to assets in the organization, (2) people who knew how to get this information, (3) people who were committed to making time for risk measurement.

c Team Coordinator: A team coordinator should control and coordinate the risk assessment process. The tasks of the coordinator team were (McDermott et al., 2009): (1) organizing and facilitating meetings including FMEA schedules and documents to be filled out, (2) ensuring that the team concerned was present, (3) ensuring the success of risk assessment until completion.

- Determine Assessment Model

This stage determined the design of FMEA documents along with the criteria scale used in risk assessment(Carlson, 2014). Following were the modifications made for the assessment method:

a Added the source of threat categorization (*people, process,* and *technology*) in the risk register. Looked for the root cause that was rarely seen in a system component (Cameron et al., 2017). The source of threat categorization could minimize ambiguity in understanding failure.

b Removed the detection variable in risk assessment. The justifications for the removal of detection variables were:

1) Severity and occurrence values were the main keys that might be used in the analysis compared to detection (D) parameters (Xiao et al., 2011).
2) Detecting risk was required tools, while in the case study, there were no detection tools, such as the event monitoring tools. This also reduced the team's effort to apply risk assessment and speed up the risk assessment process.
3) Referring to ISO 31000, the important variables in measuring risk were the probability (occurrence) and consequences (severity).

c In Potential Effect of Failure column, used the criteria scales categorization (operational/service, media attention, and regulation) (Wibowo, 2005).

d Current compensating controls (Compensate Vulnerability) consists of preventive control and detective control(Ramanan, 2008). Table 3 showed an improved FMEA document design.

e Criteria scale of Severity and Occurrence

The severity criteria scale had been customized with risk categorization in potential effect(s) of failure column (Figure 7). Thus, the measurement instrument was in accordance with the intended risk. Occurrence scale criteria were used as an instrument for assessing the frequency of potential failure (Figure 8).

f Risk Level

The risk level was used as a reference to categorize the urgency and the unurgency risk (Figure 9).

- Training/Procedure Understanding

The facilitator explained the detailed steps in analyzing and assessing risk using the FMEA method (Estorilio and Posso, 2010). The training brought together the perceptions and knowledge of team members on the IT risks to be assessed (Carlson, 2014).

- Brainstorming Potential Failure

The initial stage taken to measure risk was the identification of critical assets by collecting data related to existing conditions. Stages in

Scale	Scale Level	Severity of		
		Service/operational	Media Attention	Regulations
1	Insignificant	No Impact	No Impact	No Impact
2	Minor	An impact can be ignored	Potential is in the public spotlight	Attempt to access the system
3	Moderate	Operational activities or performance are hampered	Negative reporting on the mass media	The operational system is penetrated by hackers
4	Major	Services are interrupted for more than 24 hours.	Main exposure (in mass media) more than a day	An investigation by the authorities or regulator.
5	Fatal	Meaningful inconvenience or anxiety.	Become the government's attention or lose public trust	Overall system failure or total system malfunction.

Figure 7. Severity scale criteria.

Scale	Scale Level	Occurrence
1	Rare	Can be ignored
2	Unlikely	It's less likely to occur
3	Often	Possibilities are happening or can occur
4	Likely	Most likely
5	Expected	Will occur (in all situations)

Figure 8. Occurrence scale criteria.

Inherent Risk		Risk Level	Action Plan
1-5	Very low	Accepted	-
6-10	Low	Accepted	-
11-15	Medium	Accepted	-
16-20	High	Unaccepted	Eliminated, mitigated, transferred
21-25	Very High	Unaccepted	Eliminated, mitigated, transferred

Figure 9. Risk level.

identifying existing conditions were by building an asset-based threat profile. After that, identify infrastructure vulnerability(Alberts and Dorofee, 2002).

- List of Risk Register

The results of potential failure brainstorming obtained in the previous stages were included in the FMEA document, in which its format has been provided. Thus, a risk register was ready to be used at the next stage.

- Assess Each Parameters Risk

The parameters used were severity and occurrence. The assessment referred to the design of FMEA documents that have been compiled, and the assessment time was not more than 90 min (Estorilio and Posso, 2010).

- RPN Calculation. The calculation of RPN in improved FMEA used Eq. (2).

$$RPN = severity \times occurance \quad (2)$$

- Risk Prioritization

This stage sorted the RPN value from the largest to the smallest and determined the risk level. This risk level determined the risk that could be ignored or accepted, eliminated the source of the threat, mitigated risk, or monitored the source of the threat.

- Recommendation Control Documentation

This stage was documentation for risk evaluation on the sustainability of risk assessments that have carried out control recommendations.

4.2.2. Validation

The validation of traditional FMEA documents was performed by two IT practitioners, and then the validation of improved FMEA documents was performed by experts in the field of risk management. Figure 10 shows the validation results for each modification stage in FMEA (improved FMEA).

4.2.3. Improved FMEA consistency results

A risk assessment by improved FMEA that used by both teams lasted less than 90 min. The team 1 completed the risk assessment within 40 min, while the team 2 within 30 min. This means that weaknesses related to time-consuming in the risk assessment process had been minimized. The shorter evaluation times also had an impact on minimizing subjective and bias issues. The longer evaluation time made the FMEA team following emotions and feelings in risk assessment (Estorilio and Posso, 2010; McDermott et al., 2009).

Both teams produced RPN values that could be considered consistent (Figure 11). Both of teams obtained the highest RPN amount 25 with an ID risk of 'NT03'. NT03 was the ID risk for network connectivity risk that decreased due to network failure. This risk classified as serious because it often happened almost every day, and employees feel uncomfortable with the situation. The team 1 categorized two risks in the medium to the high level, three risks in medium level, 13 risks in low to medium level, and 18 risks at a low level. The team 2 categorized three risks in the medium to the high level, two risks in medium level, 9 risks in low to medium level, and 22 risks at a low level.

The other difference was based on the dynamics of the answers in each parameter. In Figure 12, it could be seen that both teams had a small difference of severity parameters in some risks. In Figure 13, it could be seen that both teams were not too different from assessing the occurrence parameter compared to the severity parameter. Risk assessment of severity parameters had many different than the occurrence parameter.

The similarity of severity assessment was more similar in the action research 2 than the action research 1. The difference in the severity parameters of the action research 2 that occurred at some risk was not in too long gaps. This was also influenced by the scale range, where it was 1–5 scales. The action research 1 used a 1–10 scale. The difference in the occurrence parameters of both teams in the action research 2 did not

Stages	Sub-Stage	Description	Status
Determine the risk assessment requirement	Identify Context	System object and asset identifications.	*Valid*
	Identify Business Process	The understanding of business process flow.	*Valid*
	Establish FMEA Team	Determine the FMEA team member.	*Valid*
	Determine Assessment Model	Used the criteria scale and document of Improved FMEA.	*Valid*
	Training/Procedure Understanding	Training and explanation about Improved FMEA procedure.	*Valid*
Risk identification	Brainstorming Potential Failure	Used the OCTAVE methodology (identify critical assets, build an asset-based threat profile and identify infrastructure vulnerabilities)	*Valid*
	List of Risk Register	Synthesis of the brainstorming result in the Improved FMEA document.	*Valid*
Risk Analysis and evaluation	Assess Each Parameters Risk (control: time estimation <90 minutes)	Add value to each parameter (occurrence and severity) with a 1-5 scale.	*Valid*
	RPN calculation	Calculation of the RPN.	*Valid*
	Risk Prioritization	Sort the largest to smallest RPN values the categorize the RPN based on risk level.	*Valid*
Recommendation control and documentation	Recommendation control and documentations.	The risks that will be evaluated and mitigated are incorporated into the control recommendation documentation.	*Valid*

Figure 10. Validation improved FMEA.

Team 1							Team2						
Code	*Event Risk*	*Potential Cause(s) of Failure*	*SEV*	*OCC*	*RPN*	*Risk Level*	*Code*	*Event Risk*	*Potential Cause(s) of Failure*	*SEV*	*OCC*	*RPN*	*Risk Level*
NT03	Decreased network connectivity	network failure	5	5	25	VH	NT03	Decreased network connectivity	network failure	5	5	25	VH
DA07	Corrupt Data	network connection is not optimal	5	4	20	H	HW04	Server down	DDOS attack.	4	4	16	H
NT01	Network disconnect	network failure	4	4	16	H	DA07	Corrupt Data	network connection is not optimal	4	4	16	H
DA03	breaking data/info	sharing password	3	4	12	M	NT01	Network disconnect	network failure	4	4	16	H
HW04	Server down	DDOS attack.	3	4	12	M	DA03	breaking data/info	sharing password	5	3	15	M
SW02	Virus attack	Antivirus is not reliable	3	4	12	M	SW02	Virus attack	Antivirus is not reliable	3	5	15	M
PP03	Fraud or misuse of access rights	There is a conflict interest	5	2	10	L	HW13	Illegal Information access	The access right is weak and no passwords	3	3	9	L
DA02	unconfidentiality data	Misuse of access	5	2	10	L	PP01	Human Failure	Human error (invalid input data) and misuse device	3	3	9	L
PP01	Human Failure	Human error (invalid input data) and misuse device	3	3	9	L	HW12	Loss PC components	Theft	4	2	8	L
PP02	Human Failure	Human resource incompetent	3	3	9	L	HW14	network failure	Network infrastructure damage	4	2	8	L
HW12	Loss PC components	Theft	4	2	8	L	DA02	unconfidentiality data	Misuse of access	4	2	8	L
HW17	Loss of network device components	Theft	4	2	8	L	HW17	Loss of network device components	Theft	4	2	8	L
HW01	Server burned	Server overheat	4	2	8	L	HW09	Computer damage	software out of dates	3	2	6	L
HW13	Illegal Information access	The access right is weak and no passwords	2	3	6	L	PP02	Human Failure	Human resource incompetent	2	3	6	L
HW14	network failure	Network infrastructure damage	3	2	6	L	PP03	Fraud or misuse of access rights	There is a conflict interest	3	2	6	L
SW01	Software failure	software out of dates	2	3	6	L	HW02	Server burned	Power failure	4	1	4	VL
HW08	Computer damage	Computer config error	3	2	6	L	HW07	Computer damage	Virus attack	2	2	4	VL
HW09	Computer damage	software out of dates	3	2	6	L	SW01	Software failure	software out of dates	1	4	4	VL
HW15	network failure	network config manipulation	3	2	6	L	HW08	Computer damage	Computer config error	3	1	3	VL
HW03	Server overheat	AC is not working	2	2	4	VL	HW15	network failure	network config manipulation	3	1	3	VL
HW05	Server damage	controlling and maintenance are not routine	2	2	4	VL	HW01	Server burned	Server overheat	1	2	2	VL
DA04	Data invalid	Human error (invalid input data)	2	2	4	VL	HW03	Server overheat	AC is not working	1	2	2	VL
HW02	Server burned	Power failure	4	1	4	VL	HW05	Server damage	controlling and maintenance are not routine	2	1	2	VL
HW07	Computer damage	Virus attack	1	3	3	VL	DA04	Data invalid	Human error (invalid input data)	2	1	2	VL
HW10	Computer damage	Force of Nature	2	1	2	VL	HW06	Server damage	Force of nature	1	1	1	VL
HW20	Loss printer/scanner	Theft	1	2	2	VL	HW10	Computer damage	Force of Nature	1	1	1	VL
DA01	Full Capacity	uncontrol memory capacity	2	1	2	VL	HW11	HW out of dated	Technology outdated	1	1	1	VL
NT02	Network disconnect	network or electricity failure	2	1	2	VL	HW16	Network device malfunction	Force of nature and animal	1	1	1	VL
HW19	Printer/scanner damage	Force of nature	1	1	1	VL	DA01	Full Capacity	uncontrol memory capacity	1	1	1	VL
SW03	System failure	Security hole	1	1	1	VL	DA05	Lost Data	Software and network failure	1	1	1	VL
DA05	Lost Data	Software and network failure	1	1	1	VL	DA06	Cybercrime (hacker attack)	firewall security	1	1	1	VL
HW06	Server damage	Force of nature	1	1	1	VL	HW18	Printer/scanner damage	controlling and maintenance are not routine	1	1	1	VL
HW11	HW out of dated	Technology outdated	1	1	1	VL	HW19	Printer/scanner damage	Force of nature	1	1	1	VL
HW16	Network device malfunction	Force of nature and animal	1	1	1	VL	HW20	Loss printer/scanner	Theft	1	1	1	VL
DA06	Cybercrime (hacker attack)	firewall security	1	1	1	VL	NT02	Network disconnect	network or electricity failure	1	1	1	VL
NT04	IP Addressing Errors	Human error	1	1	1	VL	NT04	IP Addressing Errors	Human error	1	1	1	VL
HW18	Printer/scanner damage	controlling and maintenance are not routine	1	1	1	VL	SW03	System failure	Security hole	1	1	1	VL

Figure 11. RPN results of action research 2.

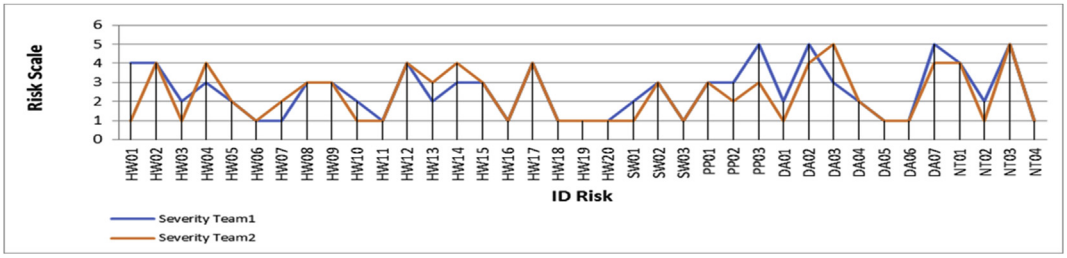

Figure 12. Comparison of risk assessment in Severity parameters (Action Research 2).

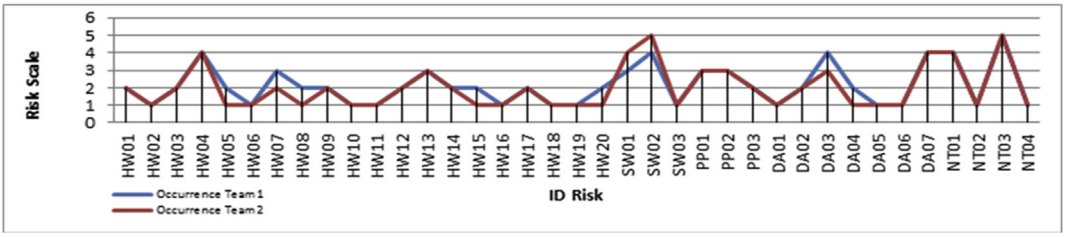

Figure 13. Comparison of risk assessment in Occurrence parameters (Action Research 2).

have a big difference compared to action research 1. In both action research cycles, both teams correctly understood the organizational environment so that they could provide the right assessment. The occurrence assessment of both teams has more similiarities compared to other parameters.

Both teams received training related to improved FMEA procedures. This training was very helpful in equating perceptions among team members regarding improved FMEA procedures and regarding the risks involved in the case study. The severity scale had been adjusted to the risks that existed in the organization. The severity level was divided into three categories of impact risk, namely service/operational risk, media attention risk, and regulatory risk. The severity parameters in risk assessment had been suitable with the risk assessment instrument by the categorization of risk. Modification of FMEA documents and criteria scale could minimize the weaknesses of FMEA, namely the difficulty of problem root finding and the difficulty of risk appropriately evaluation.

Traditional FMEA weaknesses related to the importance of parameters had been proved to be minimized by eliminating the detection variable. The main key in risk analysis was severity and occurrence parameters. In the results of the action research 1, the most significant difference in the dynamics of assessment parameters was the detection parameter. The elimination of the detection parameter also reduced the risk assessment time-consuming.

4.3. Comparison between action research 1 and action research 2

Action Research 1 (AC1) proved that traditional FMEA produced inconsistent values. However, Action Research 2 (AC2) proved that the FMEA weaknesses identified could be minimized. AC2 produced a consistent RPN. The comparison of the results of both action research is illustrated in Figure 14. There was a gap between the result of the risk level of AC1 and AC2 in the same team in the single study case.

The sensitivity of AC2 was observed very high, especially at a very high-risk level. The traditional FMEA modification in AC2 considered could minimize the gap between team 1 and team 2. The focus attention on the RPN level was on a very high level. The very high level risk is the risk that has the highest urgency level to be mitigated, eliminated, or prevented.

The gap in AC1 at very high levels was 4 risks. In AC1, team 1 categorized the highest risk with 3 risks, while Team 2 acquired 7. Unlike AC2, both teams had the same number at a very high-risk level. This meant that the sensitivity of changes on this level was high. The improved FMEA framework proved to have a high impact on high-risk levels and provided more consistent results. On a high level, there was no significant gap in both action research cycles. Both action research cycles had a risk gap. Comparisons at the medium level in both action research cycles had no significant gaps. Both action research cycles had a gap value of both teams. Comparison at the low level both action research cycles had a smaller gap. The gap of AC1 was 6, while AC2 was 4. Sensitivity on the low level

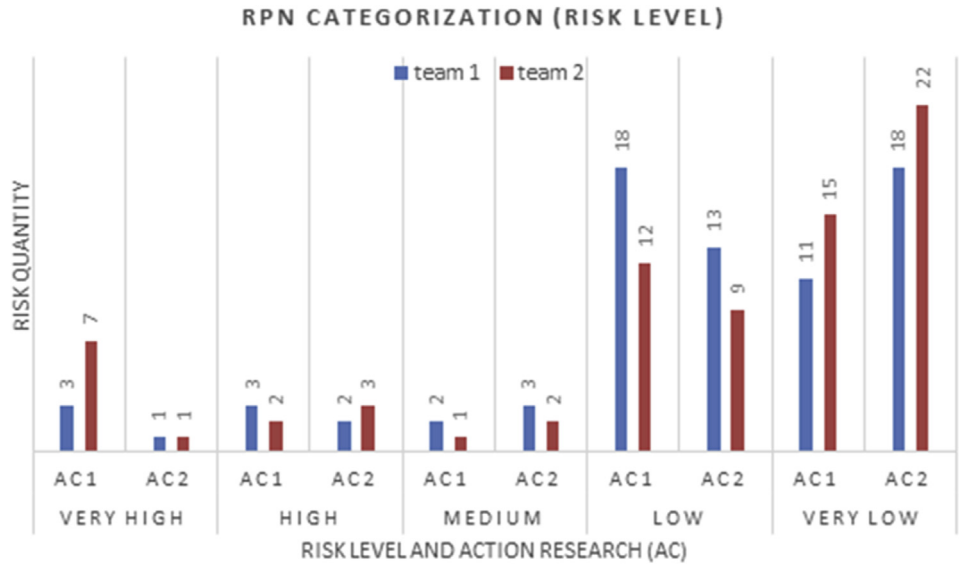

Figure 14. Risk level action research.

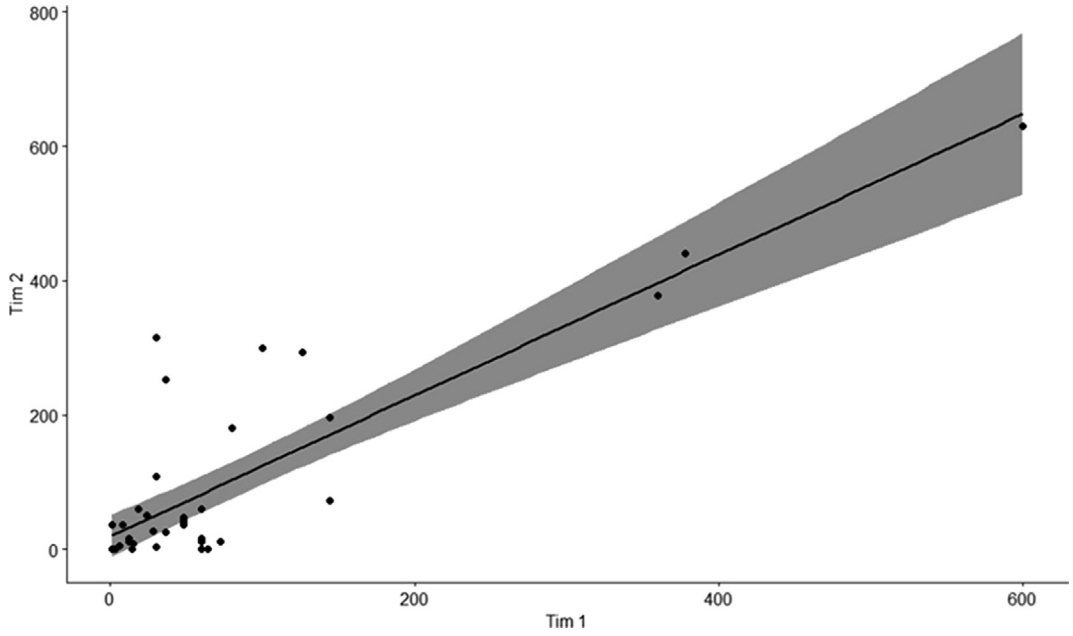

Figure 15. Scatter plot action research 1.

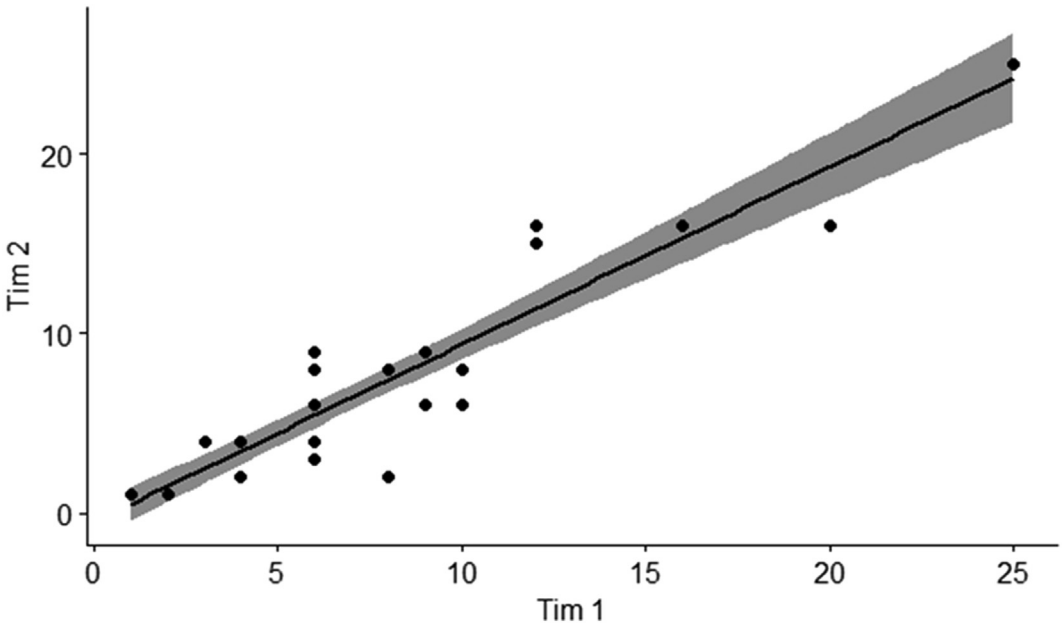

Figure 16. Scatter plot action research 2.

in AC2 was high. At the medium level, there was no significant gap in both action research cycles. The gap value of both research actions was 1.

Correlation analysis is a test tool used to determine how much RPN consistency produced by both cycles. This was related to the order of risk prioritization on each level of risk (VH, H, M, L, and VL). The results of the correlation analysis test using SPPS Inc 2017 were based on the Pearson correlation value. The description of the gap in the RPN scores for both teams is shown in the graph of scattered plots (Figure 15 and Figure 16). Based on a range of correlation level categories (de Vaus, 2002), both action research cycles had not only a significant difference number of risks in risk level categorization but also a different risk order in each risk level categorization. Pearson correlation value in AC1 was 0.848 (very high correlation) whereas, in the AC2 was 0.937 (Near Perfect Correlation). AC1 in the scattered plot diagram in Figure 15 showed that the gap between both teams was immense. The gap was illustrated by the spread of the RPN scores of both teams. The large gray area contained in the scattered plot illustrated the results gained. The results were not consistent. The black dots spread in all directions, whereas some dots away from the diagonal line.

The spread of RPN value by both teams is shown in Figure 16. The scattered plot AC2 diagrams showed that the gap was not too far between the teams. The gray area in the scattered plot of the AC2 was smaller or thinner than the gray area in the scattered plot of AC1. B lack dots in the scattered plot of AC2 were thicker than of AC1. The thickness of the point indicates that the dynamics of the RPN in both teams were almost identical, and the gap was not too big. The distribution of black points was also close to the diagonal line than the scattered plot of AC1. Thus, from the appearance of the two scattered plot diagrams, the level of consistency of improved FMEA was higher (more consistent) compared to traditional FMEA.

In terms of completion time, in AC1, there was no estimated time in the risk assessment, while in AC2; it was given an estimated time fewer than 90 min. In terms of knowledge and understanding of procedures, both action research cycles were given instructions equally on assessment procedures. However, AC2 was more systematic, and the training stages were included in improved FMEA model.

5. Conclusion

Traditional FMEA, based on the results of the action research 1, proved inconsistent. The action research 1 produced a gap analysis as input for the next cycle. The action research 2 was proved that the results of risk assessment with improved FMEA were more consistent. The RPN results obtained by both teams in the second research action were similar. Based on the correlation test conducted, the Action Research 2 consistency was 0.937, which was categorized as a near-perfect correlation. The consistency of the Action Research 1 was 0.848, which was classified as a very high correlation. From these two values, it can be seen that the consistency of improved FMEA proves to be more consistent than traditional FMEA. It can be concluded that the weakness of FMEA can be minimized by applying the improved FMEA model.

Improved FMEA consists of four main stages, namely determination of the risk assessment requirements (context identification, business process identification, team establishment, assessment methods determination, and training), risk identification (brainstorming potential failures, listing risk register), risk analysis, and evaluation (assessing each parameter risk, RPN calculation, risk prioritization, and control recommendations). The synthesized FMEA framework has been validated by experts and tested in a case study. The stages of risk assessment parameters required an estimated time fewer than 90 min. The design of FMEA documents was modified by categorizing the failure effects into three parts, namely the services/operational, media attention, and regulation. The next modification will be the addition of a threat source variable, which consists of three categories, namely people, technology, and processes. The range of scale criteria used was a 1–5 scale. On the severity criteria scale, improved FMEA used a clear parameter based on the type of risk impact category (align with the failure effect). The parameter variables used were the severity and occurrence. The RPN formulation is severity time occurrence. The detection level was not included in the risk assessment but defined on the FMEA documents only (column of Current Compensating Controls).

The limitation of this research is the existence of memory issues because both implementations of action research were carried out in the same case study field. Future studies are expected to be able to test the

comparison of traditional FMEA frameworks and improved FMEA in the same case studies and also in the different divisions or test both frameworks in the different case studies.

Declarations

Author contribution statement

Apol Pribadi Subriadi & Nina Fadilah Najwa: Conceived and designed the experiments; Performed the experiments; Analyzed and interpreted the data; Contributed reagents, materials, analysis tools or data; Wrote the paper.

Funding statement

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Competing interest statement

The authors declare no conflict of interest.

Additional information

No additional information is available for this paper.

References

Alberts, C., Dorofee, A., 2002. Managing Information Security Risks : the OCTAVE Approach. Addison Wesley.
Bandyopadhyay, K., Mykytyn, P.P., Mykytyn, K., 2011. A framework for integrated risk management in information technology. Manag. Decis. 37 (5), 437–445.
Banghart, M., 2014. Utilizing Confidence Bounds in Failure Mode Effects Analysis (FMEA) Hazard Risk Assessment.
Barends, D.M., Oldenhof, M.T., Vredenbregt, M.J., Nauta, M.J., 2012. Risk analysis of analytical validations by probabilistic modification of FMEA. J. Pharm. Biomed. Anal. 64 (65), 82–86.
Baykasoğlu, A., Gölcük, İ., 2017. Comprehensive fuzzy FMEA model: a case study of ERP implementation risks. Operational Research 1–32.
Cameron, I., Mannan, S., Németh, E., Park, S., Pasman, H., Rogers, W., Seligmann, B., 2017. Process hazard analysis, hazard identification and scenario definition: are the conventional tools sufficient, or should and can we do much better? Process Saf. Environ. Prot. 110, 53–70.
Carlson, C.S., 2014. Understanding and applying the fundamentals of FMEAs. In: 2014 Annual Reliability and Maintainability Symposium, 12. RAMS).
Chai, K.C., Jong, C.H., Tay, K.M., Lim, C.P., 2016. A perceptual computing-based method to prioritize failure modes in failure mode and effect analysis and its application to edible bird nest farming. Applied Soft Computing Journal.
Chen, F., 2015. An Investigation and Evaluation of Risk Assessment Methods in Information Systems. Chalmers University of Technology, Sweden.
de Vaus, D., 2002. Survey in Social Research, fifth ed. Allen & Unwin, Australia.
Estorilio, C., Posso, R.K., 2010. The reduction of irregularities in the use of "process FMEA. Int. J. Qual. Reliab. Manag. 27 (6), 721–733.
Gary Teng, S., Ho, S.M., Shumar, D., Liu, P.C., 2006. Implementing FMEA in a collaborative supply chain environment. Int. J. Qual. Reliab. Manag. 23 (2), 179–196.
Hall, W., Coats, M., 2005. Action Research: A Guide for Associate Lecturers, 28. The Open University. Retrieved from: www.open.ac.uk/cobe.
Jain, K., 2017. Use of failure mode effect analysis (FMEA) to improve medication management process. Int. J. Health Care Qual. Assur. 30 (2).
Janneti, A.J., 2012. A Representation: Incorporating a Needs Assessment and gap Analysis into the Educational Design. Author, Pitman,NJ .
Lai, L.K.H., Chin, K.S., 2014. Development of a failure mode and effects analysis based risk assessment tool for information security. Industrial Engineering and Management Systems 13 (1), 87–100.
Liu, H., Liu, L., Liu, N., 2013. Expert Systems with Applications Risk evaluation approaches in failure mode and effects analysis : a literature review. Expert Syst. Appl. 40 (2), 828–838.
McDermott, R.E., Mikulak, R.J., Beauregard, M.R. (Eds.), 2009. The basic of FMEA, second ed. CRC Press, New York. Taylor & Francis Group.
Murphy, M., Heaney, G., Perera, S., 2011. A methodology for evaluating construction innovation constraints through project stakeholder competencies and FMEA. Constr. Innovat. 11 (4), 416–440.
Najwa, N.F., Subriadi, A.P., 2018. A need to modify the method of failure mode and effect analysis (FMEA) and risk management. International Journal of Scientific Research in Computer Science, Engineering and Information Technology 3 (6), 143–158.
Oldenhof, M.T., van Leeuwen, J.F., Nauta, M.J., de Kaste, D., Odekerken-Rombouts, Y.M.C.F., Vredenbregt, M.J., et al., 2011. Consistency of FMEA used in the validation of analytical procedures. J. Pharm. Biomed. Anal. 54 (3), 592–595.
Paciarotti, C., Mazzuto, G., D'Ettorre, D., 2014. A revised FMEA application to the quality control management. Int. J. Qual. Reliab. Manag. 31 (7), 788–810.
Ramanan, B., 2008. An Ilustration of Application of Failure Mode and Effect Analysis (FMEA) Techniques to the Analysis of Information Security Risks (ISO 27001). Retrieved from: www.ISO27001security.com.
Raspotnig, C., Opdahl, A., 2013. Comparing risk identification techniques for safety and security requirements. J. Syst. Softw. 86 (4), 1124–1151.
Rose, S., Spinks, N., Canhoto, A.I., 2015. Management Research: Applying the Principles.
Sankar, R.N., Prabhu, B.S., 2001. Modified approach for prioritization of failures in a system failure mode and effects analysis. Int. J. Qual. Reliab. Manag. 18 (3), 324–336.
Sawhney, R., Subburaman, K., Sonntag, C., Rao Venkateswara Rao, P., Capizzi, C., 2010. A modified FMEA approach to enhance reliability of lean systems. Int. J. Qual. Reliab. Manag. 27 (7), 832–855.
27001 Security, I., 2008. An Illustration of the Application of Failure Modes and Effects Analysis (FMEA) Techniques to the Analysis of Information Security Risks. United States of America.
Sharma, R.K., Sharma, P., 2010. System failure behavior and maintenance decision making using, RCA, FMEA and FM. J. Qual. Maint. Eng. 16 (1), 64–88.
Silva, M.M., De Gusmão, A.P.H., Poleto, T., Silva, L.C.E., Costa, A.P.C.S., 2014. A multidimensional approach to information security risk management using FMEA and fuzzy theory. Int. J. Inf. Manag. 34 (6), 733–740.
Software, S.P.L.M., 2016. How to conduct a failure modes and effects analysis. In: A White Paper Issued by: Siemens PLM Software. Retrieved from: www.siemens.com /polarion.
Spremic, M., Popovic, M., 2008. Emerging issues in IT Governance : implementing the corporate IT risks management model. WSEAS Trans. Syst. 7 (3), 219–228.
Stamatis, D.H., 2003. Failure Mode and Effect Analysis: FMEA from Theory to Execution (Illustrate). ASQ Quality Press, Milwaukee, Wisconsin.
Subriadi, A.P., Najwa, N.F., Cahyabuana, B.D., Lukitosari, V., 2018. The consistency of using failure mode effect analysis (FMEA) on risk assessment of information technology. In: 2018 International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2018, pp. 61–66.
van Leeuwen, J.F., Nauta, M.J., de Kaste, D., Odekerken-Rombouts, Y.M.C.F., Oldenhof, M.T., Vredenbregt, M.J., Barends, D.M., 2009. Risk analysis by FMEA as an element of analytical validation. J. Pharm. Biomed. Anal. 50 (5), 1085–1087.
Whitman, M.E., Mattord, H.J., 2012. Principles of information security. Course Technology 1–617.
Wibowo, A.M., 2005. ISO 27001 : 2005 Information Security Management Systems. Risk Management. Retrieved from itgov.cs.ui.ac.id.
Xiao, N., Huang, H.Z., Li, Y., He, L., Jin, T., 2011. Multiple failure modes analysis and weighted risk priority number evaluation in FMEA. Eng. Fail. Anal. 18 (4), 1162–1170.
Zhao, X., Bai, X., 2010. The Application of FMEA Method in the Risk Management of Medical Device during the Lifecycle. In: 2010 2nd International Conference on E-Business and Information System Security, pp. 455–458. EBISS2010.