Security Risk Assessment of Online Fish Quarantine Information System Using FMEA

by Okfalisa Okfalisa

Submission date: 05-Jan-2021 10:07AM (UTC+0700)

Submission ID: 1483147848

File name: Security_Risk_Assessment_of_Online_Fish_Quarantine.pdf (191.93K)

Word count: 3281

Character count: 18330

Security Risk Assessment of Online Fish Quarantine Information System Using FMEA

M Megawati[1,a)],O Okfalisa[2,b)], M Alkarim [1,c)]

[1] *Department of Information Systems, Universitas Islam Negeri Sultan Syarif Kasim Riau, Indonesia.*
[2] *Department of Informatics Engineering, Universitas Islam Negeri Sultan Syarif Kasim Riau Indonesia.*

[a)]Corresponding author: megawati@uin-suska.ac.id
[b)]okfalisa@gmail.com
[c)]m.alkarim007@gmail.com

Abstract. Risk is the main cause of uncertainty in an organization thus it affects the achievement of objectives. Therefore, the identification of risks and employing the procedure to mitigate potential issues is an essential part of effective organizational business. Karoline (Online Fish Quarantine Information System) is an application that monitors the operational activities of the Fish Quarantine Agency, quality control, and safety of fishery products. Lack of updated data management, limited access to the system, and inadequacy of system security put forward this Karoline information system under uncontrolled and at risk. To date, this study tries to measure the risk level of this application using Failure Mode and Effect Analysis (FMEA). This study reveals the place of the significant issue on the values of Risk Priority Number (RPN) assessment viz. cybercrime, firewall, and people. Moreover, the analysis prepared with the recommendation to aid in making the right decision and corrective action for an organization is facing a high risk of the system.

INTRODUCTION

The fish quarantine station that is allocated at Riau province is engaged in controlling the quality and safety of fishery products under the supervised government quarantine agency. This agency is tasked to check the status of fish for entrepreneurs engaged in fisheries. The entrepreneurs must be ensured their fish is certified, healthy, not contaminated with viruses, fungi, bacteria, or parasites. The agency adopted information technology namely an Online fish quarantine information system (Karoline). Karoline Information System is a service system that regulates the operational flow activities at Quarantine Agency. An interview with a head division of Information Technology at Quarantine Agency identified the emergence of issues that affected to the security and working of the system including the lacking of data management, high dependency on the central network, outdated the support of technology infrastructure of hardware, and software, human factors errors, lack of system security that easy to be an intrusion by hackers, and the delays of data transmission and entry process.

In a nutshell, this situation grows into the high risks for the business process and disrupts organizational performance. Information technology adoption as well as online readable-machine databases have emerged as one of the most significant infrastructures in the last decade of the burgeoning information industry. The online database is utilized to make a connection of digital information storage thus it smooths the way access of large and small networks and the internet. The collection of information embedded in online databases provides the users to search or retrieve the data [1][2]. Therefore, to minimize the threat and risk of information technology adoption inclusive of the Karoline information system, it is necessary to have information technology assessment of security risk management as sides of aspects of confidentiality, integrity, and availability [3].

According to Kasidi (2014), risk management can be defined as an effort to reduce the possible losses of the arisen risks [4]. Meanwhile, Stoneburner, et al. (2002) [5] designates the risk management as Information Technology (IT) managers process in balancing the operational and economic costs towards the protection of IT data and system in supporting the achievement of organizational objectives and mission. Thus, the facing of IT risks can be reduced or eliminated [6]. The risk management presents a systematic approach of risk modeling, the interdependency and complexity between risks, identify and analyze the risks, and the evaluation, treatment, and monitoring risks [7-9].

The common method in risk management analysis is failure mode and effect analysis (FMEA) [10]. FMEA determines and prioritizes the potential risks by scoring the causes and effects of associated risks and planning the risk mitigation of critical assets [11][12]. Moreover, FMEA as semi-quantitative risk assessment hands over problem detection thus it disqualified the potential failures of the system as well as system development, system engineering, and design, system flow process, system operational management, and system service before reaching the customers [13-15]. The RPN in FMEA supports the quantitative analysis of risk events thus provide the highest accurate and quick analysis that overcome the losing information [16]. FMEA can also evaluate the potential risk critically (Murphy et al, 2011) [17] and equips the common structure and languages that can be easier to be applied in many types of organization such as manufacturing and service industries, profit and no-profit organization, private and public organization [18]. The previous researches have been successfully applied the FMEA, including Xiaotong et al (2018) who assessing information security risk for evolving smart city [19], Subriadi et al (2018) evaluated the webserver system security gap using FMEA [20], Mustafa et al (2020) hybrid the FMEA, Fuzzy Inference System (FIS), and Fuzzy Data Envelopment Analysis (DEA) to calculate a novel score of risk analysis in health, safety and environment in the chemical industry [21)], Linhan et al (2019) employed an interval probability-based FMEA model for assessing the assemble process of spark plugs [22].

RESPONSE SURFACE METHODOLOGY

Data Collection

Data collection was carried out through thorough observation, interviews, and questionnaires dissemination. The observations were made within two months at Fish Quarantine Agency to discover the currents issues and problems regarding the Karoline system and business process activities in a particular environment. The interviews were organized by questioning three key actors in this study, including the administrator of the Karoline system, head division of Information Technology at Quarantine Agency, and the manager operational of the Quarantine Agency. Meanwhile, the questionnaires were distributed to the above respondents in order to measure the responsibility, accountability, consulted, and informed of the Karoline system. The procedures place on the RACI (Responsible, Accountable, Consulted, and Informed) models. The RACI is capable of improving project organization, identify the roles involved, and how the roles may be organized [23][24].

Business Process Analysis

The changes in information technology adoption can be determined by understanding the improvements in business models, business process activities, strategies, and organizational directions [25]. Karoline information system administers the operational regulation services at the Fish Quarantine Agency office. Firstly, the customers submit the request letter to permit their fishery business scrutinized. The administrator received the requirements and proceed with a data system entry. Secondly, the customers then accede the fish into laboratory inspection and external domestic certification test. Finally, the payments via bank transfer are round of the activities.

Risk Analysis

The next step is conducting the risk analysis on the ongoing Karoline system using the FMEA method [26]. The flow activities of FMEA can be depicted in Fig.1 [10]. Risk analysis was organized by analyzing the strengths and weaknesses of the organization and system. The effect analysis was supervised to pinpoint the potential threats and its implication on the organization. The components and listing assets were determined by following the RACI model. In the end, the values of RPN were calculated by ensuing the formula below [10].

$$\text{RPN} = \text{severity x detection x occurrence} \qquad (1)$$

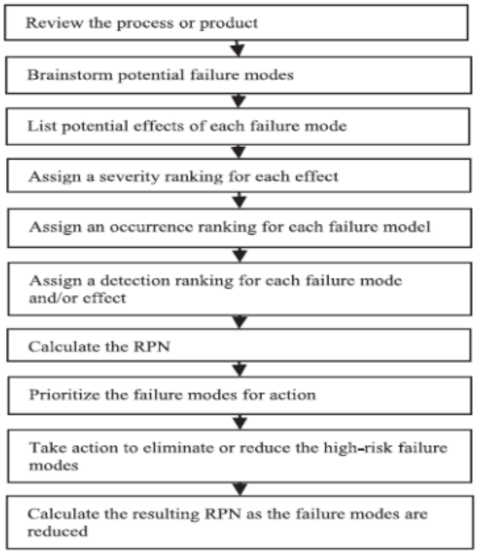
Review the process or product
Brainstorm potential failure modes
List potential effects of each failure mode
Assign a severity ranking for each effect
Assign an occurrence ranking for each failure model
Assign a detection ranking for each failure mode and/or effect
Calculate the RPN
Prioritize the failure modes for action
Take action to eliminate or reduce the high-risk failure modes
Calculate the resulting RPN as the failure modes are reduced

FIGURE 1. FMEA Process Activities

The prioritized risks were determined based on the consistency values of RPN described in the 1-10 scale of highest urgency risk. The RPN is a useful and simple tool for measure risk, takes the occurrence of failure modes, the severity of failures affect, and the probability of not detecting the failure into account [27]. Many scholars found that RPN enhances the uncertainty of FMEA assessment capabilities [28]. The RPN scale is commonly used and prioritize the risk assessment into very high, high, medium, low, and very low-risk level. The risk level is a reference for the elimination of the high risk of failure mode before suggesting the recommendation as improvement and corrective actions.

RESULTS AND DISCUSSIONS

Analysis of Organizational Strengths and Weaknesses

Reviewing the emergence of possible risks at the Fish Quarantine Agency, Table 1 was defined as follows.

TABLE 1. Organizational Strengths and Weaknesses

Organizational Strength	Organizational Weaknesses
The strategic office location and easy to find. An adequate office	Inadequate office facilities
Every room is equipped by closed-circuit television (CCTV) for security	The centralized of decision-making systems
The replacement of three security guards	Un-standard IT infrastructure
The readiness of standard operating procedure at each section	Lack of human resources capabilities
The availability of job description for each division	Lack of transparency at recruitment selection system
Fast service system	Lack of training and activities in supporting the competency improvement

The availability of an online quarantine information system (Karoline)	Lack of IT infrastructure in supporting the Karoline system
The availability of online registration	Lack of monitoring system and devices
The easy access for payment	
The readiness of administrative and infrastructure services.	

Analysis of Strengths and Weaknesses of Karoline System

The review analysis of the strengths and weaknesses of the Karoline system is explained in Table 2.

TABLE 2. The Karoline System Strengths and Weaknesses

System Strengths	System Weaknesses
Provides an online registration feature	The system only can be accessed by restricted specifications of infrastructures
The system provides with four-level access permissions	Centralized of system upgraded
The secure of system access	System maintenance is centralized
The periodic maintenance of system security	It found a security gap in the Karoline system
The period of data backup	The limitation of network availability
Perform the maintenance of system upgrading	The upgraded centralized system impacts to the whole area
The system is equipped with a certificate and payment print out	The system operation is influenced by the upgraded centralized system
Upgraded antivirus	System maintenance is controlled by the center office
The maintain of IT infrastructure with standard antivirus	The availability of data multi-leveling access

The analysis of organizational strengths and weaknesses regards on Karoline system can be utilized as a reference in designing a questionnaire as process control for values detection.

Effect Analysis

In order to analyze the effect analysis, potential, and non-potential effects, Table 3 is explained.

TABEL 3. Effect Analysis

Potential	Potential Effects
Server on fires	Operational activity or performance has stopped thus effect to the financial loss
Server on overheat	Operational activities or performance are hampered
Server down	Operational activities or performance are hampered
Server in failure	The server cannot be used and financial loss
Computer in damage	Operational activities or performance are hampered
The computer cannot be used	Operational activities or performance are hampered and financial losses
The computer equipment is out of dated	Operational activities or performance are hampered and
Loss of computer components	Financial losses

Illegal access to IT infrastructure	Unsecure information and loss of agency reputation
Network failure	Operational activities or performance are hampered
Network device damage	Operational activities or performance are hampered
Printer / Scanner damage	Cannot print and scan data
Loss of printer/scanner	Unable to print and scan data, financial loss
Software Failure	Operational activities or performance are hampered
Virus attack	Operational activities or performance are hampered
System failure	Operational activities or performance have stopped
Human failure	Un-optimal the professionalism of prospective service users
Falsification or abuse of access rights	Agency reputation
Full capacity	Data confidentiality
Information spread	Data confidentiality
Data/information breaches	Data confidentiality
Incompatible system data	Data integrity

RACI Chart Mapping

The RACI chart serves the roles and responsibilities of key stakeholders who are directly related to the IT management process at Fish Quarantine Agency, including the head of the IT division, the operational management section, and the administration section. The mapping of the RACI chart diagram is explained in Table 4.

following is a RACI Chart diagram which can be seen in Table 4:

TABEL 4. RACI Chart Diagram

Duties or Roles	IT leadership	Operations Section	Administration section
Develop, manage, operate and maintain the network infrastructure systems, servers, and databases at Quarantine Agency	R,A,C,I	R,C,I	R,C,I
Manage, operate, and evaluate IT operations	R,A,C,I	R,A,C,I	R,C,I
Making the decision and responsibility for the whole activities and employees	R,A,C	R,C,I	I
Provide the agency business solutions	R,C,I	R,A,I	R, I

List the Component Assets

Table 5 determined the list of asset components in supporting the Karoline system.

TABLE 5. List of Asset Components

Category	Asset
Hardware	Personal computer, Server, Printer, Uninterruptible power supply (UPS), Genset, Ac, Hardisk, CCTV, Hub dan Microtech
Software	Karoline system, Microsoft Office, Smadav, Avas, Web base and Operating Systems
Network	Telkomsel, Icon +(PLN), LAN, Network Cable
Data	Fish Data, Service User Data, Quarantine Data, Port Data
People	Super Admin, Administrator, Operations and PNBP / Treasurer

Assessment of Severity, Occurrence, and Detection (SOD)

The value of severity (SEV), occupancy (OCC), and detection (DET) can be seen in table 6.

TABLE 6. Determines the SOD value

Code	Process	Critical	Potential	Potential	SEV	Potential	OCC	Current	DET
	Function (Category)	Assets	Failure Modes (process defect)	Effect(s) of		Cause(s) of Failure		Process Controls	
HW01	Hardware	Server	Server Fires	Activities operational or performance stopped	5	Server overheat	7	Check the server room every day	1
HW02			Server Fires	Financial Loss	5	Short-Circuit (power failure)	1	Checking the damaged IT infrastructure	1

RPN Calculation

There were thirty-six RPN values generated with five RPN level categories, including the very high level with RPN values at 216, the medium level with the RPN values is 160, the low level with the values from 70 to 24, and a very low level with the RPN values from 18 to 1. The RPN values selection based on the level can be depicted in Table 7.

TABLE 7. Calculation of RPN

Code	Function (Category)	Assets	Failure Modes (process defects)	Effect(s) of Failure	SEV	Cause(s) of Failure	OCC	Process Controls	DET	RPN
HW01	Hardware	Server	Server Fires	Operational Activities or performance have stopped	5	Server overheat	7	Check the server Room every day	1	35
HW02	Hardware	Server	Server Fires	Financial Loss	5	Short-circuit (power failure)	1	Checking the damaged IT infrastructure	1	5
HW03	Hardware	Server	Server overheat	Operational activities or performance are hampered	5	Non-functioning AC in the server room	3	Check the server room every day	2	30
HW04	Hardware	Server	Server down	Operational activities or performance are hampered	4	Too many units are accessing the server at the same time or DDOS attacks	2	Checking the damaged IT infrastructure	3	36

Risk Priorities Analysis

The analysis of risk priorities is determined in Table 8. The risks are ranked based on the RPN values of process defects, viz., cybercrime (RPN=216), system failure (RPN=160), human failure (RPN= 112), and computer damage (RPN=70) respectively. Detailed recommendations are given in Table 9 as system improvement and corrective action.

TABLE 8. Risk Priority

Category	***Code***	***Process Defects***	***SEV***	***OCC***	***DET***	***RPN***	***Level***	**Rank**
Data	DA06	Cybercrime (hacker attack)	9	6	4	216	*Very High*	1
Software	SW03	System failure	8	5	4	160	*High*	2
People	PP02	Human failure	7	8	2	112	*Medium*	3
Hardware	HW07	Computer Damage	5	7	2	70	*Low*	4

TABLE 9. Recommended improvements

No.	Risk	Findings	Repair
1	Cybercrime	Lack of system security (firewall), Lack of transparency at recruitment selection system	Install a firewall application for all the devices in supporting the Karoline system, utilizes the original and updated software and performs the transparency of career selection
2	System failure	It found a security gap in the Karoline system, lack of system maintenance, System maintenance is centralized	Provide periodic system maintenance and use a secure socket layer in handling the overcome of a hacker for the Karoline system.
3	Human Failure	Lack of human resources capabilities and Lack of pieces of training and activities in supporting the competency improvement	Upgrade regularly the capabilities of human resources in supporting the Karoline system management.

CONCLUSIONS

The FMEA method has been successfully applied to identifying and prioritizing the risks level of the Karoline information system. A series of analyses through the calculation of RPN reveals the three significant risks thus it influences the operation of the Karoline system and Fish Quarantine Agency in achieving their sustainability of business goals, namely the emergence of cybercrime, the system failures, and human failures. Besides, FMEA provides the recommendations for key stakeholders to aid them in deciding to face the emergence of risks and handling is based on the priority level. The analysis of risk management on the Karoline system contributes to the improvement of the change in the management operations of the Fish Quarantine Agency towards the success of technology adoption.

REFERENCES

1. Feather, J., Sturges, P., “International Encyclopedia of Information and Library Science” (London: Routledge, 2003).
2. M. J. M. J. Ershadi and M. Forouzandeh, J. Digit. Inf. Manag. 17, 6, 321 (2019).

3. A. Tchernykh, U. Schwiegelsohn, E. ghazali Talbi, and M. Babenko, J. Comput. Sci. 36 (2019).
4. H. N. Alfatin and L. Leo, “Risk Analysis in A Manufacturing Company’s Inventory Cycle” (APRiSH 2018, 2019), pp. 169–177.
5. Stoneburner, G., Goguen, A. & Feringa, A., “Risk Management Guide for Information Technology Systems” (Nist Special Publication, 2002), p.58.
6. A. Martens and M. Vanhoucke, Eur. J. Oper. Res. 277, 2, 442–453 (2019).
7. SA, “Risk Management: Principles and Guidelines” (Standards Australia, Sydney, 2009).
8. Schieg, M., J. Bus. Econ. Manag. 7, 2, 77–83 (2006).
9. A. Qazi, J. Quigley, A. Dickson, and K. Kirytopoulos, Int. J. Proj. Manag., 34, 7, 1183–1198 (2016).
10. P. Chemweno, L. Pintelon, A. Van Horenbeek, and P. Muchiri, Int. J. Prod. Econ. 170, 663–676 (2015).
11. Stamatis, D.H., “Failure Mode and Effect Analysis: FMEA from Theory to Execution. ASQ Quality Press. S” (2003).
12. Kutlu, A.C., Ekmekçioğlu, M., Expert Syst. Appl. 39, 1, 61–67 (2012).
13. Cicek, K., Celik, M., Saf. Sci. 51, 1, 6–10 (2013).
14. R. Fattahi and M. Khalilzadeh, Saf. Sci. 102, 290–300 (2018).
15. T. Immawan, W. Sutrisno, and A. K. Rachman, “Operational risk analysis with Fuzzy FMEA (Failure Mode and Effect Analysis) approach (Case study: Optimus Creative Bandung)” (MATEC Web Conf., 2018).
16. A. P. Subriadi and N. F. Najwa, Heliyon 6, 1, (2020).
17. Murphy, M., Heaney, G., Perera, S., Constr. Innovat 11, 4, 416–440 (2011).
18. McDermott, R.E., Mikulak, R.J., Beauregard, M.R. (Eds.), “The basic of FMEA, second ed. CRC Press” (New York. Taylor & Francis Group., 2009).
19. X. Li, H. Li, B. Sun, and F. Wang, J. Intell. Fuzzy Syst. 34, 4, 2491–2501 (2018).
20. A. P. Subriadi, N. F. Najwa, B. D. Cahyabuana, and V. Lukitosari, “The consistency of using failure mode effect analysis (FMEA) on risk assessment of information technology,” (International Seminar on Research of Information Technology and Intelligent Systems, ISRITI 2018, 2018), pp. 61–66.
21. M. Jahangoshai Rezaee, S. Yousefi, M. Eshkevari, M. Valipour, and M. Saberi, Stoch. Environ. Res. Risk Assess. 34, 1, 201–218 (2020).
22. L. Ouyang, W. Zheng, Y. Zhu, and X. Zhou, Qual. Reliab. Eng. Int. 36, 1, 125–143 (2020).
23. C. J. Costa and J. T. Aparicio, “POST-DS: A Methodology to Boost Data Science” (Iber. Conf. Inf. Syst. Technol. Cist., 2020), pp. 24–27.
24. Ajit Tewari, Shubha Mishra, Shadab Siddiqui, Priyanka Upadhyay, "Performance measurement at the requirement phase of software development life cycle" (Computing for Sustainable Global Development (INDIACom) 2015 2nd International Conference on, 2015), pp. 1090-1094.
25. X. C. Zhang, L. Kuchinke, M. L. Woud, J. Velten, and J. Margraf, Comput. Human Behav. 71, 172–180 (2017).
26. A. M. Nur Widigdo, M. Marimin, I. Fahmi, And I. S. Beik, Al-Iqtishad J. Islam. Econ. 8, 1, 19–32 (2016).
27. J. Qin, Y. Xi, and W. Pedrycz, Appl. Soft Comput. J. 89, 106134 (2020).
28. H. C. Liu, L. E. Wang, Z. Li, and Y. P. Hu, IEEE Trans. Fuzzy Syst. 27, 1, 84–95 (2019).

Security Risk Assessment of Online Fish Quarantine Information System Using FMEA

ORIGINALITY REPORT

8%	2%	5%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Apol Pribadi Subriadi, Nina Fadilah Najwa. "The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment", Heliyon, 2020 Publication	2%
2	Submitted to UIN Sultan Syarif Kasim Riau Student Paper	2%
3	link.springer.com Internet Source	1%
4	Zairion, Fauziyah, E Riani, A A Hakim, A Mashar, H Madduppa, Y Wardiatno. " Morphometric character variation of the blue swimming crab Linnaeus, 1758) population in western and eastern part of Java Sea ", IOP Conference Series: Earth and Environmental Science, 2020 Publication	<1%
5	Carlos J. Costa, Joao Tiago Aparicio. "POST-DS: A Methodology to Boost Data Science",	<1%

	2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020 Publication	
6	www.un-page.org Internet Source	<1%
7	Wahdania Suardi, Mardiansyah. "Implementation of Participatory Policy through Quality Awareness and Quarantine Community Movement (Gemasatukata) in Untia Village, Makassar City", IOP Conference Series: Earth and Environmental Science, 2019 Publication	<1%
8	Apol Pribadi Subriadi, Nina Fadilah Najwa, Brigitta Devianti Cahyabuana, Valeriana Lukitosari. "The Consistency of Using Failure Mode Effect Analysis (FMEA) on Risk Assessment of Information Technology", 2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI), 2018 Publication	<1%
9	journals.vgtu.lt Internet Source	<1%
10	silo.pub Internet Source	<1%
11	patents.google.com Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		