

Bug/error found in Palapa, Gamel & Elisa that arises when IT staff performs maintenance. Consequences are Bugs/errors made by IT staff during maintenance greatly reduced the productivity of IT and greatly reduced the productivity of IT and users who use related applications. It developed distrust to the application being used. The total relative Risk Score is 26, as shown in Fig. 4.

A possibility of vulnerability attack by internal/external parties in Palapa, Gamel & Elisa application. Consequences are the public's overall opinion of the institution could be affected adversely. The institution's productivity would be also impacted. The total relative Risk Score is 31, as shown in Fig. 5.

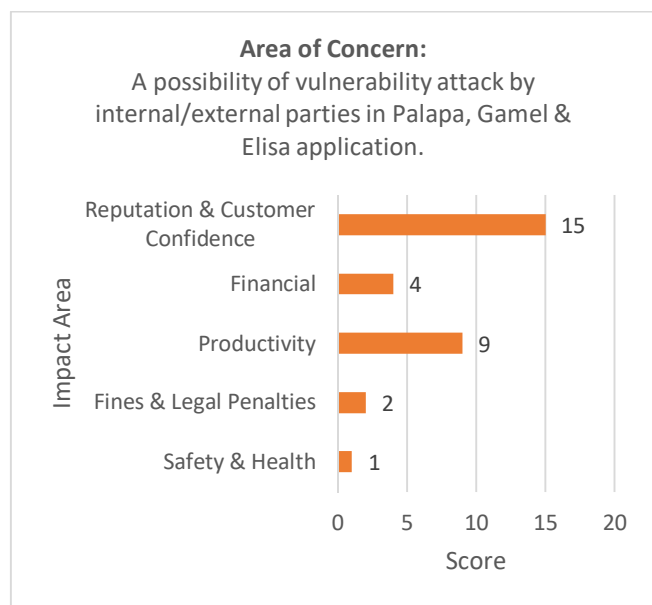


Fig. 5 Risk Analysis Area of Concern 3

H. Step 8: Select Mitigation Approach

The identified risks are sorted by risk score. Then, categorize the risks by sorting them from highest to lowest to help to formulate better mitigation strategies. After that, creating Relative Risk Matrix by separating the risks into three groups with the same number of risks.

TABLE VIII
RELATIVE RISK MATRIX

Risk Score		
35 TO 45	25 TO 34	15 TO 24
Pool 1	Pool 2	Pool 3

The next activity is deciding the mitigation approach based on pool from the Relative Risk Matrix. If the risk score is high, then it was placed in pool 1. The mitigation approach for pool 1 is mitigated. It explains the need for direct action to try to lessen the seriousness of the risks. If the risk score is medium, then it was placed in pool 2. The mitigation approach for pool 2 is mitigated or defer. It explains the need for direct action or later time action. The final one, If the risk score is low, then it was placed in pool 3. The mitigation approach for pool 3 is accepted. It explains the willingness to accept conditions.

TABLE IX
MITIGATION APPROACH

POOL	Mitigation Approach
1	Mitigate
2	Mitigate or Defer
3	Accept

TABLE X
RISK MITIGATION – STUDENT PROFILE

Area of Concern	Due to the large number of student profiles, there were errors in data input by Academic staff.
Relative Risk Score	41
Pool	Pool 1
Action	Mitigate
Container	Control
Palapa, Gamel & Elisa	Add notification for validation entries in the input fields. Each field must be validated before execution to the next process / page.
<ul style="list-style-type: none"> IT unit Staff Faculty of Medicine Academic Staff IT Staff 	Immediately modify the invalid data if it is known that an error has occurred.
Area of Concern	Bug/error found in Palapa, Gamel & Elisa that arises when IT staff performs maintenance.
Relative Risk Score	26
Pool	Pool 2
Action	Mitigate or Defer
Container	Control
<ul style="list-style-type: none"> IT unit Staff Faculty of Medicine IT Staff 	If it's an important issue, then immediately resolve application bugs/errors or crashes. However, if it's not crucial, then it can be deferred. Ensure the application passes testing and QA before deployment. Control and maintain periodically to ensure the application are free of bug/error and does not crash.
Area of Concern	A possibility of vulnerability attack by internal/external parties in Palapa, Gamel & Elisa application.
Relative Risk Score	31
Pool	Pool 2
Action	Defer
Container	Control
Database server and Palapa, Gamel & Elisa	Use/activate the transaction log on network equipment and enforce policies to review the log periodically. Adding features in the application. For example, if the application is idle for more than five minutes, it automatically logs out from the application.

Information system risk management was performed in the computing environment of Faculty of Medicine, X University. It was conducted using OCTAVE Allegro framework. The framework provides the capability to streamline and optimize information system risk management process through eight

steps and various worksheets and questionnaire sheets for guidelines. After completing all the required data, the analysis was conducted to determine the critical information assets for the organization. The results showed that there were 8 (eight) critical information assets, including Student Profile, Lecturer Profile, Course, Student Score, Class Schedule, Lecturer Attendance, Payment of Tuition, and Curriculum.

Student Profile is one of the critical information assets. It was continued to be assessed using a chronological approach of information system risk management for improving security awareness and formulating mitigation strategies as the control actions. Based on the results of the assessment: (1) errors in data input are getting the highest score and need mitigation; (2) while for the bug/error and a possibility of vulnerability attack are in pool 2 (mitigate or defer), where the institution can choose either to mitigate with the mitigation strategies offered or to delay the control actions (but if it disrupts the operation, it should be hastened).

IV. CONCLUSION

Information system risk management was conducted using OCTAVE Allegro framework. The results showed that there were 8 (eight) critical information assets. Student Profile is one of the critical information assets. It continued to be assessed. Based on the assessment results, there is a need for mitigation strategies offered or the control actions. The analysis and results of this study are expected to contribute to implementing information system risk management for real case applications in different sectors.

ACKNOWLEDGMENT

This work is supported by the Institute for Research and Community Service (LPPM) Universitas Pembangunan Nasional "Veteran" Jakarta (UPNVJ), Faculty of Computer Science UPNVJ, Information Systems Study Program UPNVJ for providing funding support and assisting the implementation of this research.

REFERENCES

[1] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," in *Procedia Computer Science*, 2018, vol. 135, pp. 202–213. doi: 10.1016/j.procs.2018.08.167.

[2] G. Strupczewski, "Defining cyber risk," *Safety Science*, vol. 135, no. December 2020, 2021, doi: 10.1016/j.ssci.2020.105143.

[3] S. A. Taleh, "Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as 'Compliance Managers' for Businesses," *Law & Social Inquiry*, vol. 43, no. 2, pp. 417–440, 2018.

[4] P. J. O. Management Studies Kuzmenko, O. v Kubálek, J. Bozhenko, V. v Kushneryov, and I. Vida, "An Approach to Managing Innovation to Protect Financial Sector Against Cybercrime," vol. 24, no. 2, 2021, doi: 10.17512/pjms.2021.24.2.17.

[5] H. Tao et al., "Economic perspective analysis of protecting big data security and privacy," *Future Generation Computer Systems*, vol. 98, pp. 660–671, 2019, doi: 10.1016/j.future.2019.03.042.

[6] D. K. Citron and D. Solove, "Risk and Anxiety : A Theory of Data Breach Harms," *Texas Law Review*, vol. 96:737, 2018.

[7] M. Setapa, M. Mamat, H. A. Bakar, S. N. S. Yusuf, and S. Kazemian, "Enterprise Risk Management: Impact on Performance of Private Higher Educational Institutions In Malaysia," *Polish Journal of Management Studies*, vol. 22, no. 1, pp. 485–501, 2020, doi: 10.17512/pjms.2020.22.1.31.

[8] C. Joshi and U. Kumar, "Information security risks management framework – A step towards mitigating security risks in university network," *Journal of Information Security and Applications*, vol. 35, pp. 128–137, 2017, doi: 10.1016/j.jisa.2017.06.006.

[9] L. Paoli, J. Visschers, and C. Verstraete, "The impact of cybercrime on businesses : A novel conceptual framework and its application to Belgium," *Crime, Law and Social Change*, 2018.

[10] W. Sardjono, E. Selviyanti, W. G. Perdana, and Maryani, "Modeling of development of performance evaluation on health information systems implementation," in *Journal of Physics: Conference Series*, Mar. 2020, vol. 1465, no. 1. doi: 10.1088/1742-6596/1465/1/012025.

[11] T. Hidayat, O. Rukmana, and A. A. Nurrahman, "Design information system of registration and scheduling information laboratory of information systems and the decision of Bandung Islamic University," in *Journal of Physics: Conference Series*, Feb. 2020, vol. 1469, no. 1. doi: 10.1088/1742-6596/1469/1/012134.

[12] E. Selviyanti and W. Sardjono, "Risk management information systems assessment at the television broadcasting company," in *Journal of Physics: Conference Series*, Mar. 2020, vol. 1465, no. 1. doi: 10.1088/1742-6596/1465/1/012016.

[13] T. Žužek, L. Rihar, T. Berlec, and J. Kušar, "Standard project risk analysis approach," *Business Systems Research*, vol. 11, no. 2, pp. 149–158, Oct. 2020, doi: 10.2478/bsrj-2020-0021.

[14] P. F. de A. Lima and C. Verbano, "Project Risk Management Implementation in SMEs: A Case Study from Italy," *Journal of Technology Management & Innovation*, vol. 14, no. 1, 2019, [Online]. Available: <http://jotmi.org>

[15] H. Očevčić, K. Nenadić, K. Šolić, and T. Keser, "The Impact of Information System Risk Management on the Frequency and Intensity of Security Incidents," 2017.

[16] O. v. Kondratyeva, O. A. Kondratyeva, and I. A. Kondratev, "The Risk Management Methodology of the Quality Reducing Process of Enterprise Management Information Systems Service Support," in *IOP Conference Series: Earth and Environmental Science*, Mar. 2021, vol. 666, no. 6. doi: 10.1088/1755-1315/666/6/062128.

[17] N. M. S. Algheriani, V. D. Majstorovic, S. Kirin, and V. Spasojevic Brkic, "Risk model for integrated management system," *Tehnicki Vjesnik*, vol. 26, no. 6, pp. 1833–1840, Nov. 2019, doi: 10.17559/TV-20190123142317.

[18] T. Karkoszka, "Risk Management System in Metallurgical Production," *Metalurgija*, vol. 60, no. 1–2, pp. 133–136, 2021.

[19] W. Zhu and Y. Jia, "The Research on Safety Management Information System of Railway Passenger Based on Risk Management Theory," in *IOP Conference Series: Earth and Environmental Science*, Jan. 2018, vol. 108, no. 4. doi: 10.1088/1755-1315/108/4/042067.

[20] B. Irvin Lamarca, "Cybersecurity Risk Assessment of the University of Northern Philippines using PRISM Approach," in *IOP Conference Series: Materials Science and Engineering*, Jun. 2020, vol. 769, no. 1. doi: 10.1088/1757-899X/769/1/012066.

[21] A. Amini and N. Jamil, "A Comprehensive Review of Existing Risk Assessment Models in Cloud Computing," in *Journal of Physics: Conference Series*, Jun. 2018, vol. 1018, no. 1. doi: 10.1088/1742-6596/1018/1/012004.

[22] P. Foroudi, Q. Yu, S. Gupta, and M. M. Foroudi, "Enhancing university brand image and reputation through customer value co-creation behaviour," *Technological Forecasting and Social Change*, vol. 138, pp. 218–227, Jan. 2019, doi: 10.1016/j.techfore.2018.09.006.