Journal of Interest: Economics, Business, and Accounting Review
Vol. 1, No. 1, January 2024

A COSO ERM integrated framework evaluation of it governance risk management

Sri Yuni
Fakultas Ekonomi dan Bisnis Universitas Palangka Raya
Ade Yuniati
Fakultas Ekonomi dan Bisnis Universitas Palangka Raya
Golda Belladonna Umbing
Fakultas Ekonomi dan Bisnis Universitas Palangka Raya

Corresponding Author:
Sri Yuni
Palangka Raya, Central Kalimantan
E-mail: sri.yuni@feb.upr.ac.id

Journal of Interest: Economics, Business, and Accounting Review
pp: 38 – 42

ABSTRACT

The implementation of information technology governance (ITG) risk management is highly imperative for universities due to its numerous advantages in effectively managing risks within the realm of ITG. Regrettably, the current state of TKTI risk management in the Faculty of Economics and Business, Palangka Raya University is suboptimal. The management of TKTI hazards in present circumstances is partially reliant on manual processes, lacking a comprehensive approach and neglecting the utilization of a risk management framework. The lack of organization inside the TKTI system results in increased effort required for the execution of the TKTI maintenance procedure. An illustrative instance pertains to the deployment of an online educational platform within the Covid-19 pandemic, wherein the utilization of applications, information systems, human resources, and networks frequently gives rise to problems. The faults manifest as either human errors or server issues. This study aims to examine the procedure of analyzing and designing Information Technology Governance Risk Management at the Faculty of Economics and Business, Palangka Raya University. The research utilizes the COSO ERM Integrated Framework to generate suggestions for TKTI. The design methodology employed encompasses five out of the eight stages within the risk management framework. These stages include the internal environment, objective setting, event identification, risk assessment, and risk response. The risk management module in question has been constructed utilizing the COSO ERM Integrated Framework. The outcome of this study is a risk management document for TKTI, which facilitates the management and mitigation of risks by the Information Technology and Systems Agency (BTSI) and the Technical Implementation Unit (UPT). This document is designed to address potential events and emerging trends, to prevent significant losses at the Faculty of Economics and Business, Palangka Raya University.

Keyword : Risk Management, Risk, TKTI, Framework, COSO ERM, Faculty of Economics and Business, Palangka Raya University

1. INTRODUCTION

Information technology (IT) assumes a significant role inside many institutions, with universities being no exception (Carayannis & Morawska-Jancelewicz, 2022). Function of information technology (IT) in the realm of higher education is around facilitating the decision-making process, enhancing the efficiency of processes and resources, and providing assistance for operational and administrative tasks. The Faculty of Economics and Business at Palangka Raya University is a public institution of higher education located in Palangka Raya City, which is situated in the province of Central Kalimantan. Based on the conducted interviews, it has been ascertained that this institution continues to encounter numerous challenges pertaining to the implementation of IT governance risk management. One issue is to the presence of security vulnerabilities due to the reliance on monthly evaluations for IT management. To address this concern, it is imperative to develop an IT governance risk management document that adheres to a comprehensive framework. This document will serve to mitigate these threats and mitigate potential substantial losses (Habbal et al., 2024).

The suitability of the institutional context and targets within an organization can be assessed using the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management

(ERM) Integrated Framework (Moloi & Marwala, 2023). This assessment allows for the identification of recommendations pertaining to the risks that have been mapped. The objective of this article is to gain insight into the process of establishing IT governance risk management, as well as to explore the methods for identifying events, risks, and corresponding risk responses through the utilization of COSO ERM. The primary advantage of this research lies in its provision of risk mapping and risk management strategies, which are presented as recommendations. These suggestions have the potential to assist organizations in formulating informed judgments and policies. The research conducted in this study is limited in scope to the IT governance system at the Faculty of Economics and Business, Palangka Raya University. The study was conducted by conducting interviews with managers and supervisors from TKTI who are responsible for ensuring quality.

2. LITERATURE REVIEW

Risk is commonly understood as a state of uncertainty about a future event, wherein judgments are made based on a range of present factors (Mousavi & Gigerenzer, 2014). Risk management is an academic discipline that examines the strategies employed by organizations to identify and address a range of potential issues (Massingham, 2010). These measures are implemented completely and methodically to effectively mitigate risks. The concept of Information Technology Governance refers to the framework and processes that organizations employ to ensure effective and efficient management of their information technology resources (Nani & Ali, 2020). It encompasses the establishment of policies. IT governance is a structured framework that establishes a connection between organizational policies and strategies in the realm of information technology. Its purpose is to foster a cohesive environment that promotes the active participation of management and directors in overseeing and executing IT management in alignment with the objectives and plans of the firm (Gutterman, 2020). The advantages of IT governance encompass strategic alignment, enhanced performance and resource management, as well as increased output quality.

The COSO Enterprise Risk Management (ERM) Integrated Framework is a comprehensive and widely recognized framework that provides guidance for organizations in managing and assessing risks (Perera et al., 2020). This study utilizes the COSO ERM Integrated Framework as a guiding tool within the context of the Faculty of Economics and Business at Palangka Raya University. Researchers have the ability to input interview data into a table format that aligns with the structure of the COSO ERM component, as depicted in Figure 1 of the COSO ERM Integrated Framework.

Figure 1. Relationship between Goals, ERM Components, Work Units
Source : (Hiles, 2012)

According to the data presented in Figure 1 located on the frontal surface of the cube, there exist a total of eight components within the COSO ERM Integrated Framework. These components are identified as the internal environment, objective setting, risk assessment, risk response, and control activities (Hill et al., 2023). The three main components of this framework include actions, information and communication, and monitoring

3. METHODS

The process of data gathering involved the administration of interviews to IT managers affiliated with the Faculty of Economics and Business at Palangka Raya University. The employed interview technique entailed an unstructured and premeditated approach (Ruslin et al., 2022). The subsequent sections outline the many processes involved in this research.

1 Data collection based on organizational conditions or internal environment (Internal Environment).
2 Determining targets (Objective Setting).
3 Risk identification.
4 Risk assessment (Risk Assessment).
5 Response to risk (Risk Response).
6 Withdrawal of risk control recommendations.
7 Drawing conclusions and suggestions.

The steps in internal environmental analysis and target setting are as follows (González-Gaya et al., 2021):

1 Presents a general overview of the institution in the form of profile, vision and mission, organizational structure, organizational culture, IT governance processes, as well as IT resources and threats.
2 Determine the problem analysis in the form of a summary of the obstacles and impacts they cause.

4. RESULT AND DISCUSSIONS

IT Governance Process, Faculty of Economics and Business, Palangka Raya University

The IT governance process at the Faculty of Economics and Business, Palangka Raya University primarily rests upon the accountability of individual units or work units. These units are tasked with developing work programs that encompass short-term, medium-term, and long-term objectives. The work programs are subdivided into smaller assignments or strategic goals. The tasks encompass daily, weekly, monthly, and annual activities that are aligned with the vision and goal of the Faculty of Economics and Business at Palangka Raya University. These tasks are designed to meet specific achievement targets. The oversight of the performance targets will be conducted by the leadership of the Faculty of Economics and Business at Palangka Raya University.

The topic of discussion pertains to the information technology (IT) resources and threats inside the Faculty of Economics and Business at Palangka Raya University. The initial step in conducting an IT resource and threat analysis involves examining the origins of hazards. Based on the findings from conducted interviews, it is evident that the Faculty of Economics and Business at Palangka Raya University possesses a range of information technology (IT) resources and is also exposed to various dangers.

1 Internal: Applications, information, network and infrastructure, HR.
2 External: unexpected events, government policies, competitors, cyber attack activities.

Risk Identification

Risk identification is carried out using 2 models, namely creating risk scenarios, and risk registration based on analysis of IT resources and threats (Filippetto et al., 2021).

Risk Scenario

Risk scenarios try to identify risks from situations where IT resources are utilized. The risk scenario can be seen in table 1.

Table 1. Risk Scenario

High-level Risk Scenario	Asset/ Resources	Threat Type
New technology	HR, applications, infrastructure	Failure, natural accidental/error
Outsourcing and Online Campus	HR, applications, infrastructure, information	Failure, natural accidental/error
Implementation	Applications, infrastructure	Failure
paid software	Applications, infrastructure	Failure
Programs that are difficult to develop	Application	Malicious, Malware
Cyber Attacks	Applications, infrastructure	Failure
Device and network failure	HR	Failure
Management dynamics	HR	Failure
Problems with IT managers	HR	Failure

Risk Register

The results of the risk scenarios that have been recorded are then described in the risk register entry or risk register(Rao, 2009). The risk register itself is the main result of risk identification. The list of risks can be seen in table 2 below.

Table 2. Risk Register

Risk	Event	Asset	Time
New technology	Every activity is handled by technology, employee reduction is due to technology.	HR, applications, infrastructure	5 years
Outsourcing and online campuses	Technological change, social and economic change, disease outbreaks.	HR, Applications, Information, Infrastructure	5 years
Difficult program to develop	Old and unsustainable technology	Applications, Infrastructure	6 months
Device and network failure	Pests, device age, natural disasters, electricity fluctuations.	Applications, Infrastructure, Information	6 months
Cyber attacks	Leaked data confidentiality, inadequate data availability	Application	5 years
Management dynamics	Rapid organizational structure changes / too dynamic	HR	3 years
Problems with IT managers	IT Manager who leaves suddenly, IT Manager who is sick for a long time.	HR	6 months
Paid software implementation	Changes in access to learning software from developers.	Aplikasi, Infrastruktur	5 years

Business competition	Inadequate performance from employees, lack of employee competence, reduced donors	SDM	6 months

Risk Assesment

During this phase, the identified risks are subjected to analysis by assigning a numerical value to each risk based on an assessment of IT resources and potential threats (Li et al., 2020). The assessment of risk in the Faculty of Economics and Business, Palangka Raya University, is conducted by considering the underlying source of the risk, its frequency, and the impact it has on IT governance. The quantification of risk probability and risk impact is represented using a numerical scale ranging from 1 to 5. The risk value is displayed in Table 3, as seen below.

Tablel 3. Risk Assesment

ID Risk	Assessment	Impact Rating	Likelihood Rating	Risk Score
R1	Paid software implementation	1	1	1
R2	New technology	1	2	2
R3	Outsourcing and online campuses	5	3	15
R4	Difficult program to develop	5	1	5
R5	Device and network failure	5	4	20
R6	Cyber attacks	1	2	2
R7	Management dynamics	3	1	3
R8	Problems with IT managers	5	2	10
R9	Business competition	5	3	15

Risk Response

The interview findings prompted the completion of a risk response form for each aspect of risk associated with IT resources and threats. The outcomes arising from IT governance risks are presented in Table 4, as depicted below.

Table 4. Risk Response

ID Risk	Risk Response For This Risk	Response Action
R1	Mitigate	Action Plan 1, Complete 1
R2	Mitigate	Action Plan
R3	Mitigate	Action Plan 1, Complete 2
R4	Mitigate	Action Plan 2, Complete 1
R5	Avoid	Action Plan 1, Complete 2
R6	Avoid	Action Plan 1, Complete 3
R7	Mitigate	Action Plan 1, Complete 2
R8	Avoid	Action Plan 2, Complete 1
R9	Mitigate	Action Plan

IT Governance Recommendations

Based on the results of the assessment and response to risks, this recommendation was made to become a reference and systematic implementation, based on practice. The recommendations given can be seen in table 5 below.

Table 5. IT Governance Recommendations

ID Risk	Risiko	Rekomendasi
R1	Implementation	Action plan: Create a TKTI grand design related to infrastructure and networks as preparation for replacing the external learning applications used, such as Zoom, Google Drive, and so on. Maximizing the implementation of open source applications, especially in all strategic and critical learning applications.
R2	Paid software	Action plan: create a grand design related to technology supporting online lectures, both hardware technology and preparation of learning content that is more optimal towards online learning. Standardize the use of operational tools in the IT governance system.
R3	New technology	Action plan: improving online learning governance from a technological perspective, in the form of responsive applications, minimizing application downtime, information can be accessed 24 hours, and so on. Procedures that have been validated must always be developed periodically and continuously by adopting new technology
R4	Outsourcing and online campuses	Action plan: using a sustainable, micro service and modular framework. Action plan: Improvement and fulfillment of bandwidth and server needs.

R5	Difficult program to develop	Action plan: Providing and using generators for short-term and temporary needs. There must be a decision letter (SK) to manage the risks of the IT governance system. There must be a disaster recovery plan procedure in the data rescue aspect, to prevent data loss.
R6	Device and network failure	Action plan: upgrading and implementing new technology. There must be a data backup procedure to minimize data loss.
R7	Cyber attacks	Action plan: transfer knowledge to new people on the team. Create a formal training plan for application use
R8	Management dynamics	Action plan: Create system automation in several activities, especially in activities that use critical and strategic applications such as elearning, SIAK, AIS. The specified knowledge sharing must be implemented by employees. Implement regular medical check ups for old employees, and medical check ups for new people.
R9	Problems with IT managers	Action plan: create a grand design related to mapping employee skills for the next 5 years. Develop innovation and maintain unique value. There is internal audit and risk-based management framework/based practice.

5. CONCLUSIONS

From the research results it can be concluded that:

1. Analysis of the internal environment and objective setting at the Faculty of Economics and Business, Palangka Raya University is used to see potential risk tendencies in conditions organizations as a basis for identifying and managing all TKTI risks.
2. The IT governance risk management design is in accordance with the COSO ERM framework with the implementation of risk identification, risk assessment and risk response components.

REFERENCES

Carayannis, E. G., & Morawska-Jancelewicz, J. (2022). The futures of Europe: Society 5.0 and Industry 5.0 as driving forces of future universities. *Journal of the Knowledge Economy*, *13*(4), 3445–3471.

Filippetto, A. S., Lima, R., & Barbosa, J. L. V. (2021). A risk prediction model for software project management based on similarity analysis of context histories. *Information and Software Technology*, *131*, 106497.

González-Gaya, B., Lopez-Herguedas, N., Bilbao, D., Mijangos, L., Iker, A. M., Etxebarria, N., Irazola, M., Prieto, A., Olivares, M., & Zuloaga, O. (2021). Suspect and non-target screening: the last frontier in environmental analysis. *Analytical Methods*, *13*(16), 1876–1904.

Gutterman, A. S. (2020). *Managing sustainability*. Routledge.

Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, Risk and Security Management (AI TRiSM): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*, 122442.

Hiles, A. (2012). Enterprise risk management. *The Definitive Handbook of Business Continuity Management*, 1–21.

Hill, M., Kalish, K., & Monts, J. (2023). Enterprise Risk Management. In *Working Capital Management: Concepts And Strategies* (pp. 433–451).

Li, M., Wang, H., Wang, D., Shao, Z., & He, S. (2020). Risk assessment of gas explosion in coal mines based on fuzzy AHP and bayesian network. *Process Safety and Environmental Protection*, *135*, 207–218.

Massingham, P. (2010). Knowledge risk management: a framework. *Journal of Knowledge Management*, *14*(3), 464–485.

Moloi, T., & Marwala, T. (2023). The Concept of Enterprise Risk Management. In *Enterprise Risk Management in the Fourth Industrial Revolution* (pp. 35–48). Springer.

Mousavi, S., & Gigerenzer, G. (2014). Risk, uncertainty, and heuristics. *Journal of Business Research*, *67*(8), 1671–1678.

Nani, D. A., & Ali, S. (2020). Determinants of Effective E-Procurement System: Empirical Evidence from Indonesian Local Governments. *Jurnal Dinamika Akuntansi Dan Bisnis*, *7*(1), 33–50.

Perera, A. A. S., Rahmat, A. K., Khatibi, A., & Azam, S. M. F. (2020). Review of literature: implementation of enterprise risk management into higher education. *International Journal of Education and Research*, *8*(10), 155–172.

Rao, A. (2009). Implementation of enterprise risk management (ERM) tools–a case study. *Academy of Accounting and Financial Studies Journal*, *13*(2), 87–103.

Ruslin, R., Mashuri, S., Rasak, M. S. A., Alhabsyi, F., & Syam, H. (2022). Semi-structured Interview: A methodological reflection on the development of a qualitative research instrument in educational studies. *IOSR Journal of Research & Method in Education (IOSR-JRME)*, *12*(1), 22–29.