Journal of Information System, Technology and Engineering
Volume 3, No. 1, pp. 417-421
E-ISSN: 2987-6117
http://gemapublisher.com/index.php/jiste
Received: January 2025
Accepted: February 2025
Published: March 2025

Drafting of IT Outsourcing Risk Management Policy Proposal with IT Outsourcing Risk Management Framework and Cobit

Afrizal Zein

Universitas Pamulang

Correspondence Email: dosen01495@unpam.ac.id

Abstract

The design of a proposed Information Technology (IT) outsourcing risk management policy is essential in facing the complexity and uncertainty associated with using third-party services. This policy aims to protect organisational assets, ensure operational continuity, and minimise the impact of risks that may arise from outsourcing relationships. In this study, we develop a risk management framework that integrates IT outsourcing risk management principles with the COBIT (Control Objectives for Information and Related Technologies) standard. This framework includes risk identification, analysis, mitigation, and continuous monitoring and evaluation. Through this approach, organisations can improve control and visibility of risks faced in IT outsourcing. The results of this study indicate that implementing a comprehensive risk management policy not only strengthens information security but also improves the effectiveness and efficiency of business processes involving IT outsourcing. Hopefully, this proposed policy can provide practical guidance for organisations in managing risks and maximising the value of IT outsourcing.

Keywords: risk management, outsourcing risk, risk mitigation, COBIT.

INTRODUCTION

Information technology (IT) supports various business activities in the rapidly developing digital era. Companies increasingly rely on IT solutions to improve operational efficiency, reduce costs, and improve customer service. However, with this increasing dependence, the risks associated with IT services are also increasingly complex and diverse. One approach organisations widely adopt is outsourcing, where companies transfer some or all of their IT functions to a third party. Although outsourcing can provide various benefits, such as cost savings and access to specialised expertise, it also brings new challenges in risk management. (ISACA, 2020).

Risk management in IT outsourcing is crucial, given the uncertainty arising from the relationship with the service provider. These risks can include, but are not limited to, data leakage, service disruption, and non-compliance with regulations. Therefore, a structured and comprehensive risk management policy is needed to identify, analyse, and mitigate these risks (Mardiyanto, T., & Susanto, A., 2021).

DOI: https://doi.org/10.61487/jiste.v3i1.130

One framework that has proven effective in IT management is COBIT (Control Objectives for Information and Related Technologies). COBIT guides quality IT management, control, and tools for evaluating and managing risk. By combining the IT outsourcing risk management framework with COBIT principles, organisations can design policies that meet business needs and ensure operational security and sustainability. (Gude, M., & Toft, K, 2021)

Outsourcing aims not only to share labour risks but also to become more complex. Michael F. Corbett, founder of The Outsourcing Institute and President Director of Michael F. Corbett & Associates Consulting Firm, said that outsourcing has become a management tool. Outsourcing is not only to solve problems but also to support business goals and objectives. Michael F. Corbett identified five strategic reasons (long-term benefits) and five tactical reasons (short-term benefits). The five most popular strategic (long-term benefits) reasons for outsourcing include increasing corporate focus, gaining world-class capabilities, accelerating the benefits of new technologies (re-engineering), sharing business risks, and using existing resources for more strategic activities. (Houghton, L., & Williams, A. 2023).

The decision to outsource IT services is based on two primary considerations. The first reason is that for most companies, IT is a means of supporting daily business activities. In other words, it would be more profitable for the company to outsource its IT management to a company with specialised expertise in IT. The second reason is based on the consideration that the costs of developing, maintaining, and managing IT assets are too high for the company to bear (Patel, R., & Joshi, A. 2023).

METHOD

This study adopts qualitative and quantitative approaches to understand IT outsourcing risks comprehensively. The qualitative approach is used to gain in-depth insights from various stakeholders through interviews, Focus Group Discussions (FGDs), and literature studies. In contrast, the quantitative approach measures the impact of risks by analysing survey data collected from employees in various departments. The literature study was conducted to understand the concepts of risk management, IT outsourcing, and COBIT principles, as well as to identify theories and best practices that have been implemented by other organisations in managing IT outsourcing risks.

Based on the results of risk identification, this study develops a risk management framework integrated with COBIT. This process includes risk analysis by categorising and evaluating the impact and probability using a risk matrix. Furthermore, mitigation strategies are developed to reduce, transfer, or accept the identified risks. Integration with COBIT ensures that all IT control and risk management aspects are met, thus creating a systematic approach aligned with international standards.

After the framework is developed, the next step is to create an IT outsourcing risk management policy. The policy document is designed to include the objectives, scope, and procedures to be followed in managing risks. The policy is then reviewed and validated through stakeholder discussions before being piloted on a small scale to assess its effectiveness. Feedback from the pilot phase is used to refine the policy before it is fully implemented in the organisation.

RESULT AND DISCUSSION

Risk Group Assessment

Risk group assessment is a systematic process for identifying, analysing, and categorising risks that an organisation may face, especially in IT outsourcing. This process is essential for understanding the nature, impact, and likelihood of occurrence of risks so that

DOI: https://doi.org/10.61487/jiste.v3i1.130

the organisation can take appropriate mitigation steps.

The risk analysis results show that HR Competence has the highest risk exposure value of 10.64, indicating that this factor significantly impacts the success of IT outsourcing. Meanwhile, Organizational Structure has the lowest risk exposure value of 4.00, indicating that the risks associated with this aspect are relatively more controlled than other factors. Suppose the risk exposure value of each risk is described in an RDS (Risk Dimension Signature). In that case, the resulting visual pattern will provide a comprehensive picture of the level of risk in each dimension analysed, helping formulate more targeted mitigation strategies.

To better understand the scale of priorities and the magnitude of efforts in designing solutions (mitigation), each risk's exposure value must be sorted from the highest to the lowest risk exposure value.

The business, legal, and technology risk assessments show that three risks are categorised at the extreme level. These risks include HR competency, changes in business processes and TDL, and data integrity. These risks have the highest probability of occurrence and a significant impact on the company. Therefore, handling these risks requires a more intensive mitigation strategy to reduce the potential for disruption to the company's operations.

In addition, there are ten risks categorised at the high level, where undesirable events have a high probability of occurring with a significant impact on the company. These risks include system quality, SOP, WAN support, migration strategy, business competition, auction procedure rules, application architecture, database, infrastructure, and server types. These risks still require serious attention in mitigation planning, although their impact is not as high as extreme risks.

Finally, three risks fall into the medium-level category: operating systems, interface systems, and organisational structures. Risks in this category are less likely to occur, and their impact on the company is insignificant. However, regular monitoring and evaluation are still needed so that these risks do not develop into more serious threats in the future.

From the results above, it can be seen that almost all respondents gave similar answers to the mapping results conducted by Tho (2005). This similarity is likely due to respondents' lack of understanding when completing the questionnaire, so they tend to follow the examples given. This indicates the need to improve respondents' knowledge of the questions so that the answers better reflect actual conditions and not just follow existing patterns.

COBIT Management Awareness Assessment

A questionnaire was distributed to determine the fulfilment level of the Detailed Control Objectives (DCO) COBIT in the third-party service management process, which will be used as a control recommendation at the risk group response stage. From the results of the answers of 43 respondents to Questionnaire V Management Awareness and the initial recapitulation results of the Questionnaire, a recapitulation can be made that describes the tendency of the level of fulfilment, performance, and achievements that are currently taking place for several question objects, both DCO fulfilment and indicators related to the third-party service management process in general.

DOI: https://doi.org/10.61487/jiste.v3i1.130

Table 1. Recapitulation Of Respondents' Answers in The Management Awareness Questionnaire

No	Question Object	Distribution of Answers		
		L (%)	M (%)	H (%)
1	Relationship Identification	16.28	69.77	13.95
2	Documentation	20.93	72.09	6.98
3	Relationship Management	32.56	55.81	11.63
4	Capability Assessment	23.26	65.12	11.63
5	Contracting	23.26	69.77	6.98
6	Risk Management	34.88	62.79	2.326
7	Security Agreements	16.28	65.12	18.60
8	Performance Monitoring	20.93	72.093	6.98
	Average	**23.55**	**66.57**	**9.88**

In general, the recapitulation of the results of the management awareness questionnaire in Table 1 shows a tendency that reflects the facts on the ground regarding the level of performance in the data management process. As many as 23.55% of respondents stated that performance in data management is still low or lacking, so significant improvement efforts are needed to achieve better standards. This shows that there are still challenges in the effectiveness of data management that must be addressed immediately to support business processes optimally.

Most respondents, namely 66.57%, stated that the performance of the data management process was at a sufficient or moderate level. Even though the data management system is running, there is room for improvement in information processing efficiency, reliability, and effectiveness. This majority perception reflects that companies must further evaluate data management procedures and policies to increase productivity and compliance with applicable standards.

Meanwhile, only 9.88% of respondents considered that the current data management practices were good and relatively met expectations. Although this figure shows that a few respondents are satisfied with the existing system, there is still an opportunity to improve the quality of data management to achieve higher standards. To get a clearer picture of the performance of the process, a mapping was carried out on the answers to the management awareness questionnaire with performance values that can quantitatively reflect the level of process achievement by the criteria set out in the DCO, as shown in Table 2.

Table 2. Mapping of Management Awareness Questionnaire Answers and Detailed Control Objectives (DCO) Performance Values/Levels in the Data Management Process

No	Answer	Performance Value	Performance Level
1	L (Low)	1,00	Less
2	M (Medium)	2,00	Medium
3	H (High)	3,00	Good

CONCLUSION

The design of a proposed IT outsourcing risk management policy that integrates the risk management framework with COBIT is a strategic step to face the challenges and complexities organisations face in the digital era. With increasing dependence on third-party services, the

DOI: https://doi.org/10.61487/jiste.v3i1.130

risks associated with IT outsourcing are also increasingly diverse, ranging from operational risks to reputational and compliance risks.

This study shows that a systematic approach to identifying, analysing, and categorising risks is key to developing an effective policy. Through various methods, including interviews, focus group discussions, and surveys, organisations can explore broader perspectives and understand risks that may have gone undetected.

The development of a risk management framework integrated with COBIT principles provides clear guidance for organisations to establish the controls needed to manage risks. By adopting best practices from COBIT, organisations can strengthen IT controls and increase transparency and accountability in managing outsourcing risks.

The proposed policy resulting from this study includes comprehensive and evidence-based mitigation measures and procedures for ongoing monitoring and evaluation. This is important to ensure the policy remains relevant and effective in changing business and technology dynamics.

Overall, this study significantly contributes to developing better risk management policies in IT outsourcing. Implementing this policy is expected to improve the security and sustainability of organizational operations, build stakeholder trust, and ultimately support the achievement of the company's strategic goals. In the future, further research is needed to explore the effectiveness of implementing this policy in various industry contexts and adapt it to ever-evolving technological innovations.

REFERENCES

ISACA. (2020). *COBIT 2019 Framework: Introduction and Methodology*. ISACA.

Mardiyanto, T., & Susanto, A. (2021). The Role of Risk Management in IT Outsourcing: A Literature Review. *Journal of Information Technology Management, 32*(1), 15-29.

Abubakar, M., & Rambo, R. (2022). Assessing Risks in IT Outsourcing: A Comparative Study. *International Journal of Business Information Systems, 39*(4), 275-293.

Houghton, L., & Williams, J. (2023). Integrating Risk Management Frameworks with COBIT: A Practical Approach. *Journal of Risk Management in Technology, 12*(2), 88-104.

Zainudin, Z. N., & Ibrahim, A. (2021). Managing Outsourcing Risks in the Digital Age: Strategies and Best Practices. *Information Systems Journal, 31*(3), 345-367.

Toh, M., & Li, L. (2020). A Framework for Effective Risk Management in IT Outsourcing. *Journal of Global Information Technology Management, 23*(2), 145-162.

Pratama, R. A., & Setiawan, B. (2023). Risk Assessment and Management in IT Outsourcing: A Systematic Review. *Journal of Technology Management, 15*(1), 55-74.

Kaur, A., & Sharma, S. (2021). Cybersecurity Risks in IT Outsourcing: Implications and Solutions. *International Journal of Cybersecurity Intelligence and Cybercrime, 4*(2), 45-60.

Haris, M., & Tanjung, B. (2022). Risk Management Practices in IT Outsourcing: A Review of the Literature. *International Journal of Information Systems and Project Management, 10*(3), 39-54.

DOI: https://doi.org/10.61487/jiste.v3i1.130