Journal of Innovation and Computer Science (JICS)
Vol. 2, No. 1, October 2025
https://journal.itqanpreneurs.com/index.php/jics/index

Information Technology Risk Management Analysis and Maturity Level Mapping at Darunnajah University Using Cobit 4.1 Framework

Aco Linggato[1], Fina Dwi Agustina[2], Muhammad Suhandar Sukma[3], Muhammad Arif[4]
[1] Information Systems and Technology Study Program, Darunnajah University, Indonesia. Email: aco@mhs.darunnajah.ac.id
[2] , Information Systems and Technology Study Program, Darunnajah University, Indonesia. Email: finadwi@mhs.darunnajah.ac.id
[3] Information Systems and Technology Study Program, Darunnajah University, Indonesia. Email: muhammadsuhandar7@gmail.com
[4] Information Systems and Technology Study Program, Darunnajah University, Indonesia. Email: zufarhanan123@gmail.com

Article History:
Received: 22-07-2025
Revised: 02-11-2025
Accepted: 03-11-2025

Keywords:
Risk Management, Maturity Level, COBIT 4.1 Framework.

How to Cite:
Linggato, A., Agustina, F. D. ., Sukma, M. S. ., Arif, . M. ., & Fawaid, A. . (2025). Information Technology Risk Management Analysis and Maturity Level Mapping at Darunnajah University Using Cobit 4.1 Framework. Journal of Innovation and Computer Science, 2(1), 18–23. https://doi.org/10.57053/jics.v2i1.126.

Abstract: *The rapid development of information technology today requires every company to continually evolve by adopting the latest technologies. On the other hand, the application of information technology requires substantial investment and poses a considerable risk of failure. Company conditions like this require consistency in managing the application of information technology. Therefore, companies need to implement risk management to identify potential risks when implementing information technology. The COBIT 4.1 framework is the framework that best suits the needs of the company because it ensures that information technology has been aligned with business processes, identifies risks, assesses risks, handles risks appropriately, maps maturity levels, and produces recommendations to be able to achieve targets that are in accordance with the company's wishes.*

Introduction

Information technology is an important element for a company to survive, compete, and achieve a competitive advantage. The use of information technology provides companies with solutions and operational, business, and financial benefits. The use of information technology also helps companies compete. However, in the use of information technology, there are always threats and risks that can interfere with the company's operational performance.

Some of the risks that usually arise when using information technology include virus attacks that can interfere with its performance, cracker attacks that can disrupt systems and even steal a company's confidential data, errors, and damage to supporting systems such as power grid failures, and so on. These risks must be managed and appropriately anticipated to avoid fatal losses.

When dealing with risks or threats, the company aims to reduce the likelihood of occurrence and overcome both frequent and rare risks. Judging from these problems, there is a need for information technology governance to address the risks that occur or have occurred.

One information technology governance framework that can help companies

manage risks is COBIT 4.1. The COBIT 4.1 framework allows companies to develop policies and best practices for information technology control. In supporting information technology governance, the COBIT 4.1 Framework ensures that information technology is aligned with business processes and information technology resources, and that information technology risks are handled quickly and appropriately.

Method

The methodology used in this study has several stages that need to be carried out, which are as follows

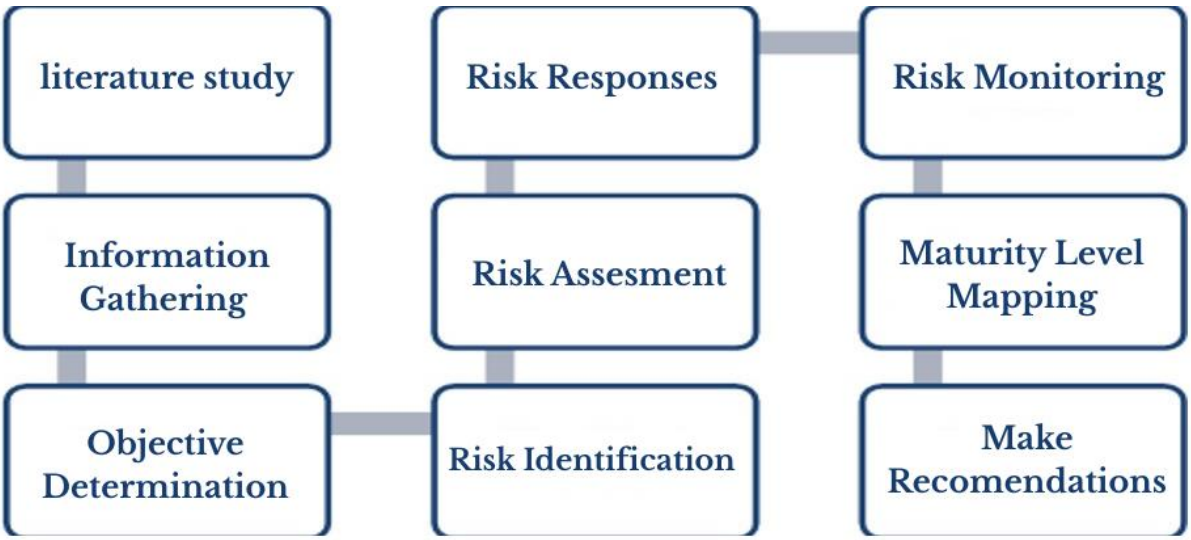

Figure 1. Research Methodology

First, Literature Studies. A literature review was conducted by searching the internet, books, and several journals on risk management, which will serve as a reference and theoretical basis for analyzing risk management at Darunnajah University. Second, Information Gathering. Deep. The information collection process has several stages carried out, which are as follows: (a). Observation. At this stage, direct observation was made at the research location to view the data related to materials needed in the preparation of the research; (b) Interview. At this stage, a question and answer process is carried out with the parties who are related to the application of information technology and information technology risk management; and (c) Questionnaire. At this stage, a random data collection process is carried out and distributed to several respondents. Data already collected will be used to analyze the risks at Darunnajah University.

Third, Setting Objectives. The principle in the COBIT 4.1 framework is to invest in information technology and to regulate and control information technology resources to meet the needs of Darunnajah University. To achieve this goal, seven appropriate information criteria are needed: Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance, and Reliability of information. Fourth, Identify Risks. This stage identifies risks that may occur during the implementation of information technology. Sources of risk often come from humans, internal and external parts of the company, disasters, computer viruses, system failures, errors in information technology selection, and problems in the development and implementation of systems.

Fifth, Risk Assessment. This stage assesses how frequently the risk occurs and its impact on the company. The impact of risk can be seen in terms of financial losses, a

declining company reputation, the suspension of ongoing operations, and even delays in decision-making. The tendency to risk is evident in the company's risk profile. The following table presents the level of risk impact and the tendency toward risk in the application of corporate information technology.

Table. 1 Impact of Risks and Trends That Occur

Level	Impact Risk (Impack)	Likelihood
5	Information systems in universities can maintain the accuracy and completeness of data	Strongly agree
4	Data damaged by a virus attack can be addressed immediately	Agree
4	There is a good mechanism in avoiding data loss due to technical faults (electricity, computer down)	Agree
3	Old, unused data is periodically managed and deleted	Neutral
5	Important information is protected from unauthorized access	Strongly agree
5	Have a security system against attempts to steal data by internal and external parties	Strongly agree
5	User passwords are stored and managed securely	Strongly agree
4	Lecturers and staff do not provide important information to outsiders carelessly	Agree
4	Information systems can be accessed at any time when needed	Agree
3	Disruptions such as power outages have been anticipated with adequate backups	Neutral
3	University hardware is protected from the risk of loss or damage	Neutral
3	System changes (application updates) are carried out according to the request of the relevant unit.	Neutral
4	The university has a formal policy on managing information technology risks	Agree
3	IT-related risks are identified and evaluated on a regular basis	Neutral
3	There are procedures in place to deal with incidents that disrupt information systems	Neutral
4	IT procedures have been documented and standardized	Agree
3	The use of information systems at Darunnajah University has been integrated with business processes	Neutral
4	Evaluation of the effectiveness of information systems is carried out regularly	Agree
3	The university already has a target for the development of information systems in the future	Neutral
4	The university conducts regular monitoring of the identified risks	Agree
3	Responses to IT incidents are carried out systematically and documented.	Neutral
4	The University has a strategic plan that is aligned with the vision and mission of the institution	Agree
3	The data backup and restore process is carried out according to the schedule and tested periodically	Neutral

Sixth, Risk response and monitoring. Risk response at this stage is to determine the process domain for risk management. The COBIT 4.1 domain processes related to risk management are: PO1 (Defines a Strategic IT Plan), PO9 (Assess and Manage Risk), AI6 (Manages Change), DS5 (Ensure System and Security), DS11 (Manage Data), and ME1 (Monitor and Evaluate IT Performance). Meanwhile, at the risk monitoring stage, it serves to ensure that risks and responses are continuously maintained and aligned with the company's desired targets.

Seventh, Maturity Level Mapping. At this stage, it is necessary to assess the company's current maturity in applying information technology, identify the desired maturity level, and determine the gap between the current and desired maturity levels. Eight, make recommendations. At this stage, the company will receive several recommendations, stages, and processes for implementing information technology to achieve its target.

Result and Discission

Risk Measurement and Evaluation of IT Maturity Level

Based on data from observations, interviews, and questionnaires with related parties at Darunnajah University, several information technology risks have been well identified. The questionnaires covered various aspects, including information security, data management, system integrity, and IT incident readiness. The risk assessment table shows that respondents score high on aspects such as protecting critical information, managing passwords, and protecting against data theft. For example, the indicators "Important information is protected from unauthorized access" and "User passwords are stored and managed securely" get the highest scores (5 – Strongly Agree). This indicates that the institution has implemented an adequate information security system.

However, several indicators still have a neutral score (3), including old data management, system backup, and IT incident handling. This shows that there are potential risks that have not been handled optimally and need to strengthen their policies and operational procedures.

Maturity Level Mapping Using COBIT 4.1

Using the maturity level scale in COBIT 4.1, a mapping of IT processes at Darunnajah University was conducted. The results show that most domains are at the Defined (3) and Managed (4) levels. By scale: Level 3 (Defined): The process has been documented and standardized, but has not been fully implemented, and Level 4 (Managed): Processes have been regularly monitored, measured, and evaluated. No domains were found at level 3 or below, indicating that the University is mature enough to manage IT, even though it has not reached the highest level of Optimized (5).

Relevance of Findings and Theoretical Implications

These findings align with the theory put forward by Weill & Ross (2004), which holds that effective IT governance will improve the efficiency of business processes and reduce the Risk of losses from system disruptions. The COBIT 4.1 framework effectively helps identify and control risks, and encourages institutions to improve IT management in a structured and sustainable manner. In addition, these results reinforce the importance of collaboration between IT units and strategic management in developing long-term technology plans aligned with the institution's vision. This also aligns with the PO1 (Define a Strategic IT Plan) and PO9 (Assess and Manage Risk) domains in COBIT 4.1.

Table 1. Descriptive Statistics

N	20
Minimum	44
Maximum	115
Mean	84.94737
Std. Deviation	18.15817442

Source: proceed

Table 2. Scale and Model Maturity Level

Scale	Model Maturity Level
4.51-5.00	5-Optimized
3.51-4.50	4-Managed
2.51-3.50	3-Defined
1.51-2.50	2-Repeatable
0.51-1.50	1-Initialization
0.00-0.50	0-None (non-existent)

Discussion

The findings of this study indicate that the implementation of information technology risk management at Darunnajah University has reached a high level of maturity, with most domains at the Defined and Managed level according to the COBIT 4.1 maturity model. This shows that information technology processes have been documented, standardized, and monitored regularly.

Theoretically, these findings align with the view of Weill and Ross (2004), who stated that effective IT governance can improve an organization's ability to anticipate risks, increase efficiency, and create added value through integration of technology and business strategies. The application of the PO1 (Define a Strategic IT Plan) and PO9 (Assess and Manage IT Risk) domains in the COBIT 4.1 framework has been proven to support the systematic identification and control of risks.

Furthermore, management's awareness of the importance of data security systems, protection against unauthorized access, and password management demonstrates the organization's level of maturity in dealing with increasingly complex information technology threats. However, there are still some weaknesses, especially in incident management, legacy data management, and backup mechanisms, which tend to receive neutral ratings from respondents. This shows that the process of strengthening policies and implementing SOPs (Standard Operating Procedures) still needs improvement to reach the optimized level.

The practical implications of these results include the importance of increased socialization of IT policies, regular training for relevant staff, and periodic audits and evaluations of all IT processes to ensure the sustainability and adaptability of systems to new risks.

Conclusion

This study concludes that the implementation of information technology risk management at Darunnajah University using the COBIT 4.1 framework has reached a high level of maturity, particularly in information security and process alignment with the established standards. Maturity level mapping shows that the organization has reached the *Defined* until *Managed* stage, indicating fairly good documentation and monitoring. However, some areas still need improvement, such as incident management, data backup, and full integration with business processes. Therefore, it is recommended that institutions make continuous improvements, such as improving IT HR training, reviewing risk policies, and periodically monitoring the effectiveness of the controls implemented. Overall, the COBIT 4.1 framework has proven to be a practical approach for assessing and managing IT risks and for providing strategic direction in developing information

systems aligned with the goals of higher education institutions.

Acknowledgements

The author would like to thank Darunnajah University for providing support and opportunities to conduct this research, as well as the staff and lecturers who have been willing to serve as respondents and resource persons in the interview process and in completing the questionnaire. Thanks are also extended to the academic supervisors who have provided direction during the preparation of this report, as well as all unnamed parties who have contributed to the completion of this research.

Reference

ISACA. (2009). *The Risk IT Framework*. www.isaca.org

Kosasi, S., Vedyanto, & Yuliani, I. D. A. E. (2017). Maturity levels of academic information services of higher education using IT governance. *Proceedings of 2017 4th International Conference on New Media Studies, CONMEDIA 2017*, *2018-January*, 56–61. https://doi.org/10.1109/CONMEDIA.2017.8266031

Mukaromah, S., & Putra, A. B. (2016). Maturity level at university academic information system linking it goals and business goal based on COBIT 4.1. *MATEC Web of Conferences*, *58*. https://doi.org/10.1051/matecconf/20165803009

Setyadi, R., & Anggoro, S. (2021). Risk Management Analysis Using COBIT 4.1 and Vehicle Testing Management Information System. *Journal of Informatics and Information Systems Engineering*, *7*(1), 231–239. https://doi.org/10.28932/jutisi.v7i1.3419

Spremic, M., & D, P. (2008). Emerging issues in IT Governance : implementing the corporate IT risks management model. *Wseas Transactions On Systems*, *7*(3), 219–228.

Sukoco, I. W., Hermadi, I., & Sasongko, H. (2021). Sipadu Maturity Level Evaluation Using Cobit 4.1: Case Study of Geospatial Information Agency. *Journal of Business and Management Applications*, *7*(1), 179–187. https://doi.org/10.17358/jabm.7.1.179

Surbakti, H. (2014). *Cobit 4.1: A Maturity Level Framework For Measurement of Information System Performance (Case Study: Academic Bureau at Universitas Respati Yogyakarta)*. *3*(8), 999–1004.