



Preventive Efforts and Risk Management in Information Technology Using COBIT 5

Sarmini¹, Agung Prasetyo², Satria Pandu Adipurwoko³

¹Department of Information System, Faculty of Computer Science, Universitas Amikom Purwokerto, Purwokerto, Indonesia, sarmini@amikompurwokerto.ac.id

²Department of Information System, Faculty of Computer Science, Universitas Amikom Purwokerto, Purwokerto, Indonesia, pras@amikompurwokerto.ac.id

³Department of Information System, Faculty of Computer Science, Universitas Amikom Purwokerto, Purwokerto, Indonesia, satriapandu20@gmail.com

ABSTRACT

Amikom University Purwokerto has implemented IT across its academic civitas but so far the risk management related to IT implementation has not been implemented optimally. This is demonstrated by the absence of guidelines and major references that should be used as a determination standard in addressing the various risks faced and also the lack of risk monitoring of IT implementation to ensure the procedure of risk management is well executed. Therefore, it is necessary to do measurement/assessment related to the management and optimization of the risk of IT implementation at Amikom University Purwokerto. One of the frameworks that can be used to evaluate IT risk management is COBIT 5, especially on EDM03 (Ensure Risk Optimization) and APO12 (Manage Risk) process domain, which discuss in detail on IT risk management. The objective of the research is to measure the level of subdomain capability of the EDM03 and APO12 processes to find out and ensure the extent of the risk optimization and risk management process related to IT implementation at Amikom University Purwokerto. The result of capability level measurement shows the capability level of both the process domain is at level 1 (Performed Process). To achieve the target level of expected capability, UPT IT of Amikom University Purwokerto needs to carry out the process of risk management related to IT based on recommendations which have been obtained from this study.

Key words: Risk, COBIT 5, EDM03, APO12.

1. INTRODUCTION

Application of Information Technology (IT) can help companies in obtaining, managing, processing, compiling, storing and manipulating data and information effectively and efficiently [1]. In addition to providing benefits for companies, the application of IT can also increase negative risks to the goals of a company [2] and pose risks that can harm the organization/company [3]. Risk is an unexpected

event that can cause bad consequences / losses [4]. In order not to hamper the achievement of the company's goals IT implementation must be free of risks[5]. IT implementation risks can be minimized by appropriate and relevant IT risk management [1]. Risk management in implementing IT is good in being able to have a good impact on the organization [6].

Amikom University Purwokerto so far has not optimally carried out risk management in IT implementation, this is indicated by the absence of guidelines and main references that must be used as a standard determination in dealing with various risks faced and also the absence of IT implementation risk monitoring to ensure management procedures the risk has been carried out well. This shows that Amikom Purwokerto University has not seriously considered the problems and risks that may occur related to IT implementation that can harm the organization / company. The likelihood of risk occurrence can be anticipated and reduced by conducting an IT risk management analysis [7]. An assessment of IT risk management implementation is needed so that the company's goals and objectives have been set [8] and minimize the risks that may occur [9]. IT risk management evaluation is one way to measure the achievement of the application of IT risk management that can be done by measuring the level of capability, gap analysis and risk assessment. Measuring management capability and risk optimization related to IT implementation can improve IT implementation risk management [3]. Measuring the level of IT risk management capabilities results in a recommendation and mitigation strategy that supports the achievement of capabilities related to IT risk management [10] and evaluation materials for the company so that the stated goals and objectives of the company can be achieved [8].

Control Objectives for Information and related Technology (COBIT) is an IT management practice standard used to help auditors, stakeholders and management, and users to bridge the gap between business risk, control needs and technical issues [11]. The COBIT 5 framework assists companies in creating optimal value from IT by maintaining a balance between the realization of benefits, risk optimization, and resource optimization [12]. IT risk management can be

measured using COBIT 5 capability levels, conducting gap analysis and providing recommendations in the form of corrective steps to achieve the expected IT risk management and the level of failure / loss that can be minimized [3]. There are 2 (two) process domains in COBIT 5 that specifically address IT risk management, namely the EDM03 and APO12 process domains [10][3]. Therefore this research is focused on EDM03 (Ensure Risk Optimization) and APO12 (Manage Risk) domains related to IT risk management. In detail, the EDM03 domain ensures that the risks associated with IT do not exceed risk appetite and tolerance, companies can identify, manage and minimize the potential failure of the impact of IT risks. As for the APO12 domain, it discusses the integration and balance of costs and benefits of managing IT related companies [13]. Risk optimization aims to make the company able to manage, assess and reduce risks associated with IT properly and ensure that the company has a risk appetite and tolerance that is understood and continuously [14]. The research conducted aims to determine the extent of management capability and risk optimization of IT implementation at the University of Amikom Purwokerto.

2. METHODS

In this study through several stages, the following stages of problem solving are presented in the research framework (figure 1).

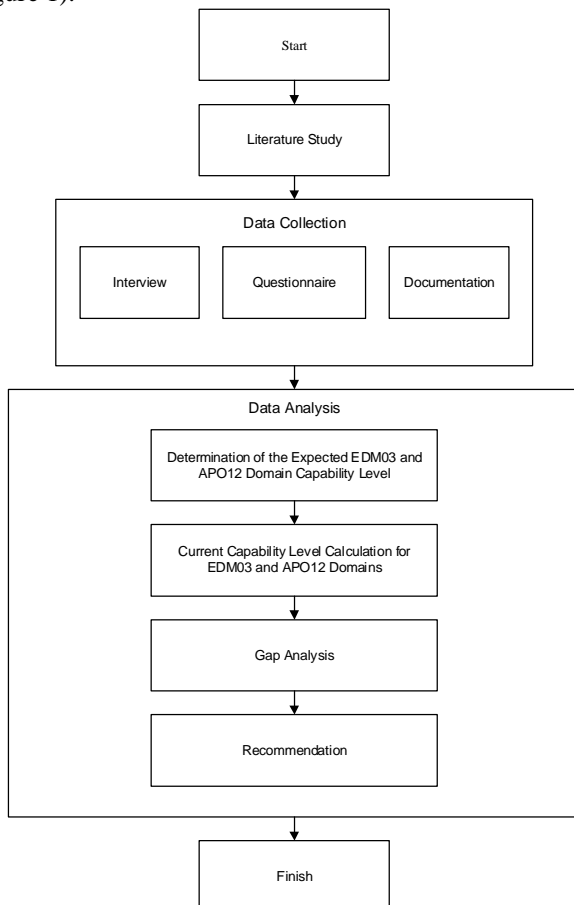


Figure 1: Research Framework

Description:

- a. Study of literature
Literature studies are carried out to explore information related to research carried out by searching and studying reference books, journals, articles and information from the internet and other media.
- b. Data collection
This stage is done to collect data needed in research. In this research, data collection was carried out using several data collection techniques, namely: interviews, questionnaires and documentation.
- c. Determination of the expected capability level
At this stage done to determine the level of capabilities expected by the company / organization.
- d. Current capability level calculation.
The current capability level calculation phase is carried out by using an average calculation formula for interview data and filling out questionnaires with interested parties at Amikom University, Purwokerto. The value calculation for each Key Management Practice (KMP) uses the following calculation formula [15]:

$$KMP = i \times 100 / h$$

Description:

i = Number of outcomes that have existed

j = Number of outcomes for each KMP

And the calculation of Average Score for each COBIT 5 Process:

$$\text{Average Score} = ((X1 + X2 + X3 + X4 + X5 + Xn)) / Y$$

Description:

Xn = Total value of each KMP

Y = Number of KMP

While in the assessment at each level, the results will be classified in 4 categories as follows (ISACA, 2012d):

- 1. N (Not achieved)
This category shows that there is little evidence of the attainment of process attributes with ranges of values ranging from 0-15%.
- 2. P (Partially achieved)
This category shows that there is some evidence about the approach and achievement of attributes with a range of values ranging from 15-50%.
- 3. L (Largely achieved)
This category shows evidence of a systematic approach and significant achievements, although there may still be weaknesses but they are not significant. The range of values achieved in this category ranges from 50-85%.
- 4. F (Fully achieved)
This category shows there is evidence of a systematic and complete approach, and full achievement and no weaknesses related to the attributes of the process with the range of values achieved in this category ranging from 85-100%.

e. Gap analysis

The gap analysis phase is the stage carried out to determine the gap between the current capability level and the expected capability level in the EDM03 and APO12 domains. To find out the gap is done by calculating the difference between the level of capability currently achieved with the expected level of capability.

Recommendations, after calculating the current capability level and knowing the gap analysis of each domain, the next step is to make recommendations for better IT risk management and be able to achieve the expected capability level based on the results of the analysis conducted on the EDM03 process domain and APO12.

3. RESULT AND DISCUSSION

3.1 Mapping Enterprise Goals

The first step is to identify the company's goals in accordance with the COBIT 5 framework that has been developed using the Balanced Scorecard (BSC) dimension. The mapping results can be seen in table 1.

Table 1: COBIT 5 Mapping Results

Problems	Enterprise Goals
1. Do not have the main guidelines and references that must be used as a standard for determining strategies in dealing with various risks associated	3. Managed business risk (safeguarding of assets) (Management of business risks, especially security of assets)

with IT implementation
 4. There is no monitoring of the implementation of risk management to ensure risk management procedures related to IT implementation.
 5. Compliance with internal policies

3.2 Mapping Enterprise Goals to IT-Related Goals

After the results of the enterprise goals mapping are found, then the IT-related goals mapping is conducted. The results of mapping IT-related goals can be seen in table 2.

Table 2: COBIT 5 Mapping Results Enterprise Goals to IT-Related Goals

No	IT-Related Goals
02	IT compliance and support for business compliance with external laws and regulations
04	Managed IT-Related business risk
10	Security of information, processing infrastructure and applications
15	IT compliance with internal policies
16	Competent and motivated business and IT personnel

3.3 Mapping IT-Related Goals to Processes

The IT-related goals to processes mapping is to map IT-related goals to the process domains in COBIT 5.

COBIT 5 Process			IT-related Goal																	
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	
Evaluate, Direct and Monitor	EDM01	Ensure Governance Framework Setting and Maintenance	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S	S
	EDM02	Ensure Benefits Delivery	P		S		P	P	P	S			S	S	S	S		S	P	
	EDM03	Ensure Risk Optimisation	S	S	S	P		P	S	S		P			S	S	P	S	S	
	EDM04	Ensure Resource Optimisation	S		S	S	S	S	S	S	P		P		S			P	S	
	EDM05	Ensure Stakeholder Transparency	S	S	P			P	P						S	S	S			S
				Financial					Customer			Internal					Learning and Growth			
Alignment of IT and business strategy																				
IT compliance and support for business compliance with external laws and regulations																				
Commitment of executive management for making IT-related decisions																				
Managed IT-related business risk																				
Realised benefits from IT-enabled investments and services portfolio																				
Transparency of IT costs, benefits and risk																				
Delivery of IT services in line with business requirements																				
Adequate use of applications, information and technology solutions																				
IT agility																				
Security of information, processing infrastructure and applications																				
Optimisation of IT assets, resources and capabilities																				
Enablement and support of business processes by integrating applications and technology into business processes																				
Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards																				
Availability of reliable and useful information for decision making																				
IT compliance with internal policies																				
Competent and motivated business and IT personnel																				
Knowledge, expertise and initiatives for business innovation																				

Figure 2: Mapping IT-related Goals to Processes



3.4 Calculation of Capability Level

A. Process domain EDM03 - Ensure Risk Optimization

in the EDM03 process domain are presented in the table below:

The results of a summary calculation of the level of capability

Table 3: Summary of Achieving the Capability Level of the EDM03 Process Domain

Goals	Ensuring that company risks related to IT do not exceed risk appetite and risk tolerance, the impact of IT risks on company value is identified and managed, and the potential for compliance failure is minimized.									
Process (<i>Ensure Risk Optimization</i>)	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5				
		PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Rating based on percentage	100%	0%								
Color based rating										

Based on the table 3 above shows the achievement of the capability level in the EDM03 process domain of IT implementation at Amikom University Purwokerto is at level 1 with a status not achieved with a value of 0% so that the calculation cannot proceed to the next level because at level 1 there are still a number of requirements that have not been met. The following are activities on IT risk management EDM03 process domain at UPT IT of Amikom University, Purwokerto:

The EDM03 process domain conditions that have been carried out at the UPT IT of the University of Amikom Purwokerto:

1. There is an act of reporting IT risks from the user to the UPT IT directly (verbally).
2. The handling and classification of IT risk levels at UPT IT in Amikom Purwokerto University has been carried out based on intuition from UPT IT itself.



The condition of the EDM03 process domain that has not been implemented at the UPT IT of Amikom University Purwokerto:

1. Lack of identification and communication of risk thresholds related to key IT risks.
2. The absence of standards in risk management makes risk management related to IT less effective and efficient.
3. The absence of identification and management related to the impact of IT risk on Amikom Purwokerto University which is used as a risk determination in relation to IT does not exceed risk appetite.

b. APO12 process domain - Manage Risk

The results of a summary calculation of the level of capability in the APO12 process domain are presented in the table below:

Table 4: Summary of Achieving the Capability Level of the APO12 Process Domain

Goals	Integrate enterprise risk management related to IT with overall ERM, and balance the costs and benefits of managing IT related company risk									
Process (<i>Manage Risk</i>)	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5				
		PA.	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
Rating based on percentage	100%	0%								
Color based rating										

Based on the table 4 above shows the achievement of the capability level in the APO12 process domain of IT implementation at Amikom University Purwokerto is at level 1 with a status not achieved with a value of 0% so that the calculation cannot proceed to the next level because at level 1 there are still a number of requirements that have not been met. The following are activities on IT risk management in the APO12 process domain at UPT IT, Amikom University, Purwokerto:

The conditions of the APO12 process domain that have been implemented at the UPT IT of the University of Amikom Purwokerto:

1. There is an act of reporting IT risks from the user to the UPT IT directly (verbally).
2. The handling and classification of IT risk levels for UPT IT in Amikom Purwokerto University has been carried out based on intuition from the IT department itself.

The condition of the APO12 - Manage Risk domain that has not been implemented at the UPT IT of the University of Amikom Purwokerto:

1. Lack of identification, analysis, management of IT-related risks.
2. There is no complete risk profile documentation.

3. There is no management and control of risk management measures.

3.5 Recommendations

Based on the results of the gap analysis in the EDM03 and APO12 process domains of IT implementation at the University of Amikom Purwokerto, it can be concluded that there is no identification, analysis, and management of IT-related risks and identification of documented risk impacts into a complete risk profile. So the risk management process becomes less effective and efficient. Recommendations that can be made are that the IT UPT at the University of Amikom Purwokerto needs to carry out a risk management process related to IT by referring to ISO 31000 standards that provide principles, frameworks and risk management processes that can be used as risk management architecture in an effort to ensure the effective application of risk management [16][17][18].

For risk management to work properly, a risk management framework is needed. This framework will be the basis and arrangement which covers all risk management activities at the organizational level. This framework will assist UPT IT at Amikom Purwokerto University in managing risks effectively, ensuring complete and adequate risk information that will be reported and used as a basis for decision making. In implementing the risk management framework, UPT IT should [19][20][21]:

1. Establish the right strategy and time to implement this framework.
2. Apply risk management policies and risk management processes to organizational processes.
3. Comply with all applicable laws and regulations.
4. Document the decision making process, including the process of setting targets that are consistent with the results of the risk management process.
5. Carrying out risk management awareness raising and training.
6. Communicate and consult with stakeholders to ensure that the risk management framework is appropriate and effective.

4. CONCLUSION

Based on the calculation of the capability level in the EDM03 and APO12 process domains at Amikom University, Purwokerto is at level 1 (Performed Process)[23][24]. To achieve the expected capability level target, UPT IT of Amikom Purwokerto University needs to carry out IT-related risk management processes based on the recommendations obtained from this study. And for consideration, Amikom University Purwokerto needs to do strategic planning related to IT implementation to create good IT governance in IT related business processes.

ACKNOWLEDGEMENT

The authors would like to thank the financial support from Department of Information System, Faculty of Computer

Science, and Institute of Research and Community Service Universitas Amikom Purwokerto.

REFERENCES

1. F. T. Riadi, A. D. Manuputty, and A. Saputra, “Evaluasi Manajemen Risiko Keamanan Informasi Dengan Menggunakan COBIT 5 Subdomain EDM03 (Ensure Risk Optimisation) (Studi Kasus : Satuan Organisasi XYZ – Lembaga ABC),” JUTEI, vol. 02, no. 1, pp. 1–10, 2018.
2. N. D. Setyaningrum, Suprpto, and A. Kusyanti, “Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5 (Studi Kasus : PT . Kimia Farma (Persero) Tbk – Plant Watudakon),” J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 1, pp. 143–152, 2018.
3. N. Z. Firdaus and Suprpto, “Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT . Petrokimia Gresik),” J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 1, pp. 91–100, 2018.
4. H. Darmawi, **Manajemen Risiko. 2 ed.** Jakarta: PT. Bumi Aksara, 2016.
5. N. M. Rahmania, Suprpto, and A. R. Perdanakusuma, “Penilaian Kapabilitas Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Cobit 5 (Studi Kasus : Daerah Operasional (DAOP) XX),” J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 12, pp. 6828–6836, 2018.
6. R. E. Putri, “Model Penilaian Kapabilitas Proses Optimasi Resiko TI Berdasarkan COBIT 5,” *Semin. Nas. Inform.*, pp. 252–258, 2015.
7. G. M. Husein and R. V. Imbar, “Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT . Jabar Telematika (JATEL),” *J. Tek. Inform. dan Sist. Inf.*, vol. 1, no. 2, pp. 75–87, 2015. <https://doi.org/10.28932/jutisi.v1i2.368>
8. Y. I. Putri, Suprpto, and A. D. Herlambang, “Penilaian Kapabilitas Penerapan Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi pada PDAM Kota Malang Jawa Timur),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4855–4862, 2018.
9. R. Puspita, Murahartawaty, and E. K. Umar, “Perancangan Manajemen Risiko Teknologi Informasi Pada Core Processes EDM03 Dan Key Supporting Processes EDM01, EDM02, dan EDM05 Menggunakan Framework COBIT 5 (Studi Kasus : Dinas Komunikasi dan Informatika Pemerintah Kota Bandung),” in *e-Proceeding of Engineering*, 2016, vol. 3, no. 2, pp. 3255–3262.
10. M. H. Arief and Suprpto, “Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi Kasus Pada Perum Jasa Tirta I Malang),” *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 1, pp. 101–110, 2018.

11. ISACA, **COBIT 5 : A Business Framework for the Governance and Management of Enterprise IT**. USA: ISACA, 2012.
12. M. D. Rahmatya, A. Hadiana, and I. Maliki, “**Pengukuran Manajemen Risiko TI di PT. X Menggunakan COBIT 5,**” *J. Tata Kelola dan Kerangka Kerja Teknol. Inf.*, vol. 2, no. 1, 2016.
13. ISACA, **COBIT 5: For Risk**. Rolling Meadows: ISACA, 2012.
14. ISACA, **COBIT 5: Process Assessment Model (PAM): Using COBIT 5**. 2013.
15. A. M. Y. Amin, I. Hermadi, and Y. Nurhadryani, “**Evaluasi Penerapan Manajemen Teknologi Informasi Menggunakan COBIT Pada Unit Arsip IPB,**” *J. Pustak. Indones.*, vol. 15, no. 1, 2016.
16. ISO, **ISO 31000 Risk Management - Principles and Guidelines**. 2009.
17. Hariguna, T., Adiandari, A. M., & Ruangkanjanases, A. (2020). Assessing customer intention use of mobile money application and the antecedent of perceived value, economic trust and service trust. *International Journal of Web Information Systems*.
<http://doi.org/10.1108/IJWIS-12-2019-0055>
18. Hariguna, T., & Ruangkanjanases, A. (2020). Elucidating E-satisfaction and Sustainable Intention to Reuse Mobile Food Application Service, Integrating Customer Experiences, Online Tracking, and Online Review, *XXIX*, 122–138.
<http://doi.org/10.24205/03276716.2020.704>
19. Hariguna, T., Rahardja, U., & Ruangkanjanases, A. (2020). The impact of citizen perceived value on their intention to use e-government service: An empirical study. *Electronic Government, an International Journal*, 16(1), 1. <http://doi.org/10.1504/eg.2020.10028551>
20. Hariguna, T., Maulana, W., & Nurwanti, A. (2019). Sentiment Analysis of Product Reviews as A Customer Recommendation Using the Naive Bayes Classifier Algorithm. *International Journal of Informatics and Information Systems*, 2(2), 48–55.
21. Imron, M., Hasanah, U., & Humaidi, B. (2020). Analysis of Data Mining Using K-Means Clustering Algorithm for Product Grouping. *International Journal of Informatics and Information Systems*, 3(1), 12–22.
22. Hariguna, T., & Rachmawati, V. (2019). Community Opinion Sentiment Analysis on Social Media Using Naive Bayes Algorithm Methods. *International Journal of Informatics and Information Systems*, 2(1), 33–38.
23. Santiko, I., & Subarkah, P. (2019). Comparison of Cart and Naive Bayesian Algorithm Performance to Diagnose Diabetes Mellitus. *International Journal of Informatics and Information Systems*, 2(1), 9–16.
24. Hariguna, T., Hung, C., & Sukmana, H. T. (2019). The antecedent of citizen intention use of e-government service. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 17(1), 202–209.
<http://doi.org/10.12928/TELKOMNIKA.v17i1.11588>