E-Government Risk Optimization Capability Measurement

Anita Wulansari[1*], *Carena Learns* Prasetyo[2], *Siti* Mukaromah[3] , *Dhian Satria Yudha* Kartika [4], *Eristya Maya* Safitri[5] and *Abdul Rezha Efrat* Najaf[6]

[1,2,3,4,5,6] Information System Department, Universitas Pembangunan Nasional Veteran Jawa Timur, Surabaya , Indonesia

Abstract. Bureau XYZ strived to facilitate the realization of good governance through electronic government (e-government). There were various information systems that were implemented as part of this effort, one of which was the mail management information system. Bureau XYZ has implemented an Information Security Management System (ISMS) using ISO 27001:2013 standards. Nevertheless, optimization and management of information technology risks were necessary to ensure that the implementation of the software was in accordance with the capabilities and objectives of the organization. Therefore, it was necessary to measure the capability level to determine the actions that need to be taken to improve information security risk management in implementing the software. This study aimed to obtain the capability level of the mail management information system's information security risk management process, find out the gap between the actual and desired capability level and provide recommendations for improvement according to COBIT 5. This study measured the EDM03-Ensure Risk Optimization process. The assessment results showed that the EDM03 process was at Level 1 (Performed) and had a gap value of 2 from the desired capability level, Level 3 (Established). Recommendations for improvement were also included in this study to help the organization achieve the desired level based on the assessment results, list of findings, and validation of work products.

Keywords: E-government, risk optimization, capability

1 Introduction

Technology-based service implementation within government organizations is beneficial to both government and citizens, especially in this current pandemic era [1]. The benefits may vary from government service availability [2], public participation improvement and regulation transparency [3]. However, e-government implementations were not always carried out as expected. Some possible risks and threats may arise and harm the organization [4]. Therefore it was important for the organization to manage the risks to minimize the impact of the risks [5]. Information security risk management is a systematic and continuous process of analysis and monitoring of the IT environment, which aims to reduce the possibility of unexpected results and minimize the emergence of threats due to unmanaged information important for the organization [6].

As one of the governmental institutions, Bureau XYZ was responsible for managing information in one of the five largest cities in Indonesia. One of the applications owned by Bureau XYZ is the mail management information system. This software was used to assist correspondence activities, including the disposition of letters to the intended party. To realize good governance through electronic government (e-government), Bureau XYZ has established an SOP and conducts periodic monitoring and evaluation of the implementation of SOPs related to this software. However, the software has experienced data loss or mail disposition errors due to deficient server performance or user error.

Bureau XYZ knew more action was needed than just establishing regulations or SOPs to minimize risk to optimize risks that may occur in the future. Therefore, it is necessary to measure the level of capability to determine the extent to which risk management, especially in IT-related information security, has been carried out so that it can conclude whether it has been effectively implemented [7]. A standard base practice needs to be applied to measure the capability to analyze the optimization of information security risk management that has been implemented and be a guide for managers. Therefore, this study used COBIT 5 to measure the level of risk management optimization capability of the software application in Bureau XYZ.

2 Research Methods

This research was developed using the COBIT 5 approach, as shown in Fig 1. The methodology below shows the step-by-step of this research. There were four

* Corresponding author : anita.wulansari.sisfo@upnjatim.ac.id

stages in the research method: COBIT goals cascade analysis, RACI Chart mapping in organization, data and evidence collection, and capability level and gap analysis.

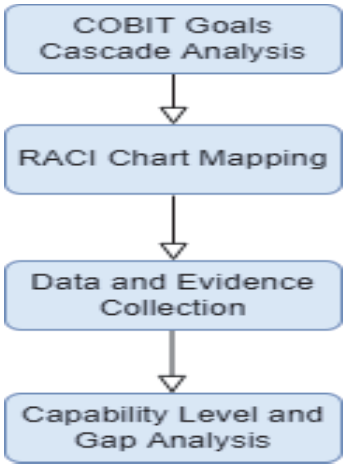

Fig. 1. Research Methodology

The first step was stakeholder drivers, stakeholder needs, enterprise goals, IT-related goals and enabler goals analysis. The output of this stage was the e-government process that will be prioritized for audit [8]. s the core of COBIT 5, COBIT Goals Cascade Analysis interpreted stakeholder needs into business and IT-related objectives, generating processes and activities that would be prioritized for assessment [9]. The requirements 'mapping' for this purpose was the key to supporting alignment between enterprise requirements and IT solutions and services [10].

The collection of data and evidence was carried out by interviewing the selected respondents. Respondents who were interviewed were determined by the RACI method. In this study, only the role of R (Responsible) will be the resource person for data collection because this role was responsible for the activities of the IT process directly, so this role became the most abundant and accurate source of information and data sources [11] [12].

The last stage was capability level and gap analysis. The process capability level measurement was done based on the findings of information and documentary evidence collected from the results of interviews and observations that have been made. In this stage, each base practice and work product value was determined using the N-P-L-F level rating in which N score was 0-15%, P score was 15-50%, L score was 50-85% and F score was 85-100%. Then the base practice percentage value was calculated by dividing base practice score by total base practice, while the work products percentage value was calculated by dividing the work products score by total work products. The calculation results would then determine the extent of the capability level and its category in the N-P-L-F level rating [13].

Gap analysis is a process of evaluating the performance of the company's internal management to help measure the quality of the company. By doing this, an organization can identify where gaps are and what differences exist between an organization's current situation and "what ought to be" in place. The gap value was obtained by calculating the difference between the desired level and the actual level. The smaller the gap, the better the performance quality of the company or agency. The desired capability level of Bureau XYZ was Level 3. The gap value in this research was obtained from the difference between the expected rating level percentage and the actual rating level percentage.

After getting the gap value, an improvement strategy was carried out based on what Bureau XYZ has not achieved, according to the percentage generated in the previous stage. As a part of the improvement strategy, some recommendations would be given based on the EDM03 processes from COBIT 5. Bureau XYZ should heed the proposed recommendations to achieve the desired security risk management capability level of the mail management information system.

3 Result and Discussion

3.1 COBIT Goals Cascade Analysis

The stakeholder needs question related to optimizing risk management was "Is the information I am processing well secured?" and focused on EG15's enterprise goal, namely compliance with internal policies. Based on the results of the mapping between enterprise goals and IT-related goals, there were three selected IT goals, including IT compliance and support for business compliance with external laws and regulations, security of information, processing, infrastructure, and application and IT compliance with internal policies. The selected IT-Related Goals were those with a P (Primary) scale, which means that these points play an essential role in supporting the company's goals. The results of the mapping showed that among those three IT objectives, IT-Related Goals number 10: security of information, processing, infrastructure, and application, was selected because it was the most suitable for this case. After deciding on the appropriate IT goals to be used in this research, the selected IT-Related Goals were re-mapped into the processes in COBIT 5. The mapping resulted in four selected IT processes that could be used for research into information security risk management case studies: EDM03–Ensure Risk Management, APO12–Managed Risk, APO13–Managed Security, and BAI13–Managed Changes. Following the problems on Bureau XYZ, this study measured the maturity of the EDM03 Ensure Risk Management process as a process that focuses on optimizing risk management.

3.2 RACI Chart Mapping in Organization

In the functional structure mapping between RACI Chart from COBIT 5 and the functional structure in the Bureau XYZ, the source person was selected based on the functions and tasks that had been given. The mapping results can be seen in Table 1.

Table 1. RACI Chart Mapping

No	COBIT 5 Functional Structure	Bureau XYZ Functional Structure
EDM03.01 Evaluate Risk Management		
1	Chief Risk Officer	Sub Koordinator Keamanan Informasi dan Persandian
2	Strategy Executive Committee	Kepala Seksi Tata Kelola dan Evaluasi Layanan Pemerintah Berbasis Elektronik (e-Gov)
EDM03.02 Direct Risk Management		
3	Chief Risk Officer	Sub Koordinator Keamanan Informasi dan Persandian
EDM03.03 Monitor Risk Management		
4	Chief Risk Officer	Sub Koordinator Keamanan Informasi dan Persandian
5	Strategy Executive Committee	Kepala Seksi Tata Kelola dan Evaluasi Layanan Pemerintah Berbasis Elektronik (e-Gov)

3.3 Data and Evidence Collection

Interviews were conducted with respondents selected on the RACI mapping to determine the implementation of each process goal. In addition, evidence in the form of reports and documents was collected to confirm the results of the interviews.

Table 2. EDM03 Implementation

Process Goals	Criteria	Score	Work Products	Evidence
EDM03-01 EDM03.02	EDM03.BP01 Evaluate Risk Management	F	Risk Appetite guidance	Risk Management SOP
			Approved Risk Tolerance Level	Risk Management SOP
			Evaluation of risk Management activities	Risk Assessment
EDM03-02 EDM03-03	EDM03.BP02 Direct Risk Management	P	Risk management policies	Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik
			Key objective to be monitored for risk management	Formulir Statement of Applicability (SOA). Scope of Implementation: Pengembangan dan Operasional Aplikasi and Database The software.
			Approved process for Measuring risk management	Risk Assessment
	EDM03.BP03 Monitor Risk Management	L	Remedial actions to address risk management deviations	Risk Assessment
			Risk management issues for the board	Not Found

3.4 Capability Level and Gap Analysis

At this stage, the implementation of the EDM03 process was scored based on the data and evidence found. Based on the assessment in the previous stage, a level would be given as the level of achievement of the current Bureau XYZ. The scoring was obtained from the findings and interviews that were conducted. The results of the practice criteria assessment can be seen in Table 3.

Table 3. EDM03 Process Score

Process Objective	Base Practice	Score	Process Objective Score
EDM03-01 Risk thresholds are defined and communicated, and key IT-related risks are identified.	EDM03.BP01 Evaluate Risk Management	F 100%	F 100%
EDM03-02 The organization manages critical IT-related risks effectively and efficiently.	EDM03.BP01 Evaluate Risk Management	F 100%	L 78.33%
	EDM03.BP02 Direct Risk Management	P 50%	
	EDM03.BP03 Monitor Risk Management	L 85%	
EDM03-03 IT-related enterprise risk does not exceed the IT risk appetite and the impact of IT risk on the identified and managed enterprise value.	EDM03.BP02 Direct Risk Management	P 50%	L 67.5%
	EDM03.BP03 Monitor Risk Management	L 85%	
	Average score of EDM03 process objectives		**81.94%**

The scoring of work products uses the Guttman scale with a value of 1 if there are work products and a value of 0 if no work products are found. Based on the assessment, seven work products were found and one work product could not be found.

Table 4. EDM03 Work Products Score

Base Practice	Work Products	Findings	Score (%)
EDM03.01 Evaluate Risk Management	Risk Appetite guidance	1	F 100%
	Approved Risk tolerance levels	1	
	Evaluation of risk management activities	1	
EDM03.02 Direct Risk Management	Risk management policies	1	F 100%
	Key objectives to be monitored for risk management	1	
	Approved process for measuring risk management	1	
EDM03.03 Monitor Risk Management	Remedial actions to address risk management deviations	1	P 50%
	Risk management issues for the 50% board	0	
	Average score of EDM03 work products		**83.33%**

Based on the average score of the process objectives and the average score of work products, therefore the calculation of the overall score of the EDM03 process is as follows:

$$EDM03\ Score = \left(\frac{Process\ Goals\ Score + Work\ Products\ Score}{2}\right)\%$$

$$EDM03\ Score = \left(\frac{81.94 + 83.33}{2}\right)\%$$

$$EDM03\ Score = 82.64\%$$

The score from the EDM03 process is 82.64% which belongs to the L score category (Largely Achieved). Therefore, the EDM03 Ensure Risk Optimization process is at Level 1 Performed. Based on the assessment of the EDM03 process that has been carried out, the value of the gap in the capability level between the current condition and the expected condition is 2, with the level category being at L (Largely Achieved).

4 Conclusion

The level of information security risk management capability of the mail management information system implemented by Bureau XYZ for the EDM03 Ensure Risk Optimization process was Level 1 (Performed), with a score of 82.64%. Thus, the gap score with the desired capability level was 2. Therefore, to achieve the desired level, Bureau XYZ had to make improvements at Level 1 until it achieved the F (Fully Achieved) score category. Next, Bureau XYZ had to continue improving to fulfill the criteria of level 2 (Managed) and level 3 (Established). Bureau XYZ should make detailed risk management plans and complete records (5W1H) of security incidents that have occurred. By doing this, Bureau XYZ will have sufficient information to optimize its risk management planning. It was also necessary to fulfill risk management issues for the board work products, which contain risk management issues, so the issues can be handled by involving the board of directors.

The expected future research was to continue this research by designing a work product template that has not been created by the organization and an information technology governance mechanism that has not been established. In addition, the scope of further research can be expanded by measuring the APO12 (Managed Risk), APO13 (Managed Security), and BAI13 (Managed Changes) processes which were other selected processes from the mapping carried out in this case study, and also risk management related processes.

References

[1.] [D. E. Uwizeyimana, "Analysing the importance of e-government in times of disruption: The case of public education in Rwanda during Covid-19 lockdown," *Eval. Program Plann.*, vol. **91**, p. 102064, 2022, doi: https://doi.org/10.1016/j.evalprogplan.(2022).102064.

[2.] N. Nurdin, "Institutional Arrangements in E-Government Implementation and Use: A Case Study From Indonesian Local Government," *Int. J. Electron. Gov. Res.*, vol. **14**, no. 2, pp. 44–63, (2018), doi: http://doi.org/10.4018/IJEGR.2018040104.

[3.] J. Martins and L. G. Veiga, "Digital government as a business facilitator," *Inf. Econ. Policy*, vol. **60**, p. 100990, (2022), doi: https://doi.org/10.1016/j.infoecopol.2022.100990.

[4.] M. Venkatasen and P. Mani, "A risk-centric defensive architecture for threat modelling in e-government application," *Electron. Gov. an Int. J.*, vol. **14**, no. 1, pp. 16–31, (2018).

[5.] M. Nasrullah, S. H. Suryawan, N. P. Istyanto, and T. Kristanto, "Risk Priority Analysis for Change Management on E-Government using RIPC4 and AHP," *J. Inf. Syst. Informatics*, vol. **4**, no. 1, pp. 16–29, (2022).

[6.] M. N. Aleksandrov, V. A. Vasiliev, and S. V Aleksandrova, "Implementation of the Risk-based Approach Methodology in Information Security Management Systems," in *(2021) International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 2021, pp. 137–139. doi: 10.1109/ITQMIS53292.2021.9642767.

[7.] M. Yasin, A. Akhmad Arman, I. J. M. Edward, and W. Shalannanda, "Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," in *(2020) 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA*, 2020, pp. 1–5. doi: 10.1109/TSSA51342.2020.9310875.

[8.] G. M. W. Tangka, A. T. Liem, and J. Y. Mambu, "Information Technology Governance Audit Using the COBIT 5 Framework at XYZ University," in *2020 2nd International Conference on Cybernetics and Intelligent System (ICORIS)*, (2020), pp. 1–5. doi: 10.1109/ICORIS50180.2020.9320803.

[9.] et al. Bartens, Yannick, "Business/IT Alignment in Two-Sided Markets: A COBIT 5 Analysis for Media Streaming Business Models," in *Sustainable Business: Concepts, Methodologies, Tools, and Applications (4 Volumes)*, IGI Global, (2020), pp. 1123–1146. doi: https://doi.org/10.4018/978-1-5225-9615-8.ch051.

[10.] Yulandi, Y. Suryanto, and K. Ramli, "A COBIT-Based Critical Asset Evaluation of Electronic Certificate Management in Central, Urban, and Rural Government Agencies: Study and Analysis," in *(2018) International Conference on ICT for Rural Development (IC-ICTRuDev)*, (2018), pp. 98–104. doi: 10.1109/ICICTR.2018.8706851.

[11.] M. R. Katili, V. Pateda, M. G. Djafri, and L. N. Amali, "Measuring the capability level of IT governance: a research study of COBIT 5 at Universitas Negeri Gorontalo," *J. Phys. Conf. Ser.*, vol. **1387**, no. 1, p. 12021, (2019), doi: 10.1088/1742-6596/1387/1/012021.

[12.] Imany, Y. D., N. Hayuhardhika, W., Putra, and A. D. Herlambang, "Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. **3**, no. 6, pp. 5926–5935, (2019).

[13.] ISACA, "COBIT Self-assessment Guide: Using COBIT 5. In COBIT 5." ISACA, (2013).