Adoption of COBIT 5 Framework in Risk Management for Startup Company

Yeni Kusumaningrum[1], Wella[2]

[1,2]Information System Department, Universitas Multimedia Nusantara, Tangerang, Indonesia
https://orcid.org/0000-0002-9587-1057

Article History: Received: 10 November 2020; Revised: 12 January 2021; Accepted: 27January 2021; Published online: 05April 2021

Abstract: The research method used is qualitative, where data collection is done by interviewing informants related to risk findings and identification of the root of the problem using fishbone analysis with category 6M (Man, Money, Machine, Material, Method, Measurement). The results of the identification of the root causes are included in the risk quadrant with the risk probability categories (high, medium, low) and risk impact categories (high, medium, low). After getting the data needed, the stages of creating a risk management model that is mapping the results of identifying the root causes with the COBIT 5 framework. The results of interviews related to the risks experienced by small and medium enterprises obtained as many as 19 risks and the results of fishbone analysis (identification of the root causes) obtained as many as 48 root causes, but this study took a quadrant I-VI with a total of 24 root causes. This research produces a risk management model in the form of COBIT 5 process that is in line with the root of the problem that occurs in small and medium-sized enterprises, namely EDM03 (Ensure Risk Optimization), APO12 (Manage Risks), BAI02 (Manage Requirements Definition), DSS05 (Manage Security Service) , MEA02 (Monitor, Evaluate and Assess the System of Internal Control).

Keywords:COBIT 5, Risk Management, Small medium enterprise

1. Introduction

As the development of increasingly sophisticated information technology, the need for guarantees of the value of information technology, management of information technology risks and the need for control of information have been understood as key elements in the governance of agencies or organizations [1]. To achieve this, the need for good and correct IT management so that the existence and development of IT benefits can be felt by the organization [2]-[4]. In processing information technology, a management model is needed that can be used as a reference in accordance with organizational strategy and objectives, then it can be used as a measurement tool in overcoming problems that occur in organizations such as COBIT [1], [5], [6].

Indonesia through Law No. 20 of 2008 concerning Micro, Small and Medium Enterprises (UU MSME), defines MSME through the category of business entity independence, total net worth and annual sales results [7], [8]. IT can increase negative risks to the goals of a company, where the company's dependence on IT will further increase the impact of risk on the company [9]. Poor management of IT will result in suboptimal critical business processes [10], [11]. Risks that arise need to be regulated so as to minimize the impact of losses that will arise if the risk actually occurs [12]-[14].

Risk management is the process of identifying assessments, and developing IT risk mitigation and communication strategies that have the potential to adversely affect or adversely affect the organization [15]. With the implementation of measured risk management, it will make the development of small and medium-sized businesses based on the settlement of potential risks more on target, and eventually small and medium-sized businesses become more competitive both in the domestic and foreign markets [16]. Thus, small and medium businesses need and are eligible to accept new risk management methods, tools and approaches to take advantage of managing risk and increasing the value of their business [17], [18].

Research on risk management has never been found on small and medium-sized businesses, so this research was conducted to determine the process of the COBIT 5 framework related to risk management models that are appropriate for small and medium enterprise.

2. Literature Review

- *Small and Medium Enterprise*

Micro, Small and Medium Enterprises (MSMEs) are the most numerous business groups and resistant to various economic crises. MSMEs have distinguishing characteristics of business actors based on the scale of their businesses [16]. The World Bank classifies MSMEs into three groups, as follows:

- Micro, which is a business with a workforce of 10 people.
- Small, namely businesses with a workforce of 30 people.

- Medium, i.e. businesses with a workforce of up to 300 people.
- *Risk Management*

Risk management is the process of identifying assessments, and developing IT risk mitigation and communication strategies that have the potential to adversely affect or adversely affect the organization, while the control and measurement of the performance of risk management is carried out by all parties by determining which risks should receive attention and at what level the risks can be accepted by the organization [15].

- *COBIT 5*

Control Objectives for Information and Related Technology (COBIT) is a set of guidelines and documentation results that serve to assist auditors, stakeholders and users in connecting between the business control model and the IT control model [15]. The COBIT framework provides measures, indicators, processes and a collection of best practices to help companies optimize the management of information technology and develop controls on information technology management that is appropriate for an organization [1]. COBIT 5 has 5 domains namely Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Deliver, Service and Support (DSS), Build, Acquire and Implement (BAI), Monitor, Evaluate and Assess (MEA) and COBIT 5 also has 37 processes.

3. Research Method

- ***Research Object***

The object of research is the subject of research. The object of this research are two small and medium businesses based on information technology. The first research object is CV. RedimInotechSolusindo and the second is PT. FinAccel Technology Indonesia.

- ***Research Methods Comparison***

This research is more appropriate to use the COBIT 5 framework, because COBIT 5 enables better IT management and regulation within the scope of the organization, COBIT 5 also covers the entire scope of business and IT functions that takes into account stakeholder interests related to IT, and COBIT 5 helps organizations know the extent where IT performance and can identify areas that need to be improved performance, which can support the success of good IT governance.

Table 1. Comparison Methods [2]

COBIT 5	OCTAVE ALLEGRO
Enables better IT management and organization within the organization.	OCTAVE Allegro method only focuses on information assets.
Covering the entire scope of business and functional IT that takes into account the interests of stakeholders related to IT.	OCTAVE Allegro method is only for information systems security assessment.
Organizations can know the extent of IT performance and can identify areas that need to be improved performance, which can support the success of good IT governance.	Previous studies using OCTAVE Allegro method were mostly in the field of education.

- ***Research Methods***

The method in this study uses qualitative data with interviews related to the risks experienced by small and medium businesses. This study adopts the COBIT 5 framework as a reference for making risk management models suitable for small and medium businesses.

- ***Research Variables***

The research variables are divided into two categories, namely independent variables and dependent variables. The independent variables used in the study are all COBIT 5 domains, namely EDM, APO, BAI, DSS and MEA. While the dependent variable used in the study is the finding of small and medium business risks.

- ***Data Collection Techniques***

Data collection techniques are done by interview. Interviews were conducted with a question and answer session to two speakers via chat using the Line application and via video conference using the Zoom application.

- ***Data Analysis Techniques***

The results of interviews in the form of qualitative data that will be used to process and analyze data from the formulation of the problem.

- ***Research Methodology***

The first step is to collect data through interviews related to the risks experienced by the company to the root of the problem. After getting the data needed, the next step is mapping the risk management model by adopting all processes in the COBIT 5 framework that matches the problems experienced by the two research objects, so that it will produce a risk management model for SMEs. Because no research has been found on the creation of a risk management model, this research must be validated by involved sources such as expert COBIT 5 sources and sources of research objects, with the aim of producing a credible risk management model.

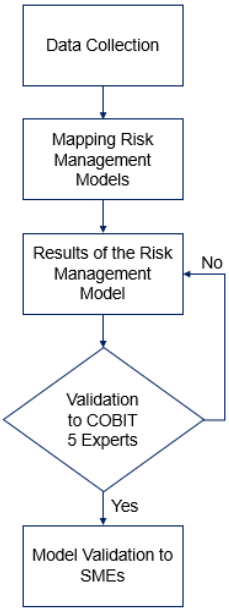

Figure1. The whole flow of the research methodology

4. Result and Discussion

- ***Data Collection***

Data collection is done in the form of interviews related to the risks experienced by small and medium businesses and the root of the problem until the risk can occur using fishbone analysis. Fishbone is one of the tools or tools used to identify the root cause of a risk. So that the data collected obtained produces qualitative data that will be used for data processing at a later stage.

Table 2. Risk SMEs

Risk Code	Risk Description	Object 1 (R)	Object 2 (K)
T1	Internet not connected.	✓	
T2	The office must be temporarily closed and work from home.	✓	✓
T3	Damage to the company's assets / hardware (mouse).	✓	
T4	The company does not have a fixed vendor related to the purchase of company assets such as hardware.	✓	
T5	Theft of corporate client data.	✓	
T6	Doesn't have an online database for sales data.	✓	
T7	Miscalculation of salary and commission expenses obtained becomes even greater, because the commission is obtained from the value of the project being worked on.	✓	

T8	Website got hacked.	✓	
T9	Jobdesc added to two staff.	✓	
T10	The company doesn't record risks that have occurred.	✓	
T11	The company doesn't capture when the risk is ongoing.	✓	
T12	The company doesn't have procedures to capture ongoing risks.	✓	
T13	The company doesn't identify risks when developing the company's website.	✓	
T14	The company doesn't have a decision-making procedure for handling the risks that occur.	✓	
T15	Theft of company data due to malware attacks.		✓
T16	Theft of company data from public parties or hackers.		✓
T17	Irresponsible employees can access data that should not be accessed.		✓
T18	Data on employee laptops can be lost.		✓
T19	User's account application was hacked.		✓

The method used to find out the root cause of each risk uses fishbone analysis. Fishbone analysis is a tool or tool used to identify the root cause of a risk. In fishbone analysis there are six categories, namely:
- Man, identification of the root causes of problems caused by human resources.
- Money, identification of the root causes of problems caused by finance.
- Machine, identification of the root causes of problem caused by technology.
- Material, identification of the root causes of problem caused by misinformation.
- Method, identification of the root causes of problem caused by method or process used.
- Measurement, identification of the root causes of problem caused by incorrect measurement.

After analyzing the root of the problem, the next step is to analyze the probability and impact. Probability is the possibility of root causes in a company, probability has 3 categories, namely high, medium and low, as follows:
- High, possibly under 1 year.
- Medium, it is likely to occur between 1 to 3 years.
- Low, possibly over 3 years.

Impact is the impact of losses experienced by the company and the impact also has 3 categories, namely high, medium and low, as follows:
- High, a loss of more than IDR 10 billion.
- Medium, losses between IDR 100 million to IDR 10 billion.
- Low, losses below IDR 100 million.

Risk Quadrant		Risk Impact		
		Low	Medium	High
Risk Probability	High	IV	II	I
	Medium	VII	V	III
	Low	IX	VIII	VI

Figure 2. Risk quadran

RISK MATRIX - Probability vs Impact				
Risk Quadrant		Risk Impact		
		Low	Medium	High
Risk Probability	High	6	0	7
	Medium	2	1	0
	Low	14	8	10

Figure 3. Risk matrix

Quadrant	Risk Level Count	Percentage
I	7	15%
II	0	0%
III	0	0%
IV	6	13%
V	1	2%
VI	10	21%
VII	2	4%
VIII	8	17%
IX	14	29%
Jumlah	48	100%

Figure 4. Risk level count

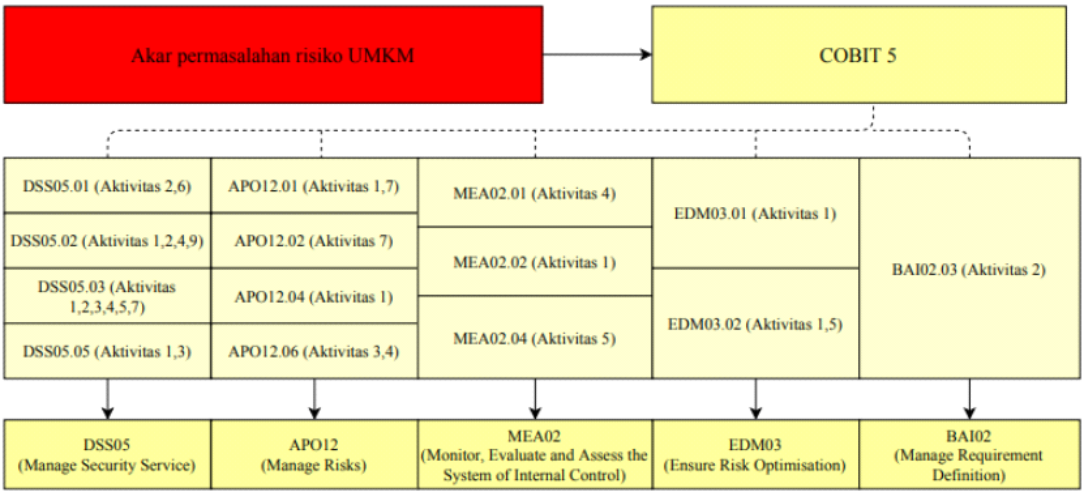

Figure5. Result risk management models

The DSS05 (Manage Security Service) process is in accordance with the identification of risks and root causes experienced by small and medium enterprises, so it is hoped that their security system must be further improved such as periodically monitoring security systems, the purpose of which is to minimize the risk of risk of data theft from parties not responsible.

The APO12 (Manage Risks) process and when identifying root causes, a description is found that there are still small and medium businesses that have not identified risks if they are carrying out a new or continued development, they should do business identification and assess risks, so that if there is a risk when a new development has been released or continued, they understand how to deal with risk.

The MEA02 (Monitor, Evaluate and Assess the System of Internal Control) process, there are still small and medium businesses that have not yet adopted a framework (IT governance) for their companies. In fact, in the industrial world, a framework is needed to help manage internal controls. By adopting a framework, discrepancies experienced by small and medium enterprises will be helped by appropriate remedial actions using the framework they adopt.

The EDM03 (Ensure Risk Optimization) process has the goal that the risks faced must be understood and communicated, because stakeholders will certainly face risks that may occur, the goal is that they understand the risks experienced and understand how to deal with these risks.

The BAI02 (Manage Requirement Definition) process helps identify solutions to organizational risk. Small and medium enterprises should know how probability the risk is experienced and how big is the impact of the loss experienced, the goal is that small and medium enterprises can transfer the risk or accept the risk.

- ***Validation of Risk Management Models to COBIT5 Expert***

The resource persons involved in this research are Mrs. Wella, S.Kom., M.MSI., COBIT5., As a COBIT 5 expert who has approved the results of this study and also Mr. SyahrakiSyahrir Muhsin as COBIT 5 expert (Vice President of ISACA Indonesia Chapter) who has validated this research. The validation needed for this research to produce a credible new model for small and medium enterprises, so that future research can use a risk management model that has been created.

- ***Validation of Data Collection to Research Object***

The purpose of the validation is needed to the parties involved in this research so that the data collection that has been obtained is valid and as supporting evidence interviews have been carried out during the process of conducting this research. As for other objectives, so that the parties involved know the results of research that have been made and also understand the importance of risk management, so as to minimize the risk of risks that may occur in the business they live.

- ***Discussions***

Risk findings obtained are 19 risk findings. On the CV. Redim Infotech Solusindo got 14 risks, while at PT. FinAccel Technology Indonesia gets 5 risks. Results of root cause analysis using fishbone obtained as many as 48 root problems. On the CV. Redim Infotech Solusindo gets 37 root problems, while at PT. FinAccel Technology Indonesia gets 11 root problems. The results from the quadrant I-VI sample got 24 total root problems. The quadrant sample taken is probability high with impact high (quadrant I) getting 7. Probability high with impact medium (quadrant II) is 0 and probability medium with impact high (quadrant III) is 0 or none. Probability high with low impact (quadrant IV) gets 6. Probability medium with impact medium (quadrant V) gets 1 and lastly probability low with impact high (quadrant VI) gets 10. Mapping the root of the problem with the COBIT 5 framework produces some of the most frequently occurring COBIT 5 processes that are suitable for managing risk to small and medium enterprises, the processes that often arise namely DSS05 (Manage Security Service), APO12 (Manage Risks), MEA02 (Monitor, Evaluate and Assess the System of Internal Control), EDM03 (Ensure Risk Optimization), BAI02 (Manage Requirement Definition). From the overall results of the mapping, there is an important concern for small and medium enterprises, namely the security system. For small and medium enterprises, the security system is a very important aspect to be the main development target in risk management. If SMEs has a weak security system, the business undertaken will be easily affected by risks that are quite detrimental to the business continuity of the business, so the target of achieving the internal security system must be strengthened to minimize the risks that might occur.

5. Conclusion

Mapping the root of the problem with the COBIT 5 framework produces some of the most frequently occurring COBIT 5 processes that are suitable for managing risk to small and medium enterprises, the processes that often arise namely DSS05 (Manage Security Service), APO12 (Manage Risks), MEA02 (Monitor, Evaluate and Assess the System of Internal Control), EDM03 (Ensure Risk Optimization), BAI02 (Manage Requirement Definition). From the overall results of the mapping, there is an important concern for small and medium enterprises, namely the security system. For small and medium enterprises, the security system is a very important aspect to be the main development target in risk management. If SMEs has a weak security system, the business undertaken will be easily affected by risks that are quite detrimental to the business continuity of the business, so the target of achieving the internal security system must be strengthened to minimize the risks that might occur.

6. Future Works

Based on the results of the mapping that has been done, to get the results of the risk management model by adopting the COBIT 5 framework, there are several things that can be suggestions, namely:

• It is expected that in subsequent studies to take measurements to small and medium businesses using a risk management model that has been made, with the aim to get a level score from COBIT 5 and can provide recommendations accordingly.

• It is also hoped that in future research, the object of research can be expanded more broadly to small and medium-sized businesses whose businesses are not based on information technology, such as restaurants, beauty salons and lodging places.

7. Acknowledgement

Thank you to Mr. SyahrakiSyahrir Muhsin as Vice President of ISACA Indonesia Chapter, who have taken the time to be experts in this research.

References

1. F. Ajismanto, "Analisis Domain Proses COBIT Framework 5 Pada SistemInformasi Worksheet (StudiKasus: Perguruan Tinggi STMIK, PoliteknikPalcomtech)," CogITo Smart Journal, vol. 3, no. 2, p. 2017, 2018.
2. L. N. Amali, M. R. Katili, S. Suhada dan L. Hadjaratie, "EVALUASI Tingkat Kapabilitas Proses Tata KelolaTiBerdasarkanKerangkaKerjaCobit 5 Dalam Domain Evaluate, Direct And Monitor (EDM)," Seminar Nasional SistemInformasi, vol. 3, pp. 1089-1096, 2018.
3. Setiawan, H., &Mustofa, K. (2013). Metode Audit Tata KelolaTeknologiInformasi di InstansiPemerintah Indonesia. Iptek-Kom, 15(1), 1–15.
4. Purba, E. (2018). PerananTeknologiInformasiDalamMengefektifkan Keputusan Pemberian Dana Corporate Social Responsibilty(CSR). E-Journal Budi Darma, 2(3), 69–75.
5. Fajrin, R. A., Murahartawaty, M., &Gumilang, S. F. S. (2016). Perancangan Tata KelolaTeknologiInformasi di BAPAPSI Pemkab Bandung Menggunakan framework COBIT 5 Pada Domain EDM dan DSS. Journal of Information Systems Engineering and Business Intelligence, 2(2), 74. https://doi.org/10.20473/jisebi.2.2.74-80
6. Sorongan, E. (2018). Analisis Tata KelolaTeknologiInformasi pada Domain. 6(1), 27–32.
7. Fahrurozi, "Supporting Ease Of Doing Business For Micro, Small, And Medium Enterprises In Legal Entity Form Through Single Shareholder Idea In Limited Liability Company Establishment," vol. 7, pp. 445-463, 2018.
8. Aprilinda, Y., &Puspa, A. K. (2018). Pemetaan COBIT 4.1 UntukPenilaianKematangan Tata Kelola TI. Jurnal Management SistemInformasi Dan Teknologi, 08(01).
9. N. D. Setyaningrum, S. dan A. Kusyanti, "EvaluasiManajemenRisikoTeknologiInformasiMenggunakan Framework COBIT 5 (StudiKasus: PT . Kimia Farma (Persero) Tbk – Plant Watudakon)," JurnalPengembanganTeknologiInformasi dan IlmuKomputer, vol. 2, no. 1, pp. 143-152, 2018.
10. H. M. Kurnia, R. N. Shofa dan R. , "Audit Tata KelolaTeknologiInformasiMenggunakan Framework Cobit 5 Berdasarkan Domain Apo12," JurnalSistemInformasi Dan Teknologi, vol. 1, no. 2, pp. 100-106, 2018.
11. Cahyadi, I. (2016). EvaluasiRisikoProyekImplementasiSistemErp Di Usaha Kecil Dan Menengah. Jurnal Teknik Industri, 15(2), 161. https://doi.org/10.22219/jtiumm.vol15.no2.161-169
12. H. B. Santoso dan L. Ernawati, "ManajemenRisiko Pada Pusat Data Perguruan Tinggi DenganKerangkaKerja NIST 800-30 (StudiKasus : Universitas Kristen Duta Wacana)," JurnalInformatika dan SistemInformasi (JUISI) UniversitasCiputra, vol. 3, no. 2, pp. 8-17, 2017.
13. Purwidiantoro, M. H., S.W, K. D. F., &Hadi, W. (2016). PengaruhPenggunaan Media SosialterhadapPengembangan Usaha Kecil Menengah (UKM). Jurnal EKA CIDA, 1(1), 30–39.
14. Ardia Sari, R., Yuniarti, R., &Puspita A, D. (2017). Analisa ManajemenRisiko Pada Industri Kecil Rotan Di Kota Malang. Journal of Industrial Engineering Management, 2(2), 39. https://doi.org/10.33536/jiem.v2i2.151
15. Z. Firdaus dan S. , "EvaluasiManajemenRisikoTeknologiInformasiMenggunakan COBIT 5 IT Risk (StudiKasus : PT . Petrokimia Gresik)," JurnalPengembanganTeknologiInformasi dan IlmuKomputer, vol. 2, no. 1, pp. 91-100, 2018.
16. M. A. Alifiana dan N. Susanti, "Analisis Dan PerancanganSistemInformasiPemetaanUmkmBerdasarPotensiRisikoBerbasis GIS," Seminar Nasional Multi DisiplinIlmu, pp. 289-294, 2018.
17. Ferreira de Araújo Lima, M. Crema dan C. Verbano, "Risk Management in SMEs: A Systematic Literature Review and Future Directions," European Management Journal, 2019.
18. Ekwere, N. (2016). Framework of Effective Risk Management in Small and Medium Enterprises (SMESs): a Literature Review. Bina Ekonomi, 20(1), 23–46.