Prisma Sains: Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA IKIP Mataram
https://e-journal.undikma.ac.id/index.php/prismasains/index
e-mail: prismasains.pkpsm@gmail.com

October 2023. Vol. 11, No. 4
p-ISSN: 2338-4530
e-ISSN: 2540-7899
pp. 1028-1036

Systematic Literature Review on Auditing Information Technology Risk Management Using the COBIT Framework

***Rizky Handayani, Ema Utami, Emha Taufiq Luthfi**
Master of Informatics Engineering, Universitas Amikom Yogyakarta, Jl. Padjajaran Ring Road Utara, Daerah Istimewa Yogyakarta 55283, Indonesia

*Corresponding Author e-mail: rizkyhandayani@students.amikom.ac.id

Received: August 2023; Revised: September 2023; Published: October 2023

Abstract

Information technology has an important role in carrying out company management activities. It is important that information technology is managed properly so that no risks arise that could endanger the company. Companies can implement information technology risk management through risk management audits. An audit on information technology risk management can help evaluate companies by identifying information technology risks and minimizing information technology risks. Such audits can be carried out with the help of the COBIT framework. This study intends to conduct a systematic literature review on risk management audits related to information technology using the COBIT framework. Literature search from IEEXplore, ScienceDirect and Garuda Kemdikbud database sources. Papers were selected based on inclusion criteria. Inclusion criteria include paper language is Indonesian and English, paper is published between 2019-2023, the paper describes COBIT in IT risk management audits, and paper is available as full text. The results obtained were 24 papers. There are two criteria for assessing paper quality, namely the paper contains the COBIT framework used for IT risk management audits and the paper contains the COBIT domain used. The results of the analysis of research questions indicate that COBIT 5 is a guide used by many researchers in information technology audits for risk management. COBIT 5 provides a complete and comprehensive risk governance guide for measuring enterprise IT risk management. Implementation of COBIT 5 in IT risk management audits to assist in risk assessment and risk management in order to minimize and prevent IT risks that may occur. Domain APO12 (Manage Risk) and EDM03 (Ensure Risk Optimization) as a reference in conducting IT risk management.

Keywords: IT Audit, COBIT, Risk Management, Systematic Literature Review

How to Cite: Handayani, R., Utami, E., & Luthfi, E. (2023). Systematic Literature Review on Auditing Information Technology Risk Management Using the COBIT Framework. *Prisma Sains : Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA IKIP Mataram*, *11*(4), 1028-1036. doi:https://doi.org/10.33394/j-ps.v11i4.8871

https://doi.org/10.33394/j-ps.v11i4.8871

INTRODUCTION

Information technology (IT) plays an important role in almost all areas of human life. Almost all companies currently use IT to carry out company management activities. IT can speed up the process of managing the company because there is integration or unification of data and there are several company operations that have been automated with IT support (Dzakiyyah et al., 2021). The company strives for a commitment to compliance and good management that is in line with the mission of the company. The use of IT in a company's business operations must be balanced with good IT management.

IT risks arise because IT is not managed properly, so these risks must be managed properly so that they do not harm the company because most of the company's business processes are supported by the use of IT. So IT risk management is very important to note. Companies can manage IT risk by identifying everything related to IT risk and then mitigating steps can be taken to minimize IT risk (Silvianthie & Perdanakusuma, 2022). IT risk

management can be done by conducting IT governance audits. The application of IT governance helps optimize the achievement of value from the use of IT (Puspitasari et al., 2020). Audits in the field of IT governance describe the ability of a company's IT to support and improve business processes (Audia & Sugiantoro, 2022). Thus, an IT risk management audit helps evaluate companies in identifying IT risks and minimizing these risks so as not to harm the company.

The framework used to assess companies in managing IT risk is the Control Objective for Information and Related Technology (COBIT). COBIT is a standard practice guide regarding IT management (Alfiansyah et al., 2020). COBIT considers governance and risk management to be a component of overall enterprise IT governance and management. This framework or guidance framework can help companies obtain risk-specific results, namely risk management strategies, risk management communication plans and risk mitigation (Ahmed, 2017). COBIT provides comprehensive and complete guidelines for measuring corporate IT risk management which is useful for helping achieve the goals of corporate IT governance (Sarmini & Adipurwoko, 2019). In COBIT presents a list of risk policies and their descriptions to help develop a company's customized risk policy. This list is for an IT risk management guidance framework that contains the components that must exist for effective IT risk management (Salman, 2017).

Several studies have used the COBIT guidance framework for the implementation of IT risk management audits. Farikhah et al (2021) uses COBIT in IT risk management on IoT to help analyze operational risk and provide solutions for managing these risks. Rajjani et al (2021) implements risk management at PT Semen Indonesia by adopting COBIT guidelines to measure a company's ability to anticipate or handle IT risks. Zakkadiaksa et al (2020) implements COBIT at UPT-TIK Universitas Brawijaya to assess risk and manage risk. Based on some of these studies that COBIT has a broad scope. IT risk management audit is important for companies so it needs to be implemented by a company. IT risk management is carried out by identifying IT risks to anticipate and deal with these risks. So that risk management helps companies manage IT risks and avoid the negative impacts they cause. Kurniati et al., 2020) researched Information Technology Risk Management on e-government: Systematic Literature Review. This research provides information regarding the implementation of risk management standards in the e-government sector and the benefits of implementing risk management as well as the factors that determine the success of implementing risk management in e-government. Ikhsan et al (2021) researched the Systematic Literature Review on Corporate Information Technology Governance in Indonesia using Cobit 2019. This research discusses the topic of IT governance in COBIT 2019 and provides a summary of COBIT 2019 research to make it easier to understand the implementation of COBIT 2019. The previous literature review focuses on IT risk management in e-government and IT governance in Indonesia uses COBIT 2019. Meanwhile, this research focuses on IT risk management audits using the COBIT framework.

This research uses a systematic literature review approach to analyze the use of COBIT for IT risk management audits. The selected papers in this research will be reviewed and analyzed so that this research can provide a summary of the application of COBIT for IT risk management audits. This research is expected to make it easier for future researchers to understand COBIT in IT risk management audits and as a study that helps an organization or company in IT risk management audits using the COBIT framework.

METHOD

The method applied in this study is the Systematic Literature Review (SLR). The SLR method is an activity of identifying, analyzing, and interpreting previous research in relation to research questions (Kurniati et al., 2020). The following are the SLR steps from this study.

1. Research Questions

The research questions in this research are as follows.

- RQ1: How is the COBIT framework used in an IT risk management audit?
- RQ2: What COBIT domains are used in an IT risk management audit?

2. Literature Search
   Literature search is the process of obtaining relevant research papers to obtain answers to research questions. The following databases were selected for the literature search:
   - IEEXplore
   - ScienceDirect
   - Garuda Kemdikbud

   Selected papers with publication range from 2019 to 2023. The literature search strategy uses the keywords "Risk" and "Cobit".
3. Literature Selection
   The literature that has been searched is then selected based on the inclusion and exclusion criteria according to the needs to be used in this study. The criteria are as follows.
   Inclusion criteria:
   a) Paper language is Indonesian and English
   b) Paper is published between 2019-2023
   c) The paper describes COBIT in it risk management audits
   d) Paper is available as full text
   Exclusion criteria:
   a) Paper is not available in full text
   b) The paper does not describe COBIT in IT risk management audits
   c) Paper is not literature review research
   d) Paper language is not Indonesian and English
4. Quality Assessment
   The next step is to provide a quality assessment of the paper that has been selected by setting quality criteria. The quality assessment criteria in this study are as follows.
   - QA1: Does the paper contain the COBIT framework used for IT risk management audits?
   - QA2: Does the paper state which COBIT domain to use?

RESULTS AND DISCUSSION

The process of searching for papers using predetermined keywords resulted in 90 papers originating from IEEEXplore, ScienceDirect and Garuda Kemdikbud database sources. The papers were then selected based on inclusion and exclusion criteria so that a total of 24 papers were obtained. Table 1 describes the detailed results of the literature search process.

Table 1. Literature Results

Database	Literature search	Literature selection
IEEEXplore	28	7
ScienceDirect	47	3
Garuda Kemdikbud	15	14
Total	**90**	**24**

The selected papers undergo a quality assessment. Papers containing the COBIT framework used in IT risk management audits and the COBIT domains suggested in the selected papers were identified. This study has two research questions used. The first research question is how the COBIT framework is used in an IT risk management audit (RQ1). Table 2 describes the framework used in IT risk management audits.

Table 2. Framework For IT Risk Management Audits

No	Author	Framework
1	(Othman et al., 2021)	ISO, COBIT, NIST dan ITIL

No	Author	Framework
2	(Aprianto & Nugroho, 2021)	COBIT 5 dan ISO 31000:2018
3	(Goman, 2019)	PMBOK, COBIT 5, ITIL V3, ISO 27005:2011 dan ISO 31000:2009
4	(Monev, 2020)	ISO 27001:2013 dan COBIT 5
5	(Irsheid et al., 2022)	COBIT 5, ISO27005, CRAMM, NIST SP 800-30, Allegro, OCTAVE, dan CORAS
6	(Amirta et al., 2023)	COBIT 2019
7	(Flores & Morocho, 2020)	OCTAVE-S, COBIT 5 dan ISO 27005
8	(Miranda et al., 2019)	COBIT 4.1
9	(Yubo, 2020)	COBIT 4.1
10	(Hasibuan & Setyadi, 2022)	COBIT 4.1
11	(Prasetyo & Setyadi, 2022)	COBIT 4.1
12	(Setyadi & Prabowo, 2021)	COBIT 4.1
13	(Setyadi & Anggoro, 2021)	COBIT 4.1
14	(Ximenes, 2019)	COBIT 4.1
15	(Hartono et al., 2019)	COBIT 5
16	(Wulandari et al., 2019)	COBIT 5
17	(Zakaria et al., 2019)	COBIT 5
18	(Prasetyo et al., 2023)	COBIT 5
19	(Setiawan & Fianty, 2023)	COBIT 5
20	(Sarmini & Adipurwoko, 2019)	COBIT 5
21	(Khairuna et al., 2020)	COBIT 5
22	(Alfiansyah et al., 2020)	COBIT 5
23	(Farikhah et al., 2021)	COBIT 5
24	(Nugraha et al., 2021)	COBIT 5

Referring to the systematic literature review to answer RQ1 in this research, the COBIT 5 framework is still widely used in IT risk management audits as seen in table 2. COBIT was prepared by the Information Systems Audit and Control Foundation (ISACA). COBIT is a guide or guide used in governance and management related to technology and information of an organization that is intended not only for IT but for the entire company. COBIT 5 is a framework that contains an overall business overview of an enterprise's IT governance to describe the use of IT. The COBIT 5 domain includes Evaluate, Direct and Monitor (EDM), Build, Acquire and Implement (BAI), Align, Plan and Organize (APO), Monitor, Evaluate and Assess (MEA), and Deliver, Service and Support (DSS). The maturity level in COBIT 5 uses the ISO/IEC 15504-2:2003 standard from level 0 to level 5 (ISACA, 2013). COBIT 5 for risk is the globally accepted and used part of COBIT 5 for enterprise IT risk management in IT governance and management. COBIT 5 for risk contains a comprehensive and complete risk management guide or guideline that can help companies measure IT risk management so that corporate IT governance goals can be achieved (Sarmini & Adipurwoko, 2019).

Implementation of risk management using COBIT 5 to ensure risk management procedures that can occur from the use of IT so as not to cause losses to the company. So that the application of risk management can minimize the risks that might occur from the use of IT (Goman, 2019; Othman et al., 2021; Sarmini & Adipurwoko, 2019). For example, research Irsheid et al (2022); Nugraha et al (2021) uses COBIT 5 to minimize some risks in order to maintain information security from IT use. Risk management can assist in preventing and protecting against the impact of threats that cause loss and damage to the use of IT (Prasetyo et al., 2023; Prasetyo & Setyadi, 2022). COBIT 5 is also used to carry out risk assessments. Risk assessment ensures that risks that are likely to occur can be identified and managed properly so as not to disrupt the company's business processes (Wulandari et al., 2019). Risk

assessment helps provide risk ratings and risk management strategies based on company risks. The results of the COBIT 5 maturity level as a source of input in risk assessment (Monev, 2020).

There are two risk perspectives in COBIT 5, namely the function of risk and risk management. The functional view of risk describes the need for an enterprise to create and maintain an efficient and effective risk management and IT governance. The risk management view describes the basic process of managing risk in identification, analysis, response and risk reporting which is supported by the COBIT 5 enabler (Ahmed, 2017). The scope of COBIT 5 for risk includes:

a) Focus on implementing COBIT 5 for risk
b) Help enable governance and risk management functions efficiently and effectively
c) Provide guidance in identifying, analyzing and responding to risks through the implementation of core risk management processes and risk scenarios
d) Aligned with and linked to enterprise risk management standards, frameworks and initiatives
e) Provides a link between COBIT 5 enablers and risk scenarios for risk mitigation

Table 3. COBIT domains

No	Author	Domain
1	(Hasibuan & Setyadi, 2022)	PO9
2	(Prasetyo & Setyadi, 2022)	PO9
3	(Setyadi & Prabowo, 2021)	PO9
4	(Setyadi & Anggoro, 2021)	PO9
5	(Sarmini & Adipurwoko, 2019)	EDM03 dan APO12
6	(Alfiansyah et al., 2020)	EDM03 dan APO12
7	(Nugraha et al., 2021)	EDM03 dan APO12
8	(Flores & Morocho, 2020)	EDM03 dan APO12
9	(Miranda et al., 2019)	PO, AI, DS dan ME
10	(Ximenes, 2019)	PO, AI, DS dan ME
11	(Yubo, 2020)	AI1, AI2, AI3, AI4, AI5, AI6
12	(Hartono et al., 2019)	EDM03, APO12, BAI06, APO13, DSS05
13	(Amirta et al., 2023)	EDM03, APO12, DSS03 dan DSS05
14	(Farikhah et al., 2021)	EDM03, APO12, EDM01, APO02, APO07, APO08, BAI08
15	(Wulandari et al., 2019)	APO12 dan DSS01
16	(Prasetyo et al., 2023)	APO12
17	(Khairuna et al., 2020)	APO12
18	(Aprianto & Nugroho, 2021)	APO12
19	(Setiawan & Fianty, 2023)	EDM02, APO07, APO10

The second research question is what COBIT domain is used in an IT risk management audit (RQ2). Based on table 3 that in risk management, APO (Align, Plan, Organize) and EDM (Evaluate, Direct, Monitor) are the most widely used domains. The APO domain focuses on all IT-enabled organizations, activities, and strategies. Meanwhile, the EDM domain focuses on the objectives of stakeholder governance, risk optimization, resource optimization and IT direction activities. Other domains in COBIT 5 include DSS, BAI, and MEA (ISACA, 2013). The EDM and APO domains that are widely used in risk management are EDM03 (ensuring risk optimization) and APO 12 (manage risk). EDM03 and APO12 as domains that are a reference for evaluating companies in managing risks from the use of IT (Salman, 2017). Both of these domains have been widely used by previous researchers who focused on risk

management in IT audits (Alfiansyah et al., 2020; Flores & Morocho, 2020; Nugraha et al., 2021; Sarmini & Adipurwoko, 2019)

EDM03 aims to ensure that IT risks to the company's business operations do not exceed the company's risk tolerance and risk requirements, identify and manage the impact of IT threats on the company's business value and minimize compliance violations. In this domain it provides an understanding to address and resolve existing and potential risks. EDM03 there are 3 management practices or sub domains:

a) EDM03.01 (Evaluate risk management)
b) EDM03.02 (Direct risk management)
c) EDM03.03 (Monitor risk management)

APO12 aims to integrate IT risk management into overall enterprise risk management and balance the costs and benefits of managing enterprise IT risk. There are 6 management practices in APO12:

a) APO12.01 (Collect data)
b) APO12.02 (Analyze risk)
c) APO12.03 (Maintain a risk profile)
d) APO12.04 (Articulate risk)
e) APO12.05 (Define a risk management action portfolio)
f) APO12.06 (Respond to risk)

CONCLUSION

This study presents the SLR on IT risk management audits using the COBIT guidance framework to analyze and identify the application of COBIT as an IT risk management standard. From the results of the analysis of the first research question, the COBIT version 5 guideline framework is widely used in IT risk management audits. The COBIT 5 section, namely COBIT 5 for risk, focuses on risk governance guidelines to measure enterprise IT risk management, so that corporate goals can be achieved regarding IT governance. COBIT 5 is implemented in auditing in risk management to help manage risks that may occur from the use of IT in order to minimize these risks. In addition, to assess risks so that they can be identified and managed properly so as not to disrupt the company's business processes. The results of the second research question are that there are 2 COBIT 5 domains used in IT risk management audits, namely EDM03 and APO 12. These two domains are used as a basis and reference for evaluating companies in managing risk in IT. This study can be used as a reference and reference for further studies, which focus on auditing IT risk management with COBIT work standards.

RECOMMENDATION

Recommendations that can be given for further research are research on risk management using COBIT which focuses on government or information systems.

REFERENCES

Ahmed, H. S. A. (2017). COBIT 5 for Risk—A Powerful Tool for Risk Management. *ISACA*. https://www.isaca.org/resources/news-and-trends/industry-news/2017/cobit-5-for-riska-powerful-tool-for-risk-management

Alfiansyah, F. I., Trias Hanggara, B., & Suprapto. (2020). Evaluasi Manajemen Risiko Teknologi Informasi menggunakan Standar Cobit 5 IT Risk pada PTPN X Pabrik Gula Meritjan Kediri. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *4*(11), 4207–4216. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/8289

Amirta, H. C. T., Jambak, M. I., Suarli, P. P., Utama, Y., Wedhasmara, A., & Sevtiyuni, P. E. (2023). Risk Management Evaluation in Hospital Management Information Systems Using Framework COBIT 2019-Case Study: Ernaldi Bahar South Sumatera Hospital.

Sriwijaya Journal of Informatic and Applications, *4*(1), 2807–239. http://sjia.ejournal.unsri.ac.id

Aprianto, K., & Nugroho, S. M. S. (2021). Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000:2018 di Kabupaten Magetan E-Government Risk Management Analysis Using COBIT 5 For Risk and ISO 31000:2018 in Magetan Regency. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *23*(2), 107–123. https://doi.org/http://dx.doi.org/10.33169/iptekkom.23.2.2021.107-123

Audia, R., & Sugiantoro, B. (2022). Evaluation and Implementation of IT Governance Using the 2019 COBIT Framework at the Department of Food Security, Agriculture and Fisheries of Balangan Regency. *International Journal on Informatics for Development*, *11*(1), 152–161. https://doi.org/10.14421/ijid.2022.3381

Dzakiyyah, A., Nurul Zahra, M., Azizi Rachim, N., & Khofifah Munjiyanti, S. (2021). Manajemen Risiko Sistem Informasi Rumah Sakit (Studi Kasus : Rumah Sakit EMC Tangerang). *Seminar Nasional Mahasiswa Ilmu Komputer Dan Aplikasinya (SENAMIKA)*, 456–469.

Farikhah, N., Fauzi, R., & Dewi, F. (2021). Analisis Manajemen Risiko TI Menggunakan Seven Enablers Berdasarkan COBIT 5 For Risk (Studi Kasus: PT. ABC). *Journal of Science and Social Research*, *4*(3), 236–240. http://jurnal.goretanpena.com/index.php/JSSR

Flores, D. A., & Morocho, G. (2020). Cloud-GMR: A Qualitative Framework for Governance and Risk Management of Cloud-hosted Public Services. *Proceedings - 2020 46th Latin American Computing Conference, CLEI 2020*, 294–303. https://doi.org/10.1109/CLEI52000.2020.00041

Goman, M. (2019). Current State of IT Risk Analysis in Management Frameworks: Is It Enough? *2019 60th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS) IEEE*, 1–5. https://doi.org/10.1109/ITMS47855.2019.8940653

Hartono, S., Tjahyadi, R., & Cassandra, C. (2019). Analysis of Trouble Ticket System Using COBIT 5 Framework (A Case Study Approach). *2019 International Conference on Information Management and Technology (ICIMTech)*, 420–425. https://doi.org/10.1109/ICIMTech.2019.8843709

Hasibuan, D., & Setyadi, R. (2022). Analysis Risk Management Application e-Raport Using COBIT 4.1. *SISFORMA: Journal of Information Systems*, *9*(1), 32–37. https://doi.org/10.24167/sisforma.v8i2.4038

Ikhsan, M., Widodo, A. P., & Adi, K. (2021). Systematic Literature Review on Corporate Information Technology Governance in Indonesia using Cobit 2019. *Prisma Sains : Jurnal Pengkajian Ilmu Dan Pembelajaran Matematika Dan IPA IKIP Mataram*, *9*(2), 354. https://doi.org/10.33394/j-ps.v9i2.4370

Irsheid, A., Murad, A., Alnajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, *204*, 205–217. https://doi.org/10.1016/j.procs.2022.08.025

ISACA. (2013). *Process Assessment Model (PAM): Using COBIT 5*. ISACA.

Khairuna, D., Wibowo, S., & Gamayanto, I. (2020). Evaluasi Pengelolaan Risiko Teknologi Informasi Menggunakan Framework COBIT 5 Berdasarkan Domain APO12 (Manage Risk) Pada Kantor Pusat BPR Agung Sejahtera. *JOINS (Journal of Information System)*, *5*(1), 18–26. https://doi.org/10.33633/joins.v5i1.3088

Kurniati, A., Edi Nugroho, L., & Nur Rizal, M. (2020). Manajemen Risiko Teknologi Informasi pada e-Government: Information Technology Risk Management on e-Government: Systematic Literature Review. *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi*, *22*(2), 207–222. https://doi.org/10.33164/iptekkom.22.2.2020.207-222

Miranda, N. B., Rodavia, M. R. D., & Miranda, M.-M. I. (2019). IT Infrastructure Auditing using COBIT Framework. *2019 6th International Conference on Technical Education (ICTechEd6) IEEE*, 1–6. https://doi.org/10.1109/ICTechEd6.2019.8790861

Monev, V. (2020). Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002. *2020 IEEE International Conference on Information Technologies (InfoTech-2020)*, 1–5. https://doi.org/10.1109/InfoTech49733.2020.9211066

Nugraha, I. P. Y., Fauzi, R., & Prasetyo, Y. A. (2021). Analisis Risiko Operasional Teknologi Informasi Menggunakan COBIT 5 For Risk Pada Dinas Komunikasi dan Informatika Kota Tangerang Selatan. *E-Proceeding of Engineering*, *8*(2), 2723–2734. openlibrarypublications.telkomuniversity.ac.id

Othman, N. A. A., Norman, A. A., & Kiah, M. L. M. (2021). Information System Audit for Mobile Device Security Assessment. *3rd International Cyber Resilience Conference (CRC)*, 1–6. https://doi.org/10.1109/CRC50527.2021.9392468

Prasetyo, B., Qomariah, L., & Retnani, W. E. Y. (2023). Risk Management using COBIT 5 for Risk : A Case Study on Local Government in Indonesia. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *8*(1), 435–444. https://doi.org/10.22219/kinetik.v8i1.1585

Prasetyo, M. A., & Setyadi, R. (2022). Risk Management Analysis Website E-klim at Civil Service Savings and Insurance Using COBIT 4.1. *SISFORMA: Journal of Information Systems*, *9*(1), 26–31.

Puspitasari, E. Y., Arifin, O., & Pentiana, D. (2020). Audit of Information Technology Governance Based on COBIT 5 (Study at the Office of Communication and Information Technology of Pringsewu Regency) Audit Tata Kelola Teknologi Informasi dengan Pendekatan COBIT 5 (Studi Pada Dinas Komunikasi dan Informatika Kabupaten Pringsewu). *Jurnal Ilmiah Esai*, *14*(1). https://doi.org/10.25181/esai.v14i1.2385

Rajjani, J. S. A., Hanggara, B. T., & Musityo, Y. T. (2021). Evaluasi Manajemen Risiko Teknologi Informasi pada Department of ICT PT Semen Indonesia (Perseo) Tbk menggunakan Framework COBIT 2019 dengan Domain EDM03 dan APO12. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *5*(5), 1734–1744. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/8982

Salman, S. (2017). COBIT 5 for Risk: Making Sense of IT Risk Management. *ISACA*. https://www.isaca.org/resources/news-and-trends/industry-news/2017/cobit-5-for-risk-making-sense-of-it-risk-management

Sarmini, & Adipurwoko, S. P. (2019). Ensure Risk Optimisation Implementasi Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5. *Jurnal SIMETRIS*, *10*(2), 795–800. https://doi.org/https://doi.org/10.24176/simet.v10i2.3496

Setiawan, J., & Fianty, M. I. (2023). Risk Assessment and Recommendation Strategy Based on COBIT 5 For Risk - A Case Study of an Internet Service Provider Company. *Journal of Information Systems and Informatics*, *5*(1), 243–258. https://doi.org/10.51519/journalisi.v5i1.453

Setyadi, R., & Anggoro, S. (2021). Risk Management Analysis Using COBIT 4.1 at Vehicle Testing Management Information System. *Jurnal Teknik Informatika Dan Sistem Informasi*, *7*(1). https://doi.org/10.28932/jutisi.v7i1.3419

Setyadi, R., & Prabowo, H. N. (2021). Risk Management Analysis Of Bus Transportation Application Using COBIT 4.1. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *7*(2), 203–212. https://doi.org/10.33330/jurteksi.v7i2.1046

Silvianthie, M., & Perdanakusuma, A. R. (2022). Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. IKI Karunia Indonesia menggunakan COBIT 2019. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *6*(12), 5726–5735. http://j-ptiik.ub.ac.id

Wulandari, S. A., Dewi, A. P., Rizki Pohan, M., Sensuse, D. I., Mishbah, M., & Syamsudin. (2019). Risk assessment and recommendation strategy based on COBIT 5 for risk: Case study sikn Jikn helpdesk service. *Procedia Computer Science*, *161*, 168–177. https://doi.org/10.1016/j.procs.2019.11.112

Ximenes, A. (2019). Risk Management Analysis on Implementation of Information System in Organization Liantimoroan Using COBIT 5. *Journal of Applied Information, Communication and Technology*, *6*(1), 29–35. https://doi.org/10.33555/ejaict.v6i1.62

Yubo, H. (2020). IT Risk Control for Internet Finance Based on COBIT. *Proceedings - 2020 International Conference on Big Data and Artificial Intelligence and Software Engineering, ICBASE 2020*, 275–278. https://doi.org/10.1109/ICBASE51474.2020.00064

Zakaria, H., Abu Bakar, N. A., Hassan, N. H., & Yaacob, S. (2019). IoT security risk management model for secured practice in healthcare environment. *Procedia Computer Science*, *161*, 1241–1248. https://doi.org/10.1016/j.procs.2019.11.238

Zakkadiaksa, I., Tria Hanggara, B., & Sapta Prakoso, B. (2020). *Evaluasi Manajemen Resiko Teknologi Informasi Menggunakan COBIT 5 dengan Domain EDM03 dan APO12 (studi kasus pada UPT-TIK Universitas Brawijaya)* (Vol. 4, Issue 8). http://j-ptiik.ub.ac.id