JEMSI: Jurnal Ekonomi Manajemen Sistem Informasi
E-ISSN: 2686-5238
P-ISSN: 2686-4916
https://dinastirev.org/JEMSI dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jemsi.v7i1

Evaluation of IT Risk Management in the Banking Industry using the COBIT 2019 Framework

Bram Rahadian[1], Raden Venantius Hari Ginardi[2]
[1]Institut Teknologi Sepuluh Nopember, Jawa Timur, Indonesia, bramrahadian3@gmail.com
[2]Institut Teknologi Sepuluh Nopember, Jawa Timur, Indonesia, hari.ginardi@gmail.com

Corresponding Author: hari.ginardi@gmail.com[2]

Abstract: Digital transformation has become a key strategy in the development of modern banking services. However, this process brings various risks that may hinder the achievement of business goals. This study aims to evaluate information technology (IT) risk management at PT. Bank Pembangunan Daerah Jawa Timur Tbk (Bank Jatim) using the COBIT 2019 framework. The main focus is directed at two domains: EDM03 (Ensure Risk Optimisation) and APO12 (Manage Risk). The research was conducted using a qualitative approach and case study method, with observation, interviews, and questionnaires as data collection techniques. The results show that Bank Jatim is currently at Level 2 for the EDM03 domain and Level 3 for the APO12 domain, while the target level for both is Level 4. Several gaps were identified, indicating the need for improvements in IT governance and risk management. Strategic recommendations are provided to support the achievement of optimal and sustainable digital transformation.

Keyword: COBIT 2019, IT Risk Management, Digital Transformation, Banking, Capability Level

INTRODUCTION

In the current digital era, the advancement of information technology has become a critical component that must be adopted by various organizations, including governmental institutions and private sector entities. Information technology now plays a pivotal role in determining organizational success, necessitating continuous adaptation to technological developments particularly within the banking industry. PT Bank Pembangunan Daerah Jawa Timur Tbk (Bank Jatim) is one of the largest regional development banks in Indonesia, classified as a BUKU 3 bank, with total assets exceeding IDR 100 trillion. In fulfilling its mandate to support regional economic development through banking services targeting local governments, the public, and the MSME sector in East Java, digital transformation has become imperative. This transformation aims to enhance operational efficiency, increase business value, and more effectively address customer needs. In response to digital disruption and the necessity for digital transformation across various business and operational activities, Bank Jatim has established a dedicated organizational structure under the Directorate of IT and Digital, encompassing Information Technology, Digital Banking, and IT Security.

The implementation of digitalization specifically the automation of manual processes through institutional applications inevitably introduces a variety of risks across human resources, business processes, and technologies. In the financial sector, information technology implementation is regulated through Bank Indonesia Regulation No. 19/12/PBI/2017 concerning the implementation of financial technology, and Financial Services Authority Regulation (POJK) No. 13/POJK.03/2022 concerning the implementation of information technology by commercial banks. These regulations underscore that IT governance is integral to good corporate governance (GCG), serving both to enhance business value and mitigate associated risks. Accordingly, Bank Jatim must address risks related to digital transformation by implementing a robust IT risk management strategy, supported by the COBIT 2019 framework, which comprises seven core assessment components. Interviews conducted with the Vice President of Bank Jatim's Information Technology Division reveal several challenges in risk management, including limited human resource competencies, lack of system integration, inadequate infrastructure, and increasing external threats. Key digital platforms such as JConnect, E-Loan, and Laku Pandai are also exposed to both internal and external risks, which can significantly affect overall organizational performance. The existence of IT risks presents potential negative impacts, thus necessitating comprehensive risk management carried out by qualified professionals. Such risk management activities include risk identification, assessment, strategic mitigation planning, and communication with relevant stakeholders to manage IT-related risks effectively. Effective risk management serves as a strategic input for decision-making processes aimed at minimizing and preventing risk impacts. However, the IT Division at Bank Jatim has yet to conduct a comprehensive, dedicated IT risk assessment, particularly in the context of ongoing digital transformation efforts. Therefore, updated risk identification is necessary, employing an appropriate framework to ensure actionable and accurate mitigation planning. Several internationally recognized frameworks are available for this purpose, including the COSO Enterprise Risk Management (ERM), Control Objectives for Information and Related Technologies (COBIT), NIST Special Publications (SP), and ISO 31000:2018.

Previous studies have explored IT governance using a range of frameworks. For instance, Rindi (2023) utilized COBIT 2019 to evaluate IT governance at PT Telkom Indonesia, providing recommendations for process capability improvements. Oktianatasari (2017) applied COBIT 5 to audit IT governance at PT Pelabuhan Indonesia III, while Juminovario and Edi (2022) examined the EDM03 and APO12 domains within a university setting using the same framework. Meanwhile, Tasha and Nurul (2022) applied NIST and ISO frameworks to assess information security in a government agency. These studies collectively affirm the critical importance of IT risk management in ensuring the success of digital transformation initiatives. Building on these studies, this research employs the COBIT 2019 framework due to its comparative advantages over ISO and TOGAF, and its alignment with existing regulatory frameworks. COBIT 2019 emphasizes strategic objective achievement across five domains: Evaluate, Direct and Monitor (EDM); Align, Plan and Organize (APO); Build, Acquire and Implement (BAI); Deliver, Support and Service (DSS); and Monitor, Evaluate and Assess (MEA). Bank Jatim's most recent IT risk evaluation was conducted in 2018 using a previous version of the framework. Consequently, a reassessment using COBIT 2019 is warranted to ensure alignment with the institution's current vision and mission. This study specifically focuses on the EDM03 subdomain, which addresses risk optimization, and APO12, which pertains to risk identification and assessment. Field observations and interview findings suggest that Bank Jatim's current IT risk handling measures are neither fully optimized nor up to date. As such, the institution plans to update its IT risk management practices using COBIT 2019, with emphasis on the EDM03 and APO12 domains, to ensure integrated risk management that balances cost and value effectively.

METHOD

This study employs a qualitative approach using a case study design. The research subject is the Information Technology Division of Bank Jatim, which plays a central role in managing the company's digital transformation. The research procedure consists of several stages:

Literature Review

Relevant literature was reviewed from COBIT 2019 documentation, Financial Services Authority (OJK) regulations, ISO 31000, as well as scientific journals on risk management and IT governance.

Field Study and Observation

Observations were conducted on the organizational structure, main duties and functions, as well as policy documents and risk reports. The researcher also mapped governance components based on the seven COBIT components: processes, organizational structures, information flows, people and skills, policies and procedures, culture, and services and infrastructure.

Interviews

In-depth interviews were conducted with five key officials within the IT and Digital Directorate, including the Vice President, Assistant Vice President (AVP) of IT Planning and Governance, AVP of Applications, AVP of Infrastructure, and the IT Security Unit. These interviews were carried out face-to-face to explore their understanding of IT risk management implementation.

Questionnaire Distribution

A questionnaire was developed based on the COBIT 2019 process attributes from Capability Level 2 to Level 5, using a Guttman scale in which "Yes" responses scored 1 and "No" scored 0. The questions focused on activities and supporting documents within EDM03 and APO12, with a total of 25 indicators developed for capability assessment. The questionnaire was administered in stages according to the COBIT 2019 capability levels, requiring each level to be fully satisfied before advancing to the next. Questions were based on relevant base practices and work products. The questionnaire was completed in the presence of the researcher, who also conducted observations and interviews to validate the documents and confirm the actual implementation of the required work products.

Data Analysis

Data were analyzed using the Capability Maturity Model Integration (CMMI) model and classified into six capability levels: Incomplete, Performed, Managed, Established, Predictable, and Optimizing. Questionnaire scores were converted into percentages and mapped onto a rating scale ranging from Not Achieved to Fully Achieved. Capability gaps were calculated based on the difference between the current level and the target level.

RESULTS AND DISCUSSION

Capability Level assessments were conducted for two selected domains in the COBIT 2019 Toolkits: **EDM03 (Ensure Risk Optimization)** with a priority of 75%, and **APO12 (Manage Risk)** with a priority of 100%. According to ISACA's *Designing an Information and Technology Governance Solution* (2018), Capability Level attributes are evaluated based on the following rating scale:

Table 1. Capability Level Assessment

Skala	Keterangan	Pencapaian (%)	Keterangan
N	Not Achieved	0% to 15%	No achievement or evidence in the assessed process
P	Partially Achieved	>15% to 50%	Some achievement or evidence exists, but certain aspects are unpredictable
L	Largely Achieved	>50% to 85%	Systematic evidence exists, though weaknesses are present in the process
F	Fully Achieved	>85% to 100%	Complete achievement with no identified weaknesses

EDM03 Capability Assessment (Ensure Risk Optimization)

Capability assessments in the EDM03 domain were conducted using Guttman scaling, where each attribute must achieve Fully Achieved (F) before proceeding to the next level.

Capability Level 1

Table 2. Capability Level 1 EDM03

Participant	Activity Score	Total Activities	Capability
Respondent 1	10	10	100%
Respondent 2	9	10	90%
Respondent 3	10	10	100%
Respondent 4	10	10	100%
Respondent 5	10	10	100%
Capability Score $\frac{Res\ 1 + Res\ 2 + Res\ 3 + Res\ 4 + Res\ 5}{\sum Responden} \times 100\%$			98%

Average Score: 98% → *Fully Achieved* → Proceed to Level 2

Capability Level 2

Table 3. Capability Level 2 EDM03

Participant	Activity Score	Total Activities	Capability
Respondent 1	8	10	80%
Respondent 2	9	10	90%
Respondent 3	9	10	90%
Respondent 4	9	10	90%
Respondent 5	10	10	100%
Capability Score $\frac{Res\ 1 + Res\ 2 + Res\ 3 + Res\ 4 + Res\ 5}{\sum Responden} \times 100\%$			98%

Average Score: 88% → *Fully Achieved* → Proceed to Level 3

Capability Level 3

Table 4. Capability Level 3 EDM03

Participant	Activity Score	Total Activities	Capability
Respondent 1	7	10	80%
Respondent 2	6	10	90%
Respondent 3	8	10	90%
Respondent 4	7	10	90%
Respondent 5	9	10	100%
Capability Score $\frac{Res\ 1 + Res\ 2 + Res\ 3 + Res\ 4 + Res\ 5}{\sum Responden} \times 100\%$			87%

Average Score: 87% → *Fully Achieved* → Proceed to Level 4

Capability Level 4

Table 5. Capability Level 4 EDM03

Participant	Activity Score	Total Activities	Capability
Respondent 1	6	10	60%
Respondent 2	5	10	50%
Respondent 3	6	10	60%
Respondent 4	5	10	50%
Respondent 5	7	10	70%
Capability Score $\frac{Res\ 1 + Res\ 2 + Res\ 3 + Res\ 4 + Res\ 5}{\sum Responden} \times 100\%$			58%

Average Score: 58% → *Largely Achieved* → **Cannot proceed to Level 5**

Capability Level 4 reached a score of 58% (Largely Achieved), which indicates that the evaluation criteria were not fully met; thus, APO12 cannot proceed to Capability Level 5. It is therefore concluded that the capability level achieved for APO12 is Level 3.
The risk management process has covered risk identification, risk analysis, and risk profiling. Documentation of analysis results and third-party evaluations is available, although not yet fully systematized. APO12 is assessed at Level 3 (Established) with a rating of *Largely Achieved*. However, the integration between IT risk management and enterprise risk management has not yet been fully realized.
The capability gap between the current state and the company's target condition for each domain EDM03 and APO12 is presented below:

Table 6. Gap Level Analysis

Objective	COBIT Domain	Current Level	Target Level	Gap
Governance	EDM03—Ensured Risk Optimization (Optimalisasi Risiko Dipastikan)	2	4	2
Management	APO12—Managed Risk (Risiko dikelola)	3	4	1

There is a **two-level gap in EDM03** and a **one-level gap in APO12**. The primary causes of these gaps include: Lack of formal documentation for risk policies, Absence of structured training and awareness programs, Limited availability of qualified human resources in IT risk management, Suboptimal collaboration between the IT division and business units.

CONCLUSION

This study demonstrates that the implementation of IT risk management at Bank Jatim is at an early stage of development. With a capability achievement of Level 2 for EDM03 and Level 3 for APO12, there is a clear need to develop documented policies and procedures, as well as to enhance human resource capabilities. COBIT 2019 has proven to be an effective tool for evaluation and guidance in improving IT risk management. The proposed strategic recommendations are expected to support Bank Jatim in achieving a predictable and adaptive risk management environment in response to technological changes.

REFERENSI

A. Rahmadana, R. Mulyana, dan A. F. Santoso, "Pemanfaatan COBIT 2019 Information Security dalam Merancang Manajemen Keamanan Informasi pada Transformasi Bank Co," *JUTISI*, vol. 12, no. 3, 2023.

A. Oktaviana, K. Adi, dan B. Warsito, "Adopting COBIT 2019 for the Evaluation of Information Technology Risk Management in a Startup Company," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 6, Jun. 2024

Ansori, A. (2011). Perancangan tata kelola jaminan ketersediaan layanan teknologi informasi pada Rumah Sakit Umum Daerah (RSUD) Kabupaten Sidoarjo [Tesis, Institut Teknologi Sepuluh Nopember].

Apriatono, N., & Wibowo, A. (2017). Analisa risiko proyek pengembangan software pada CV. XYZ. Indonesia.

Arumana, A., Rochim, A. F., & Windasari, I. P. (2014). Analisis tata kelola teknologi informasi Fakultas Teknik UNDIP. Jurnal Teknologi dan Sistem Komputer.

B. Tarbiyatuzzahrah, R. Mulyana, dan A. F. Santoso, "Penggunaan COBIT 2019 GMO dalam Menyusun Pengelolaan Layanan TI Prioritas pada Transformasi Digital BankCo," *JTIM: J. Teknol. Inf. & Multimedia*, vol. 5, no. 3, Okt. 2023.

Bagye, W. (2016). Analisis tingkat kematangan sistem informasi akademik menggunakan framework COBIT 4.1 (Studi kasus: STMIK Lombok). J. Speed – Sentra Penelitian.

C. Santoso, R. Mulyana, dan Y. W. Dwi, "Penggunaan COBIT 2019 I&T Risk Management

untuk Pengelolaan Risiko Transformasi Digital BankCo," *JUTISI: J. Ilm. Tek. Inf. & Sist. Inf.*, vol. 12, no. 3, 2023.

D. Utomo, M. Wijaya, dan N. T. M. Sagala, "Leveraging COBIT 2019 to Implement IT Governance in SME Context: A Case Study of Higher Education in Campus A," *CommIT J.*, vol. 16, no. 2, 2022.

G. M. W. Tangka dan E. Lompoliu, "IT Governance Using the COBIT 2019 Framework in Manado Post Companies," *J. Inform. & Teknol.*, 2024.

I. Ilori, F. Nwosu, dan P. Naiho, "A Comprehensive Review of IT Governance: Effective Implementation of COBIT and ITIL Frameworks in Financial Institutions," *Comp. Sci. & IT Res. J.*, vol. 5, no. 6, Jun. 2024

Juminovario, J., & Negara, E. S. (2022). Manajemen risiko divisi sistem informasi pada Universitas

M. W. Hossain George et al., "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review," *arXiv*, Mar. 2025

Megawati, T. A., Astuti, H. M., & Herdiyanti, A. (2014). Pengelolaan risiko aset teknologi informasi pada perusahaan properti PT XYZ, Tangerang berdasarkan kerangka kerja COBIT 4. In Seminar Nasional Sistem Informasi Indonesia (pp. 444–449)

Melissa I. Fianty dan M. Brian, "Enhancing Information Technology Governance: A Comprehensive Evaluation of The 2019 COBIT Framework," *Int. J. Sci. Technol. & Manage.*, Sept. 2023

N. Riznawati, R. Mulyana, dan A. F. Santoso, "SEIKO: Journal of Management & Business Pendayagunaan COBIT 2019 DevOps dalam Merancang Manajemen Pengembangan TI Agile pada Transformasi Digital BankCo," *SEIKO: J. Manag. & Bus.*, vol. 6, no. 2, 2023.

Putri, T. S., Mutiah, N. M., & Prawira, D. P. (2022). Analisis manajemen risiko keamanan informasi menggunakan NIST Cybersecurity Framework dan ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat). Coding: Jurnal Komputer dan Aplikasi, 10(2), 237.

T. Wulyatiningsih dan J. Y. Mambu, "IT Governance Maturity and Business Alignment: A COBIT 2019 Evaluation at RSUD ODSK," *Malcom Indonesian J. Mach. Learn. & Comp. Sci.*, Mar. 2025.

Weol, A. L., Wibowo, A., & Dewi, L. P. (2015). Analisa manajemen risiko pada perusahaan Real Estate X. Jurnal Infra, 3(2)

Y. P. Asih, T. Winarno, and A. Pracoyo, "Implementasi Algoritma Fuzzy Logic Control untuk Sistem Pengontrolan Suhu dan Kelembaban pada Mesin Pengering Biji Kakao Berbasis Prosentase Berat," *J. Elektron. dan Otomasi Ind.*, vol. 5, no. 3, p. 42, 2021, doi: 10.33795/elkolind.v5i3.145.