Institut Riset dan Publikasi Indonesia (IRPI)
MALCOM: Indonesian Journal of Machine Learning and Computer Science
Journal Homepage: https://journal.irpi.or.id/index.php/malcom
Vol. 5 Iss. 3 July 2025, pp: 1012-1018
ISSN(P): 2797-2313 | ISSN(E): 2775-8575

Risk Management Analysis in Digital Bank XYZ Using the COBIT 2019 Framework

Rudi Purnomo[1*], Ruki Harwahyu[2]

[1,2]Departemen Teknik Elektro, Fakultas Teknik, Universitas Indonesia, Indonesia

E-Mail: [1]rudi.purnomo@ui.ac.id, [2]ruki.h@ui.ac.id

Received Jan 02nd 2025; Revised Jun 01st 2025; Accepted Jul 12th 2025; Available Online Jul 31th 2025, Published Jul 31th 2025
Corresponding Author: Rudi Purnomo

Abstract

The digital transformation in the banking sector has driven the emergence of digital banks, offering online services without the need for physical branches. However, this transformation brings various risks, including information security threats and challenges in regulatory compliance. This study aims to evaluate the maturity level of risk management in Digital Bank XYZ using the COBIT 2019 framework. The research methodology employs a qualitative approach with gap analysis to compare the current state with expected standards. The findings reveal significant gaps in the APO13 (Managed Security) and DSS04 (Managed Continuity) domains between current risk management practices and the standards recommended by COBIT 2019. These results highlight the need for a more systematic and structured risk management approach to enhance Digital Bank XYZ's preparedness in addressing cybersecurity threats and other operational risks. Recommendations include strengthening security policies, implementing predictive technologies, and conducting regular training to improve the security team's competencies. This study is expected to serve as a strategic guideline for Digital Bank XYZ to mitigate risks, improve operational efficiency, and achieve international governance standards.

Keywords: Bank, COBIT 2019, Digital Bank, Risk, Risk Management

1. INTRODUCTION

Digital transformation in the era of the Industrial Revolution 4.0 has brought significant changes, particularly in the banking sector. Shifts in consumer behavior, which demand fast and secure services, have driven traditional banks to transition to digital banking [1], [2]. Bank Indonesia (BI) reported that the value of digital transactions in August 2023 reached IDR 5,098.6 trillion, an increase of 11.9% compared to 2022 [3]. Over the past five years, digital transactions have grown at an average rate of 12.82% per year and are projected to increase by several hundred percent by 2030 [3]. This rapid digital adoption, while offering numerous benefits, also presents significant challenges that must be addressed to ensure secure and sustainable growth. Figure 1 shows the growth of digital bank users and transaction value in Indonesia 2018-2023.

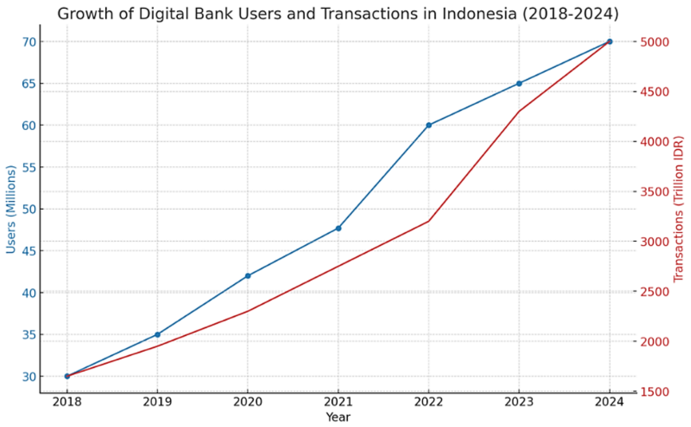

Figure 1. Growth of Digital Bank Users and Transaction Values in Indonesia 2018-2023[3], [4], [5], [6].

Indonesia is the largest digital banking user in Asia, with 47 million users in 2021, projected to increase to 74 million by 2026 [5]. However, challenges such as digital readiness, regulations, data protection, cyber risks, and the implementation of international standards persist. The Network Readiness Index 2023 ranks Indonesia 59th out of 146 countries, while Cisco's 2021 Digital Readiness Index places it 73rd out of 146 countries [7], [8]. Cyber threats, including DDoS attacks, continue to rise. In 2023, Indonesia experienced 43,879 DDoS attacks, with the largest attack reaching a bandwidth of 220.88 Gbps [9]. In terms of regulation, the Financial Services Authority (OJK) and Bank Indonesia (BI) regulate digital banks through POJK No.12/POJK.03/2018 and PBI No.20/6/PBI/2018, both of which require adherence to risk management and information security standards [10], [11]**.**

In response to these ongoing challenges, various researchers have conducted studies to evaluate IT governance and risk management approaches using different frameworks. Several studies have explored IT governance and risk management using a variety of methods, highlighting existing gaps. The first study [12] discusses the use of COBIT 2019 to evaluate IT governance at Bank Indonesia in the Bengkulu Province, focusing on the subdomains EDM03, EDM05, APO11, BAI09, DSS04, DSS06, and MEA01. The results indicate that the maturity level of IT governance is at Level 1 (Initial), meaning that Bank Indonesia in Bengkulu has not yet implemented a systematic and consistent approach to IT service quality processes. The gap analysis was conducted in the context of conventional banking.

The second study [13] evaluates IT governance in a manufacturing company using COBIT 2019, focusing on the subdomains APO07, APO12, APO13, BAI08, and DSS05. The average scores for each domain fall under the "Largely Achieved" category, with a maturity level of Level 2, but they failed to meet the company's expected targets. The researchers recommended six actions for APO07, three for APO12, three for APO13, two for BAI08, and four for DSS05. The gap analysis was conducted in the manufacturing sector context. The third study [14] examines risk management in debtor information systems using the OCTAVE Allegro method in conventional banks, focusing on the identification and assessment of threats and vulnerabilities to critical information assets such as debtor profiles, loan facilities, and credit quality. The findings highlight potential risks, including human error, application bugs, and unauthorized access, which impact customer trust, financial stability, and regulatory compliance. The gap analysis was conducted in the context of conventional banking using the OCTAVE Allegro method.

The fourth study [15] explores the use of COBIT 5 to analyze risk management in mobile banking, focusing on subdomains APO12 and EDM03. The results show that APO12 achieved a capability level of 3 (Defined Process) for APO12.1, 12.2, and 12.3, and a capability level of 2 (Managed Process) for APO12.4, 12.5, and 12.6. The gap analysis was conducted in the context of mobile banking and COBIT 5. The fifth study [16] investigates risk management in audit management systems (AMS) using the ISO/IEC 27005:2022 framework, focusing on risk threat identification, assessment, and vulnerabilities. The study identified 24 risks categorized as follows: 1 very high, 3 high, 8 medium, 11 low, and 1 very low. The gap analysis was conducted in the context of audit systems using ISO/IEC 27005:2022.

However, despite these studies, there remains a gap in research specifically focusing on digital banks, particularly in applying COBIT 2019 within this context. Digital Bank XYZ, which recorded one million users in its first six months, aims to become a market leader by 2030. To achieve this goal, a security framework such as COBIT 2019 for IT governance and management is essential. COBIT 2019 helps organizations manage risk and comply with regulations through best practices and international standards [17]. This study aims to evaluate the risk management practices of Digital Bank XYZ using the COBIT 2019 framework through process capability assessment and gap analysis, to recommend improvements and help minimize risks in order to reduce potential losses. This research not only assesses the risk management capabilities of a digital bank using COBIT 2019 but also contributes to academic discourse by addressing an underexplored area in digital financial services. To achieve these objectives, the study adopts a qualitative approach by applying COBIT 2019 capability level assessments across key IT risk domains relevant to digital banking operations.

2. MATERIALS AND METHOD

This study adopts a qualitative approach, with primary data sources obtained through interviews and observations. COBIT 2019 is used as the framework for assessment, evaluation, and recommendations. The detailed stages of the research are illustrated in Figure 2.

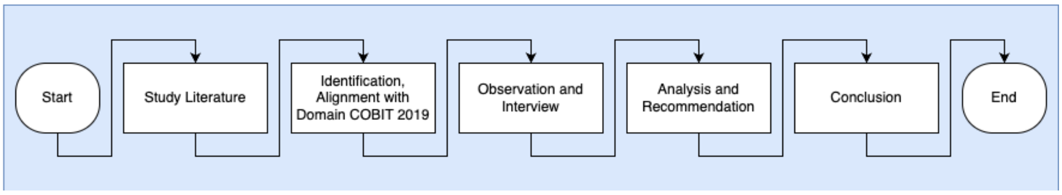
Start
Study Literature
Identification, Alignment with Domain COBIT 2019
Observation and Interview
Analysis and Recommendation
Conclusion
End

Figure 2. Research Stages

The first stage is the literature review, conducted to build a strong theoretical foundation by examining various references, including books, journals, academic articles, and other relevant documents. This stage aims to understand existing concepts and findings, identify research gaps, and provide a theoretical context for the research topic [18], [19], [20]. A review of prior studies revealed that most previous research applied COBIT 5 and primarily focused on conventional banks with general IT governance themes. In contrast, this study specifically analyzes risk management [21], [22], [23] within the context of a digital bank using the COBIT 2019 framework. The study contributes by mapping COBIT 2019 processes that are directly relevant to IT risk management and providing capability-based improvement recommendations. These contributions distinguish this research by addressing current needs in digital banking governance, an area still underrepresented in prior academic exploration, particularly in the Indonesian context.

The second stage involves mapping the organization's strategic objectives to COBIT 2019's Enterprise Goals (EG) and Alignment Goals (AG) to ensure alignment between business strategy and IT governance objectives. This process helps identify the relevant COBIT 2019 domains that will serve as the focus of the research, such as EDM03, APO12, APO13, BAI10, DSS04, and DSS05 [24]. The third stage consists of direct observations and in-depth interviews with relevant stakeholders, such as risk managers, IT security heads, and compliance staff. Observations aim to capture actual field conditions, while interviews provide expert perspectives on current risk management practices.

The fourth stage involves analyzing and discussing the collected data using gap analysis to evaluate discrepancies between current and expected performance levels. The results serve as the foundation for formulating structured improvement recommendations, such as enhancing capabilities within the identified domains. This stage is intended to improve the overall effectiveness and efficiency of risk management in alignment with the COBIT 2019 framework. The final stage summarizes the key research findings, including the maturity level of risk management, identified capability gaps, and corresponding improvement recommendations. At this stage, the researcher also provides suggestions for implementing the proposed improvement measures.

3. RESULTS AND DISCUSSION

3.1 Results

Based on the assessment results using the Process Capability Model (PCM) for the five domains EDM03, APO12, APO13, DSS04, and DSS05, the data obtained is presented in Table 1.

Table 1. Assessment Results Using the Process Capability Model (PCM)

Domain	Level 2	Level 3	Level 4	Level 5	Maturity	Desc
EDM03	100(F)	100(F)	100(F)		4	Quantitative
APO12	100(F)	100(F)	100(F)	100(F)	5	Optimizing
APO13	100(F)	83(L)	100(F)	50(P)	3	Defined
DSS04	89(F)	83(L)	75(L)	50(P)	3	Defined
DSS05	100(F)	97(F)	80(L)		4	Quantitative

The assessment results of risk management maturity at Digital Bank XYZ show that EDM03 is at maturity level 4, with processes fully managed and operating at a predictable level. APO12 has reached maturity level 5, indicating that its processes are fully optimized, with a focus on innovation and continuous improvement. APO13 is at maturity level 3, with processes largely standardized but still requiring enhancements at levels 3, 4, and 5 to achieve optimal outcomes. DSS04 also sits at maturity level 3, signaling a need for improvement at levels 4 and 5 to ensure consistency and continuous development. Finally, DSS05 has reached maturity level 4, with security services mostly managed in a quantitative and predictable manner. A gap analysis was conducted to determine whether the current maturity levels align with the expected targets. Any gap values less than zero were adjusted to zero. The gap is defined as:

$$\text{Gap} = \text{Expected Maturity Level} - \text{Current Maturity Level}$$

Table 2 and Figure 3 presents the gap values for each domain. The largest gaps are found in APO13 and DSS04, each with a gap of 1, where the current level is 3 and the target is 4. Meanwhile, EDM03, APO12, and DSS05 have already met their target maturity levels.

Table 2. Maturity Level Gaps

Domain	Current	Target	Gap
EDM03 - Ensured Risk Optimization	4	4	0
APO12 - Managed Risk	5	4	0
APO13 - Managed Security	3	4	1

Domain	Current	Target	Gap
DSS04 - Managed Continuity	3	4	1
DSS05 - Managed Security Service	4	4	0

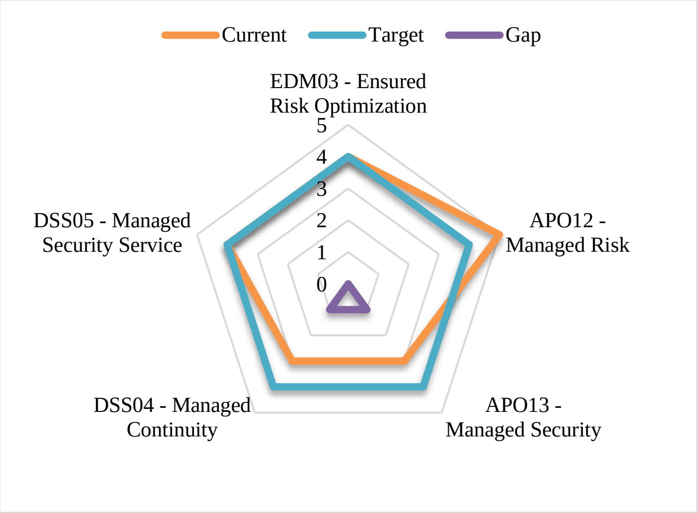

Figure 3. Maturity Level Gap Chart

From the gap analysis results, domains APO13 and DSS04 require improvements. The recommended strategic actions are as follows:

1. APO13 – Managed Security
   a. Formulate and maintain an information security risk treatment plan aligned with strategic objectives and enterprise architecture. Ensure the plan identifies appropriate and optimal security management practices and solutions, including related resources, responsibilities, and priorities to manage identified information security risks.
   b. Maintain an inventory of solution components that have been implemented to manage security-related risks.
   c. Develop a proposal to implement the information security risk treatment plan, supported by a proper business feasibility study, including considerations for funding as well as the allocation of roles and responsibilities.
   d. Provide input to the design and development of management practices and solutions selected from the information security risk treatment plan.
   e. Implement information security and privacy training and awareness programs.
   f. Integrate the planning, design, implementation and monitoring of information security and privacy procedures and other controls capable of enabling prompt prevention, detection of security events, and response to security incidents.

2. DSS04 - Managed Continuity
   a. Assess the likelihood of threats that could cause loss of business continuity. Identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.
   b. Analyze continuity requirements to identify possible strategic business and technical options.
   c. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.
   d. Obtain executive business approval for selected strategic options.
   e. Distribute the plans and supporting documentation securely to appropriately authorized interested parties. Make sure the plans and documentation are accessible under all disaster scenarios.
   f. Schedule exercises and test activities as defined in the continuity plans.
   g. On a regular basis, review the continuity plans and capability against any assumptions made and current business operational and strategic objectives.
   h. On a regular basis, review the continuity plans to consider the impact of new or major changes to enterprise organization, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.
   i. Consider whether a revised business impact assessment may be required, depending on the nature of the change.

j. Recommend changes in policy, plans, procedures, infrastructure, and roles and responsibilities. Communicate them as appropriate for management approval and processing via the IT change management process.
k. Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.

3.2 Discussion

The analysis using the COBIT 2019 framework reveals varying levels of maturity across different domains for Digital Bank XYZ. EDM03 (Ensured Risk Optimization) reached maturity level 4, indicating well-documented processes supported by quantitative measurements. APO12 (Managed Risk) achieved the highest level, level 5, reflecting continuous innovation and optimization in risk management practices. However, APO13 (Managed Security) and DSS04 (Managed Continuity) remained at level 3, highlighting the need for consistent implementation and ongoing improvement. These findings suggest that Digital Bank XYZ should prioritize enhancements in security and continuity management to strengthen customer trust, reduce operational risks, and ensure regulatory compliance. The achievement in APO12 can serve as a foundation for driving innovations that improve operational efficiency and competitiveness. Compared to prior research conducted at Bank Indonesia in Bengkulu, where maturity levels only reached level 1, Digital Bank XYZ demonstrates a significantly more advanced implementation of risk management. Similar patterns observed in manufacturing and conventional banking institutions further emphasize industry-wide challenges, particularly in cybersecurity. Despite these strengths, the analysis also indicates that Digital Bank XYZ still faces several areas requiring improvement, especially in process capability and the integration of IT risk governance into the broader business strategy. These results are consistent with previous studies, which have identified not only technical barriers but also challenges related to managerial commitment and cross-functional coordination in IT governance implementation.

This study presents a key advantage by specifically assessing risk management capabilities based on relevant COBIT 2019 domains, leading to more focused and actionable recommendations. Moreover, the use of COBIT 2019 as the latest governance framework provides a modern and responsive perspective on ongoing technological changes, particularly within the fast-evolving digital banking landscape. This is critical, as IT-related risks in digital banks differ significantly from those in conventional financial institutions in terms of threat exposure, innovation speed, and customer expectations. Therefore, implementing an adaptive, capability-based governance framework such as COBIT 2019 is highly relevant and strategic for enhancing organizational resilience and long-term competitiveness. Future research should expand the study scope to include multiple digital banking institutions, apply quantitative methods for deeper validation, and explore the role of emerging technologies—such as artificial intelligence and big data—in strengthening digital banking risk management.

4. CONCLUSION

The evaluation of IT governance maturity at Digital Bank XYZ using the COBIT 2019 framework indicates a position between level 3 (Established Process) and level 4 (Predictable Process). To enhance capabilities, several strategic steps are recommended, such as formulating and maintaining an information security risk treatment plan aligned with strategic objectives, maintaining an inventory of security solutions, developing a proposal for implementing the risk treatment plan, conducting security and privacy training, and integrating prevention, detection, and incident response processes. In addition, assessing business continuity threats, identifying specific needs, and recommending strategic options with appropriate resource allocation are also priorities. The bank is also encouraged to develop a centralized risk governance dashboard to monitor maturity level progress in real time, improve collaboration between IT and business units through cross-functional training and regular risk workshops, and initiate external benchmarking against other digital banks to gain broader insights. Moreover, the use of artificial intelligence and big data analytics should be considered not only for detecting operational risks but also for predicting potential compliance issues and security threats. Implementing these recommendations is expected to strengthen risk management, organizational resilience, and IT security, ensuring that Digital Bank XYZ is well-prepared to face future technological challenges. However, this study has several limitations; it is based on a single case study, employs a qualitative approach with limited internal data sources, and focuses only on selected COBIT 2019 processes related to IT risk. For future research, it is recommended to include multiple digital banking institutions for broader generalization, apply mixed-method approaches for deeper validation, and explore the full integration of COBIT 2019 in IT governance to assess its direct impact on organizational performance.

REFERENCES

[1] "Cetak Biru Transformasi Digital Perbankan." Accessed: Jun. 27, 2024. [Online]. Available: https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Cetak-Biru-Transformasi-Digital-Perbankan.aspx

[2] E. Indriasari, H. Prabowo, F. L. Gaol, and B. Purwandari, "Intelligent Digital Banking Technology and Architecture: A Systematic Literature Review," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 19, pp. 98–117, 2022, doi: 10.3991/ijim.v16i19.30993.

[3] "Statistik Sistem Pembayaran dan Infrastruktur Pasar Keuangan (SPIP) September 2023." Accessed: Jun. 21, 2024. [Online]. Available: https://www.bi.go.id/id/statistik/ekonomi-keuangan/spip/Pages/SPIP-September-2023.aspx

[4] "Indonesia peringkat 2 Pemilik Rekening Bank Digital Terbanyak di Dunia 2021 - GoodStats." Accessed: Jun. 27, 2024. [Online]. Available: https://goodstats.id/article/indonesia-peringkat-kedua-terbanyak-pemilik-rekening-digital-di-dunia-e04Em

[5] "Pengguna Bank Digital di Indonesia Diproyeksi Capai 748 Juta pada 2026." Accessed: Jun. 25, 2024. [Online]. Available: https://databoks.katadata.co.id/datapublish/2021/10/07/pengguna-bank-digital-di-indonesia-diproyeksi-capai-748-juta-pada-2026

[6] "BI Catat Nilai Transaksi Digital Banking 2023 Rp 58.478,24 Triliun - Diskominfo Prov. Kaltim." Accessed: Jun. 21, 2024. [Online]. Available: https://diskominfo.kaltimprov.go.id/ekonomi/bi-catat-nilai-transaksi-digital-banking-2023-rp-5847824-triliun

[7] "Indonesia – Network Readiness Index." Accessed: Jun. 25, 2024. [Online]. Available: https://networkreadinessindex.org/country/indonesia/

[8] "Indonesia - Cisco Digital Readiness 2021." Accessed: Jun. 25, 2024. [Online]. Available: https://www.cisco.com/c/m/en_us/about/corporate-social-responsibility/research-resources/digital-readiness-index.html#/country/IDN

[9] "Indonesia - Latest Cyber Threat Intelligence Report." Accessed: Jun. 25, 2024. [Online]. Available: https://www.netscout.com/threatreport/apac/indonesia/

[10] "Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum." Accessed: Jun. 27, 2024. [Online]. Available: https://ojk.go.id/id/regulasi/Pages/Penyelenggaraan-Layanan-Perbankan-Digital-oleh-Bank-Umum.aspx

[11] "Peraturan Bank Indonesia Nomor 20/6/PBI/2018 tentang Uang Elektronik." Accessed: Jun. 27, 2024. [Online]. Available: https://www.bi.go.id/id/publikasi/peraturan/Pages/PBI-200618.aspx

[12] P. Nicholas, P. Tambunan, and N. Legowo, "Evaluasi Tata Kelola TI Bank Indonesia Provinsi Bengkulu dengan COBIT 2019," *JATISI (Jurnal Teknik Informatika dan Sistem Informasi)*, vol. 11, no. 1, Mar. 2024, doi: 10.35957/JATISI.V11I1.7707.

[13] P. Kwak and R. I. Desanti, "IT Governance Evaluation Using COBIT 2019 Framework in A Manufacturing Company," in *Proceedings of the 7th 2023 International Conference on New Media Studies, CONMEDIA 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 62–67. doi: 10.1109/CONMEDIA60526.2023.10428517.

[14] *Proceeding of 2019 International Conference on Electrical Engineering and Informatics (ICEEI) : July 9th-10th, 2019, Bandung, Indonesia*. IEEE, 2019.

[15] J. N. Utamajaya, A. Ramadhan, E. Abdurachman, A. Trisetyarso, and M. Zarlis, "Risk Assessment Analysis on Mobile Banking Using Cobit 5 Framework," in *2022 IEEE Creative Communication and Innovative Technology, ICCIT 2022*, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICCIT55355.2022.10118645.

[16] D. E. R. Hidayatullah, R. Kunthi, and R. Harwahyu, "Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department," *International Journal of Electrical, Computer, and Biomedical Engineering*, vol. 2, no. 3, Sep. 2024, doi: 10.62146/ijecbe.v2i3.81.

[17] "COBIT | Control Objectives for Information Technologies | ISACA." Accessed: Jul. 06, 2024. [Online]. Available: https://www.isaca.org/resources/cobit

[18] "Bank | Definition, History, Types, Examples, & Facts | Britannica Money." Accessed: Dec. 31, 2024. [Online]. Available: https://www.britannica.com/money/bank

[19] "Bank Umum." Accessed: Sep. 19, 2024. [Online]. Available: https://ojk.go.id/id/regulasi/Pages/Bank-Umum.aspx

[20] S. Kraus, P. Jones, N. Kailer, A. Weinmann, N. Chaparro-Banegas, and N. Roig-Tierno, "Digital Transformation: An Overview of the Current State of the Art of Research," *Sage Open*, vol. 11, no. 3, 2021, doi: 10.1177/21582440211047576.

[21] "ISO 31000:2018(en), Risk management — Guidelines." Accessed: Dec. 31, 2024. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

[22] "Enterprise Risk Management | COSO." Accessed: Dec. 25, 2024. [Online]. Available: https://www.coso.org/enterprise-risk-management

[23] "Manajemen Risiko di Era Digital : Melindungi Perusahaan dari Ancaman Siber." Accessed: Dec. 31, 2024. [Online]. Available: https://pe.feb.unesa.ac.id/post/manajemen-risiko-di-era-digital-melindungi-perusahaan-dari-ancaman-siber?utm_source=chatgpt.com

[24] "Introducing COBIT 2019." Accessed: Dec. 28, 2024. [Online]. Available: https://www.isaca.org/isaca-digital-videos/cobit/introducing-cobit-2019