JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK, No.0173/C3/DT.05.00/2025
Vol. 8, No. 3, Desember 2025, pp. 181-187 p-ISSN: 2614-8897
DOI: 10.33387/jiko.v8i3.10704 e-ISSN: 2656-1948

EVALUATION OF MATURITY LEVEL INFORMATION SECURITY USING COBIT 2019 AND ISO/IEC 27001:2022

Zahrach Artamevia[1], Agung Triayudi[2]

[1] Information Technology, Faculty of Communication and Information Technology, Universitas Nasional, Jakarta, 12520, Indonesia
[2] Information Technology, Faculty of Communication and Information Technology, Universitas Nasional, Jakarta, 12520, Indonesia
Email: *1 zahrachartamevia.2024@civitas.unas.ac.id, 2agungtriayudi@civitas.unas.ac.id

(Received: 8 September 2025, Revised: 24 September 2025, Accepted: 20 October 2025)

Abstract

Information security plays a vital role in maintaining the reliability and continuity of business processes, particularly in the retail sector where data integrity is crucial for claim validation and payment systems. PT XYZ developed a Claim Management System to enhance transparency and efficiency in managing incentive claims. However, recurring challenges such as frequent data loss and weak access control disrupted operations and posed risks to business continuity. This study aims to evaluate the maturity level of information security management at PT XYZ to address these issues. COBIT 2019 was selected as the primary framework because it offers a structured and measurable approach for assessing IT governance maturity, while ISO/IEC 27001:2022 was applied to identify relevant security controls for further improvement. A descriptive comparative method was employed, utilizing questionnaires, interviews, and domain mapping. The findings indicate that PT XYZ achieved its targeted maturity level across all assessed domains, with some processes exceeding expectations. Although no significant gaps were identified, several recommendations were proposed, including regular business continuity and disaster recovery testing, integration of security controls into the ISMS, enhanced real time monitoring, and regulatory compliance mapping. The study concludes that combining COBIT 2019 and ISO/IEC 27001:2022 provides a comprehensive framework for strengthening IT governance and information security, with practical implications for improving organizational resilience.

Keywords: *Information Security, COBIT 2019, ISO/IEC 27001:2022, Maturity Level, IT Governance*

**Corresponding Author: Author1*

1. INTRODUCTION

The use of information and communication technology (ICT) in the retail sector is essential to support claim payment monitoring systems and ensure the integrity of operational processes.[1] Information Technology (IT) in business plays a key role in improving effectiveness, efficiency, and the security of customer data. Today, many companies across industries, including the retail sector, are undergoing digital transformation to maintain data integrity and strengthen competitiveness.[2]

PT XYZ, a company engaged in retail, has adopted IT in its operations. To support transparency and efficiency in incentive claim management, PT XYZ developed a Claim Management System that allows dealers to submit claims based on sales data. Claim validation is performed using this data as the basis for processing payments, with the expectation that the system produces accurate and reliable outputs.[3]

However, in practice, PT XYZ still faces serious challenges related to information security and system management.[4] One recurring problem involves data loss caused by unauthorized modifications, forcing dealers to resubmit sales data, which hinders validation and disrupts business continuity.

To address these challenges, two frameworks were considered COBIT 2019 and ISO/IEC 27001:2022. COBIT 2019 (Control Objectives for Information and Related Technology) provides a structured and measurable framework for assessing IT governance and aligning IT management with business goals.[5]

In contrast, ISO/IEC 27001:2022 offers a risk based approach to establishing and improving an Information Security Management System (ISMS) through policies, access control, backup, and change management procedures[6]

While many studies have applied COBIT for IT governance evaluation, its integration with ISO/IEC 27001:2022 in the context of the retail sector remains underexplored. Unlike models such as the Technology Acceptance Model (TAM) or Task Technology Fit (TTF), which emphasize user behavior and technology alignment, COBIT 2019 was chosen because it focuses specifically on governance, control, and maturity evaluation, which are critical for solving PT XYZ's issues of data loss and weak access control.

The use of information and communication technology in the government sector is essential to support electronic-based government systems, commonly referred to as e-government. E-government aims to simplify all activities carried out within the government. Currently, both central and regional governments are striving to improve the quality of products and services used internally within government institutions, as well as those provided to the general public, in order to realize their organizational vision and mission.[7]

The function of Information Technology (IT) in business is essential for improving effectiveness, efficiency, and the security of customer data in every service provided. Currently, many companies across various industries, including the banking sector, are implementing IT as part of their digital transformation efforts to maintain data integrity.[8]

In addition, previous studies have highlighted the importance of IT services, IT risk management, information security, and DevOps practices in supporting digital transformation (DT) in large banks, particularly with reference to the COBIT 2019 framework. Furthermore, in other financial industries, previous research has also examined information security governance, especially in insurance companies and fintech firms.[9]

The need to implement COBIT 2019 and ISO/IEC 27001:2022 in this study arises from the necessity to address issues of data loss, uncontrolled system changes, and their impact on the continuity of business relationships.[10]

ISO/IEC 27001:2022 focuses on protecting information security through the implementation of policies such as backup, access control, and change management procedures. Meanwhile, COBIT 2019 provides a comprehensive IT governance and risk management framework, ensuring that the management of information technology is aligned with the company's business goals and strategies. By integrating these two frameworks, the proposed solution is expected to resolve technical issues while simultaneously strengthening overall IT governance at PT XYZ.[11]

Based on these considerations, this study aims to analyze issues of data loss and weak access control in PT XYZ's Claim Management System, evaluate its IT process capability using COBIT 2019, identify relevant ISO/IEC 27001:2022 controls to address these issues, and propose recommendations for strengthening IT governance and information security through the integration of COBIT 2019 and ISO/IEC 27001:2022.

The contribution of this study lies in demonstrating how the combined use of COBIT 2019 and ISO/IEC 27001:2022 can strengthen IT governance and information security in the retail sector, specifically by addressing data loss and access control issues in claim management systems. This integration offers both theoretical originality and practical implications for enhancing organizational resilience, filling a gap in prior research that has focused mainly on individual frameworks or other industries.

In line with these objectives, this study seeks to answer several research questions, namely, the main issues related to data loss and weak access control in managing the Claim Management System at PT XYZ; the level of IT process capability at PT XYZ based on COBIT 2019; the relevant information security controls from ISO/IEC 27001:2022 to mitigate these issues; and how PT XYZ can implement proposed improvements in IT governance and information security through the integration of COBIT 2019 and ISO/IEC 27001:2022.

2. RESEARCH METHOD

In this study, COBIT 2019 and ISO/IEC 27001:2022 are used to measure the maturity level and recommend improvements. The issues of frequent data loss and inadequate user access control, identified as problems within PT XYZ particularly concerning security in the Claim Management System are addressed through the standards and guidelines of ISO/IEC 27001:2022 and COBIT 2019. The results of applying this method are analyzed to generate solutions in the form of descriptive recommendations.

This research adopts a descriptive comparative approach aimed at assessing and comparing the maturity level of information security management within the organization by using two main frameworks, namely ISO/IEC 27001:2022 and COBIT 2019. The study context is a real data loss incident within the company, thereby providing a practical illustration of the governance mechanisms and controls in place.

The approach applied is a quantitative method (through maturity scoring and questionnaires). This design enables the researcher to obtain a comprehensive assessment of the organization's information security governance from multiple perspectives.

The object of this research is the implementation of information security controls directly related to the prevention and handling of data loss incidents, while the research subjects consist of IT staff

Data collection is carried out through the following methods :

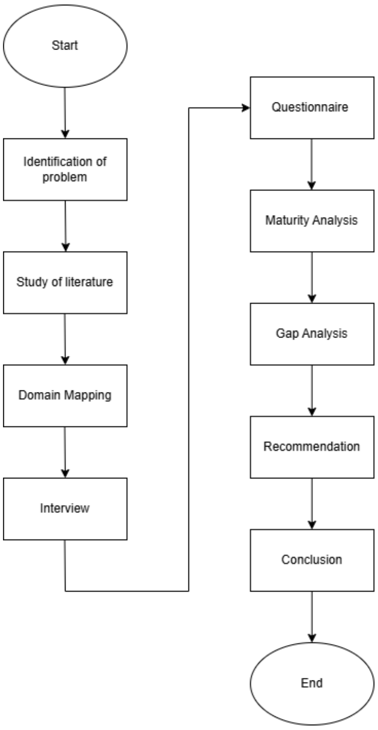

Figure 1. Example using picture

2.1. Identification of Problem

This ensures that the research not only builds upon established theories but also contributes to advancing practical solutions for improving information security and governance. The main problem identified in PT XYZ's Claim Management System is the frequent loss of sales data submitted by dealers. This issue arises from weak access control mechanisms that allow unauthorized modifications or deletions of data within the system. As a result, dealers are required to resubmit their sales data, which significantly disrupts the validation process and delays claim payments.

These recurring issues not only hinder operational efficiency but also pose risks to business continuity and trust between the company and its partners. Since data is a critical asset for ensuring transparent and accurate claim validation, the lack of proper security controls compromises the integrity and reliability of the system. Without immediate improvements, PT XYZ may face long-term challenges in maintaining partner confidence and ensuring smooth operational workflows.

Therefore, it is essential to address these problems by implementing robust IT governance and information security measures. Strengthening access controls and ensuring reliable data management are necessary steps to minimize the risk of data loss and enhance the overall effectiveness of the Claim Management System.[12]

2.2. Literature Review

The literature review is conducted by examining a wide range of theoretical information gathered from diverse sources, including journals, articles, books, and online references related to the research topic. This process plays a crucial role in establishing a strong theoretical foundation and ensuring that the study is grounded in existing knowledge. By reviewing prior research, the study identifies key concepts, frameworks, and findings that are relevant to the problem under investigation.

Furthermore, the literature review enables the researcher to identify existing gaps and opportunities that have not been fully addressed in previous studies. It also provides comparative insights into how similar issues have been approached in other contexts, particularly in the implementation of frameworks such as COBIT 2019 and ISO/IEC 27001:2022. This ensures that the research not only builds upon established theories but also contributes to advancing practical solutions for improving information security and governance.[13]

2.3. Domain Mapping

The COBIT 2019 framework domain mapping in this stage is conducted through an in-depth analysis using the Goal Cascade framework. This approach ensures that enterprise goals are systematically aligned with IT-related goals, which are then linked to governance and management objectives. By applying the Goal Cascade, organizations can trace how business needs translate into IT processes and capabilities, ensuring that every activity supports overall strategic objectives. As illustrated in Figure 2, the stages provide a structured path to identify, prioritize, and map domains within COBIT 2019, thereby creating a clear connection between organizational strategy, governance practices, and operational processes. This mapping not only enhances visibility but also strengthens accountability and performance measurement across the enterprise.[14]

2.4. Interview

Interviews with staff are conducted to gather in-depth information and insights directly from individuals who are actively involved in the system's operations. Through these interviews, the researchers can gain a clearer understanding of the challenges faced, particularly regarding issues of data loss and weak access control within the Claim Management System. This method also enables the identification of practical problems that may not be fully captured through documentation or secondary data, as staff can share their experiences, observations, and opinions about the effectiveness of existing processes and controls.[15]

In addition, interviews serve as a valuable tool for validating findings from other data collection methods, such as literature reviews and documentation analysis. By combining perspectives from staff with theoretical and documented evidence, the study provides a more comprehensive and accurate assessment of the situation. The insights gained through interviews also support the evaluation of IT governance practices based on COBIT 2019 and the identification of relevant information security controls in ISO/IEC 27001:2022, thereby making the recommendations more practical and aligned with the organization's actual conditions.

2.5. Questionnaire

The maturity assessment questionnaire is designed based on ISO/IEC 27001:2022 Annex A controls and relevant COBIT 2019 domains. This questionnaire serves as a structured instrument for evaluating the organization's current practices in information security and IT governance. By aligning the questions with established international standards and frameworks, the assessment ensures that the evaluation process is both comprehensive and measurable. It enables the organization to determine its current maturity level in managing information security, business continuity, compliance, and IT operations.

Furthermore, the use of the questionnaire provides a systematic way to capture input from different stakeholders within the organization. Their responses offer valuable insights into the effectiveness of existing security controls and governance processes. The results of this maturity assessment can then be used to identify gaps between the current state and the target maturity level, thereby supporting the development of actionable recommendations for improvement. This approach ensures that the proposed solutions are evidence-based and aligned with recognized best practices.

2.6. Maturity Analysis

At this stage, after obtaining results from interviews and questionnaires, a comprehensive analysis is carried out to determine the organization's overall maturity level. The data collected through these instruments serve as the primary source of evidence for evaluating the effectiveness of existing processes. Each response is carefully examined and categorized to identify strengths, weaknesses, and potential gaps in alignment with established standards. The maturity level can only be considered achieved if all related processes consistently meet or exceed the required maturity value. This ensures that the evaluation reflects not only isolated improvements but also the organization's collective capability to maintain, implement, and continuously improve its processes in a structured manner. By following this method, the assessment provides a reliable and objective measure of the organization's current maturity, which can then serve as a foundation for future recommendations and improvement plans.[16]

2.7. Gap Analysis

At this stage, after determining the maturity value, the results are further examined by comparing the obtained maturity level with the expected or targeted level defined by the organization. This comparison is crucial as it highlights the gaps between the current state and the desired state of process capability and governance practices. By identifying these gaps, organizations can gain a clearer understanding of areas that require improvement, prioritize processes that need immediate attention, and develop action plans to gradually close the maturity gap. Furthermore, the comparison provides valuable insights into whether the implemented strategies and controls effectively support organizational goals or if adjustments are necessary to align with industry standards and best practices. Ultimately, this step ensures that the maturity assessment is not only a measurement exercise but also a decision-making tool that guides continuous improvement and strategic alignment.[17]

2.8. Recommendation

Risk recommendations are developed using the ISO/IEC 27002:2022 framework, specifically by applying the clauses related to information security. This approach provides structured guidance for identifying, assessing, and mitigating risks that may threaten the confidentiality, integrity, and availability of information assets. By leveraging the controls and best practices outlined in ISO/IEC 27002:2022, organizations can establish a systematic method to address potential vulnerabilities, strengthen their security posture, and ensure compliance with internationally recognized standards. Furthermore, this process enables organizations to align risk management strategies with business objectives, enhance stakeholder trust, and build a sustainable foundation for continuous improvement in information security governance.

2.9. Conclusion

After conducting the research, the researcher draws conclusions based on the findings obtained throughout the study and provides suggestions for future work. The conclusions summarize the key outcomes, highlight the significance of the results, and reflect on how the study's objectives have been achieved. In addition, the researcher identifies limitations encountered during the research process, such as constraints in scope, data availability, or methodological challenges, which may have influenced the results. These limitations create opportunities for future studies to refine the approach, apply different methodologies, or expand the research context for broader insights. The suggestions for future research are intended to guide scholars, practitioners, and organizations in building upon the current findings, addressing existing gaps, and contributing to the ongoing development of knowledge in the field. In doing so, the research not only concludes its present inquiry but also lays the foundation for further exploration and continuous improvement.

3. RESULT AND DISCUSSION

At this stage, we will further discuss the data collection process and data processing carried out to obtain the results of data grouping. This process is very important to ensure that the information collected is relevant and can be processed with the right method to produce groups that suit the purpose of the research or analysis.

3.1. Maturity Level by COBIT 2019

The results of the questionnaire that has been given to the respondent and have been filled in by the respondent then get the results.

Table 1. Maturity Level COBIT 2019

Domain	Cobit 2019 Process	Current Level	Target Level	Gap
DSS04	Manage Continuity	3	3	0
DSS01	Manage Operations	3	3	0
BAI06	Manage Changes	4	3	0
APO13	Manage Security	3	3	0
MEA01	Monitor, Evaluate, and Assess Performance and Conformance	3	3	0
MEA03	Monitor, Evaluate, and Assess Compliance	3	3	0

Almost all processes indicate that the Current Level is already aligned with the Target Level, which means PT XYZ has achieved the defined process capability standards, and therefore no gap needs to be addressed.

DSS04 – Manage Continuity

Business continuity is documented, implemented, and maintained as required.

BAI06 – Manage Changes

PT XYZ is more mature than the target. Therefore, there is no gap. The change management process at PT XYZ is well managed and even exceeds expectations.

APO13 – Manage Security

The information security management process is aligned with the target and is supported by documented and implemented procedures.

DSS01 – Manage Operations

The IT operations processes at PT XYZ are standardized, executed, and measured in alignment with organizational needs

MEA01 – Monitor, Evaluate, and Assess Performance and Conformance

The process of monitoring performance and ensuring compliance with internal standards and regulations is already aligned with expectations.

MEA03 – Monitor, Evaluate, and Assess Compliance

The process of monitoring compliance with external regulations is adequate and meets expectations.

3.2. Control ISO/IEC 27001:2022

From the results of the maturity level assessment conducted using the COBIT 2019 framework, no gaps were identified. Therefore, this study provides recommendations based on ISO/IEC 27001:2022.

Table 2. Control ISO/IEC 27001:2022

COBIT 2019 Process	ISO/IEC 27001:2022 Control	Recommendation
DSS04 – Manage Continuity	A.5.29 (Information security during disruption) A.5.30 (ICT readiness for business continuity)	Conduct regular BCP/DRP testing (table-top and simulation tests) to ensure readiness in facing incidents. Document the test results as evidence of continuous improvement.
DSS01 – Manage Operations	A.8.15 (Logging) A.8.16 (Monitoring activities)	Enhance incident detection by strengthening logging and monitoring, for example by using SIEM for real-time analysis.
BAI06 – Manage Changes	A.8.32 (Change management)	Since the level is higher than the target, document the lessons learned from every major change. Implement security controls in the change management process to ensure the focus is not only on system stability.
APO13 – Manage Security	A.5 (Organizational controls) A.8 (Technology controls)	Integrate all security controls into the ISMS. Ensure that security policies, roles, and responsibilities are documented. Implement continuous improvement (PDCA).
MEA01 – Monitor, Evaluate and Assess Performance & Conformance	A.5.41 (Performance monitoring)	Evaluate the effectiveness of controls using KPI/KRI.

		Based on security risks to ensure monitoring is more proactive rather than merely administrative.
MEA03 – Monitor, Evaluate and Assess Compliance	A.5.31 (Regulatory and contractual requirements)	Create compliance mapping of regulations and contracts (e.g., GDPR, PDP Law, PDPA, PCI DSS) and conduct regular reviews to ensure the organization always complies with applicable laws.

4. CONCLUSION

The results of this study show that the maturity level of information security management at PT XYZ, evaluated using the COBIT 2019 framework, has met the defined targets, with several processes even exceeding expectations. This indicates that the company has implemented adequate governance and control mechanisms in areas such as continuity management, change management, information security, operations, and compliance monitoring. Based on these findings, recommendations were developed using ISO/IEC 27001:2022 controls to strengthen continuous improvement, particularly in testing business continuity and disaster recovery plans, documenting lessons learned from major changes, integrating security controls into the ISMS, enhancing incident detection, and ensuring ongoing regulatory compliance. These results confirm that the integration of COBIT 2019 and ISO/IEC 27001:2022 provides a comprehensive framework for improving IT governance and information security. Future research may apply this approach in different organizational contexts or industries to validate its effectiveness and identify additional opportunities for enhancement.

5. REFERENCE

[1] N. Kadek Widiartini, A. Agung Hary Susila, and P. Veda Andreyana, “Security Risk Evaluation of Licensing System Using NIST SP 800-30 Framework and Maturity Level with CMMI.”

[2] D. Dinda, B. Rama Dika, R. Mulyana, and M. Lubis, “Utilization of ISO 27001:2022 In Designing Information Security for Digital Transformation at BPRCO SME.”

[3] R. Rakan, R. Mulyana, and M. Lubis, “Utilizing ISO 27001:2022 to Design Information Security for BPRACo SME Digital Transformation,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 6, no. 4, pp. 820–831, Oct. 2024, doi: 10.47233/jteksis.v6i4.1621.

[4] L. D. Fitrani, “Risk Assessment And Development Of Access Control Information Security Governance Based On ISO/IEC 27001:2013 At XYZ University,” *Risk Assessment And Development Of Access Control Information Security Governance Based On ISO/IEC*, vol. 9, no. 2, 2022, [Online]. Available: http://jurnal.mdp.ac.id

[5] A. Viamianni, R. Mulyana, and F. Dewi, “COBIT 2019 INFORMATION SECURITY FOCUS AREA IMPLEMENTATION FOR REINSURCO DIGITAL TRANSFORMATION,” *JIKO (Jurnal Informatika dan Komputer)*, vol. 6, no. 2, Aug. 2023, doi: 10.33387/jiko.v6i2.6366.

[6] N. R. Fachrur Rozi, A. Agustav Wirabudi, and S. Arandiant Rozano, “Chance Evaluation and Improvement of Get to Control Data Security Administration Based On ISO/IEC 27001 at Telkom University Jakarta Campus,” *International Journal of Science Education and Cultural Studies*, vol. 3, no. 2, pp. 1–26, Jun. 2024, doi: 10.58291/ijsecs.v3i2.246.

[7] M. Suorsa and P. Helo, “Information security failures identified and measured–ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis,” *Information Security Journal*, vol. 33, no. 3, pp. 285–306, 2024, doi: 10.1080/19393555.2023.2270984.

[8] “Enhancing Information Security Management System using ISO controls-based framework. Enhancing Information Security Management System using ISO controls-based framework.”

[9] S. Meitarice, L. Febyana, A. Fitriansyah, R. Kurniawan, and R. A. Nugroho, “Risk Management Analysis of Information Security in an Academic Information System at a Public University in Indonesia: Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 Security Controls,” *Journal of Information Technology and Cyber Security*, vol. 2, no. 2, pp. 58–75, Nov. 2024, doi: 10.30996/jitcs.12099.

[10] A. Y. El-Bably, “Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management,” *Journal of Information Security and Cybercrimes Research*, vol. 4, no. 1, pp. 95–102, Jun. 2021, doi: 10.26735/wlpw6121.

[11] R. Purnomo and R. Harwahyu, “Risk Management Analysis in Digital Bank XYZ Using the COBIT 2019 Framework,” *MALCOM: Indonesian Journal of Machine Learning and Computer Science*, vol. 5, no. 3, pp. 1012–1018, Jul. 2025, doi: 10.57152/malcom.v5i3.1876.

[12] A. Intan Mafiana, L. Hanun, H. Mufidatul Ilmi, and S. Febriliani, “Implementasi Manajemen Keamanan Informasi Berbasis ISO 27001 Pada Sistem Informasi Akademik Universitas,” *Journal of Digital Business and Innovation Management JDBIM (Journal of Digital Business and Innovation Management*, vol. 2, no. 2, pp. 139–163, 2023, doi: 10.1234/jdbim.v2i2.57580.

[13] E. Susanto, “Hasil Penilaian Risiko Keamanan Informasi pada Laboratorium Klinik Berdasarkan Kriteria Kendali Dalam Penerapan ISO 27001,” *Jurnal Rekayasa Sistem Industri*, vol. 12, no. 2, pp. 155–164, Oct. 2023, doi: 10.26593/jrsi.v12i2.6315.155-164.

[14] . S. and F. Ajismanto, “Implementation Evaluation of Information Technology in the New Normal Era Using Cobit 2019 Method,” *KnE Social Sciences*, May 2023, doi: 10.18502/kss.v8i9.13318.

[15] A. Aminudin *et al.*, “Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001:2013 (Studi kasus: Bapenda Provinsi Jawa Tengah),” *AITI: Jurnal Teknologi Informasi*, vol. 21, no. 2, pp. 210–229, 2024.

[16] S. Samsinar and R. Sinaga, “Information Technology Governance Audit at XYZ College Using COBIT Framework 2019,” *BERKALA SAINSTEK*, vol. 10, no. 2, p. 58, Jun. 2022, doi: 10.19184/bst.v10i2.30325.

[17] M. Asriannoor, “89 Asrian-Maturity Level Analysis of FT ULM Service System Using The Cobit 2019 Framework T MATURITY LEVEL ANALYSIS OF FT ULM SERVICE SYSTEM USING THE COBIT 2019 FRAMEWORK.”