Evaluation of Maturity Level Information Security Using COBIT 2019 and ISOIEC.pdf

by Uji Turnitin

Submission date: 07-Sep-2025 11:40PM (UTC-0400)
Submission ID: 2696107959
File name: Evaluation_of_Maturity_Level_Information_Security_Using_COBIT_2019_and_ISOIEC.pdf (298.21K)
Word count: 4373
Character count: 25306

JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK,
No.0173/C3/DT.05.00/2025
Vol. x, No. x, April 2024, pp. x-x p-ISSN: 2614-8897
DOI: 10.33387/jiko 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] Faculty of Communication and Information Technology, Universitas Nasional
*Email: [1]zahracha41@gmail.com, [2]agungtriayudi@civitas.unas.ac.id

(Received: dd mmm yyyy, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

Abstract

Information security plays a critical role in ensuring the reliability and continuity of business processes, particularly in the retail sector where data integrity is essential for claim validation and payment systems. PT XYZ developed a Claim Management System to support transparency and efficiency in managing incentive claims. However, the company faced recurring challenges such as frequent data loss and weak access control, which disrupted operations and created risks to business continuity. This study aims to evaluate the maturity level of information security management at PT XYZ using the COBIT 2019 framework and to identify relevant controls from ISO/IEC 27001:2022 as a basis for improvement. A descriptive-comparative method was employed, combining questionnaires, interviews, and domain mapping to assess the maturity of IT governance processes. The findings show that PT XYZ has achieved its targeted maturity level in all assessed domains, with some processes exceeding expectations. Although no significant gaps were found, recommendations were formulated based on ISO/IEC 27001:2022 controls, including regular business continuity and disaster recovery testing, documentation of lessons learned, integration of security controls into the ISMS, enhanced monitoring through real-time analysis, and compliance mapping with regulatory requirements. The study concludes that integrating COBIT 2019 and ISO/IEC 27001:2022 provides a comprehensive framework for strengthening IT governance and information security. These results offer practical implications for improving organizational resilience, while future research may extend this approach to different industries for comparative analysis.

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 in the retail sector is essential to support the claim payment monitoring system.[1] The function of Information Technology (IT) in business is also required to enhance effectiveness, efficiency, and the security of customer data in every service provided. Currently, many companies across various industries, including the retail industry, are driven to implement IT as part of their digital transformation efforts to maintain data integrity.[2]

PT. XYZ, a company engaged in the retail sector, has utilized information technology in its business operations. To support transparency and efficiency in the incentive claim process, PT. XYZ developed a Claim Management System that enables dealers to submit claims based on sales data they input into the system. Claim validation is carried out based on the data submitted by the dealers, which serves as the basis for the company to process payments to them. This is aimed at building and maintaining the trust of business partners. It is expected that the system will be able to produce complete, accurate, and high-quality outputs.[3]

However, in its implementation, PT. XYZ still faces several serious challenges related to information security and system management.[4] One of the problems is that sales data submitted by dealers was lost due to an error caused by someone editing the data

in the system. This resulted in the loss of sales data, requiring dealers to resubmit their sales, which hindered validation and disrupted operational continuity.

COBIT 2019 stands for Control Objectives for Information and Related Technology, which is a framework that helps shape IT strategies, processes, and operations, as well as measure IT management and IT governance administration skills to achieve better optimization.[5]

ISO/IEC 27001 is a standard for the Information Security Management System (ISMS) issued by the International Organization for Standardization (ISO) in 2022. This standard contains specifications or requirements that must be fulfilled to establish an information security management system. ISO/IEC 27001 provides guidance for companies of various sizes and sectors to develop, implement, maintain, and continuously improve their information security management systems. The standard adopts a risk management–based approach. Its objective is to ensure that the implemented controls are capable of protecting information assets from various risks, thereby increasing security assurance for interested parties. The implementation of this ISMS must be supported by planning, security policies, programs (procedures and processes), risk assessment, and human resources)[6]

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. At present, 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 the organization's vision and mission.[7]

The function of Information Technology (IT) in business is also required to improve effectiveness, efficiency, and the security of customer data in every service provided. Currently, many companies across various industries, including the banking industry, are driven to implement 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, with a focus on the COBIT 2019 framework. Furthermore, in other types of financial industries, previous research has also focused on information security governance, such as in insurance companies and fintech firms.[9]

The need to implement COBIT 2019 and ISO/IEC 27001:2022 in this study is based on the necessity to address issues of data loss, system changes without adequate control, and their impact on the continuity of business relationships.[10] ISO/IEC 27001:2022 focuses on information security protection through the implementation of policies such as backup, access control, and change management procedures.[11]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 address technical issues while simultaneously strengthening overall IT governance at PT XYZ.[12]

Based on the problems described, this study has several objectives. First, to analyze the issues of data loss and weak access control in the Claim Management System at PT XYZ. Second, to evaluate the alignment of information technology management at PT XYZ with the COBIT 2019 framework. Third, to identify relevant information security controls from the ISO/IEC 27001:2022 standard in addressing data loss and system change management. Fourth, to propose recommendations for improving IT governance and information security through the integration of COBIT 2019 and ISO/IEC 27001:2022.

In line with these objectives, this study seeks to answer several research questions: what are the main issues related to data loss and weak access control in managing the Claim Management System at PT XYZ, what is the level of IT process capability at PT XYZ based on COBIT 2019, which information security controls from ISO/IEC 27001:2022 are relevant to address these issues, and how can PT XYZ 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 will be used to measure the maturity level and to recommend improvements. The issues of frequent data loss and user access control, identified as problems within PT XYZ, specifically concerning security in the Claim Management System, will be addressed through the standards and guidelines of ISO/IEC 27001:2022 and COBIT 2019. The results of applying this method will be 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 an 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, thus providing a practical illustration of governance mechanisms and controls in place.

The approach applied is a quantitative method (through maturity scoring and questionnaires). This design allows 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. The research subjects consist of IT staff.

Data collection is carried out through the following methods :

2.1. Problem Identification

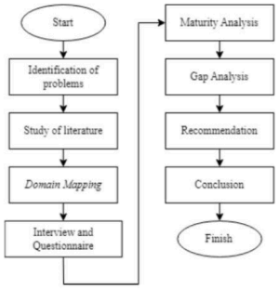

Figure 1. Research Stage

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 due to weak access control mechanisms that allow unauthorized modifications or deletions of data within the system. As a result, dealers are required to re-submit their sales data, which significantly disrupts the validation process and delays claim payments.

These recurring issues not only hinder operational efficiency but also create risks to business continuity and trust between the company and its partners. Since data is a critical asset in ensuring transparent and accurate claim validation, the lack of proper security controls compromises the integrity and reliability of the system. Without immediate improvement, 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 control and ensuring reliable data management are necessary steps to minimize the risk of data loss and improve the overall effectiveness of the Claim Management System.[13]

2.2. Literature Review

The literature review is conducted by examining a wide range of theoretical information collected 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 is able to identify key concepts, frameworks, and findings that are relevant to the problem under investigation.

Furthermore, the literature review allows the researcher to map 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.[14]

2.3. Domain Mapping

The COBIT 2019 framework domain mapping at this stage is carried out 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, 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.[15]

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, researchers can obtain a clear understanding of the challenges faced, particularly regarding issues of data loss and weak access control within the Claim Management System. This method also allows 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.[16]

In addition, interviews serve as a valuable tool to validate findings from other data collection methods, such as literature review and documentation analysis. By combining perspectives from staff with theoretical and documented evidence, the study ensures a more comprehensive and accurate assessment of the situation. The insights gained through interviews will 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, making the recommendations more practical and aligned with the organization's real 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 to evaluate 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 allows the organization to identify its current maturity level in managing information security, 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, 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

In this stage, after obtaining results from interviews and questionnaires, a comprehensive analysis is carried out to determine the overall maturity level of the organization. The data collected through these instruments serve as the primary source of evidence to evaluate 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 reach or surpass 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 enhance its processes in a structured manner. By following this method, the assessment provides a reliable and objective measurement of the organization's current maturity, which can then serve as a foundation for future recommendations and improvement plans.[17]

2.7. Gap Analysis

In this stage, after determining the maturity value, the results are further examined by comparing the obtained maturity level with the expected or targeted maturity level defined by the organization. This comparison is crucial, as it highlights the existing 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 which processes 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 are effectively supporting 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.[18]

2.8. Recommendation

Risk recommendations are developed using the ISO/IEC 27002:2022 framework procedures, 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 the organization to align its risk management strategies with business objectives, enhance stakeholder trust, and create 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 research. The conclusions summarize the key outcomes, highlight the significance of the results, and reflect on how the objectives of the study 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 open 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 aimed at guiding scholars, practitioners, and organizations to build upon the current findings, address existing gaps, and contribute to the ongoing development of knowledge in the related field. By doing so, the research not only concludes its present inquiry but also lays a 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

Domain	Cobit 2019 Process	Current Level	Target Level	GAP
DSS04	Manage Continuity	3	3	0
BAI06	Manage Changes	4	3	0
APO13	Manage Security	3	3	0
DSS01	Manage Operations	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 here show that the Current Level is already the same as the Target Level, which means PT XYZ has achieved the defined process capability standards, so there is no GAP that needs to be addressed.

DSS04 – Manage Continuity

Business Continuity has been 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, even exceeding expectations.

APO13 – Manage Security

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

DSS01 – Manage Operations

IT operations processes at PT XYZ are standardized, executed, and measured according to organizational needs.

MEA01 – Monitor, Evaluate and Assess Performance and Conformance

The process of monitoring performance and compliance with internal standards/regulations is already in line with expectations.

MEA03 – Monitor, Evaluate and Assess Compliance

The process of monitoring compliance with external regulations is also adequate.

3.2. Control ISO/IEC 27001:2022

From the results of the maturity level assessment conducted using the COBIT 2019 framework, it was found that there is no gap. 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 (Annex A)	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.
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).
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.
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

COBIT 2019 Process	ISO/IEC 27001:2022 Control (Annex A)	Recommendation
		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 the expected level. 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 can provide 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 further 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] R. Ferdinandsyah, A. Novita, D. Atmodjo, and F. D. Nugroho4, "Enhancing Access Control Security Using ISO 27001:2013 and OCTAVE Method," *bit-Tech*, vol. 8, no. 1, pp. 459–466, Aug. 2025, doi: 10.32877/bt.v8i1.2590.

[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] A. Safira Wahab, R. Bianco, and A. Hidayat Jatmika3, "Information Systems Security Risk Management Using the COBIT 2019

Framework and NIST 800-30 on the Website People's Representative Council NTB."

[12] 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.

[13] 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.

[14] 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.

[15] . 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.

[16] 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.

[17] 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.

[18] 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."

Evaluation of Maturity Level Information Security Using COBIT 2019 and ISOIEC.pdf

ORIGINALITY REPORT

18%	10%	10%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.pkm.tunasbangsa.ac.id Internet Source	3%
2	Submitted to Universitas Prima Indonesia Student Paper	2%
3	Muhamad Rendi Novrian, Erick Dazki. "Evaluation of Information Technology Governance Maturity Using COBIT 2019: Study of a Telecommunication Company", INOVTEK Polbeng - Seri Informatika, 2025 Publication	1%
4	www.grafiati.com Internet Source	1%
5	Submitted to Lambung Mangkurat University Student Paper	1%
6	www.isms.online Internet Source	1%
7	Jriesat, Elias Radi. "The Power of it Governance when Applied on Key Divisions in Financial Institutions (I.T - I.S- Risk - Audit).", Debreceni Egyetem (Hungary), 2024 Publication	1%
8	Al-Kalbani, Hajer Rashid Khalfan. "Investigating the Information Systems Security of E-Learning Knowledge Management Systems in Higher Education Institutions in Oman", Sultan Qaboos University (Oman), 2025	1%

	Publication	
9	www.coursehero.com Internet Source	1 %
10	Bel G. Raggad. "Information Security Management - Concepts and Practice", CRC Press, 2019 Publication	<1 %
11	Submitted to Munster Technological University (MTU) Student Paper	<1 %
12	ejournal.unkhair.ac.id Internet Source	<1 %
13	globalregulatoryinsights.com Internet Source	<1 %
14	Dwi Tia Shavera, Didik Kurniawan, Yunda Heningtyas. "AUDIT LAYANAN TEKNOLOGI INFORMASI RUMAH SAKIT XYZ MENGGUNAKAN FRAMEWORK COBIT 5.0 (CONTROL OBJECTIVE FOR INFORMATION AND RELATED TECHNOLOGY)", Jurnal Pepadun, 2021 Publication	<1 %
15	Submitted to Adtalem Global Education Student Paper	<1 %
16	Submitted to University of Wollongong Student Paper	<1 %
17	ijeais.org Internet Source	<1 %
18	eprints.unram.ac.id Internet Source	<1 %
19	www.mdpi.com Internet Source	<1 %

20	"Table of contents", 2018 4th International Conference on Nano Electronics Research and Education (ICNERE), 2018 Publication	<1 %
21	grominfo.eu Internet Source	<1 %
22	knepublishing.com Internet Source	<1 %
23	www.pjr.com Internet Source	<1 %
24	"TM311 week 19 information security risk management WEB106587 ", Open University Publication	<1 %
25	Djarot Hindarto. "Enterprise Architecture Development to Strengthen Sustainability in the Supply Chain", Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi), 2023 Publication	<1 %
26	Submitted to Fakultas Ekonomi Universitas Indonesia Student Paper	<1 %
27	osuva.uwasa.fi Internet Source	<1 %
28	Park, Changki. "Cybersecurity Risk Assessment in the Maritime Industry", Liverpool John Moores University (United Kingdom), 2024 Publication	<1 %
29	Vladas Leonas, Sorin Toma. "Cyber Insecurity - Examining the Past, Defining the Future", CRC Press, 2025 Publication	<1 %
30	addi.ehu.eus Internet Source	<1 %

31	journal.jis-institute.org Internet Source	<1%
32	Erdivan, Halime Eda Bitlisli. "An Information Security Assessment Model for Very Small Entities", Middle East Technical University (Turkey), 2024 Publication	<1%
33	Heemeng Ho, Ryan Ko, Lorraine Mazerolle, John Gilmour, Cheng Miao. "Using Situational Crime Prevention (SCP)-C3 cycle and common inventory of cybersecurity controls from ISO/IEC 27002:2022 to prevent cybercrimes", Journal of Cybersecurity, 2024 Publication	<1%
34	Eloff, M. M.. "Towards an Information Security Framework for Government to Government Transactions : a Perspective from East Africa", University of South Africa (South Africa) Publication	<1%
35	Styles, Christopher. "The Rise of Mobile Malware: Challenges in Securing Mobile Banking Applications in Metropolitan Atlanta's Financial Services Sector.", National University Publication	<1%
36	core.ac.uk Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		