Ranah Research:
Journal of Multidisciplinary Research and Development
082170743613 ranahresearch@gmail.com https://jurnal.ranahresearch.com
E-ISSN: 2655-0865
DOI: https://doi.org/10.38035/rrj.v6i6

Utilizing ISO 27001:2022 In Information Security Design For BPRCCo SME Digital Transformation

Fandi Ahmad Atqan Setyoso[1], Rahmat Mulyana[2], Ryan Adhitya Nugraha[3]
[1]Department of Information System, Telkom University, Bandung, Indonesia, fandisetyoso@student.telkomuniversity.ac.id
[2]Departement of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden, rahmat@dsv.su.se
[3]Departement of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden, ryan.nugraha@dsv.su.se

Corresponding Author: fandisetyoso@student.telkomuniversity.ac.id

Abstract: In the era of Industry 4.0, incumbent organizations like BPRCCo must undergo Digital Transformation (DT) to remain competitive. However, a significant challenge in this process is ensuring information security, a critical factor often leading to the failure of DT initiatives. Previous studies have emphasized the importance of ambidextrous information security management—balancing traditional and agile approaches—for large banks in achieving successful DT, particularly concerning information security. However, this approach has yet to be validated for small-scale banks like BPRs. Therefore, this research aims to develop tailored recommendations for an Information Security Management System (ISMS) suitable for Small and Medium Enterprises (SME) and assess the potential enhancements in their capabilities to support DT. The research employs Design Science Research (DSR) methodology, encompassing problem identification, requirements specification, design and development, demonstration, and evaluation phases. Data was gathered through interviews and data analysis, and subsequently analyzed using the ISMS framework aligned with the ISO 27001:2022 standard. The risk analysis and review of previous studies revealed that 29 control in the PDCA cycle and Annex are critical priorities for BPRCCo. Based on this, several ISMS-based solutions were designed. These recommendations are presented as an implementation roadmap that can guide BPRCCo in preparing and fully implementing ISMS in crucial areas to support its DT efforts. This research contributes to the understanding of ISMS in small-scale banking, offering valuable insights through a case study approach relevant to SMEs and similar organizations.

Keyword: Digital Transformation, Design Science Research, Information Security, ISO 27001:2022, BPR.

INTRODUCTION

Rapid technological changes and developments require companies to carry out digital transformation (DT) in order to adapt effectively and quickly (Panggabean, 2021). DT is a

process carried out by organizations to improve service performance, enhance customer experience, direct operations, and create new business models (Gong et al., 2020). In this context, every organization is required to be able to adapt by utilizing technology through digital transformation.

In previous studies, it has been found that many ITG mechanisms affect TD (Mulyana et al., 2021a). It is also found that digital transformation has helped organizations in providing the digital solutions they need through digital innovation (Mulyana et al., 2021b). It was also revealed that digital transformation has a great influence on TKTI on organizational performance, especially banking in Indonesia (Mulyana et al., 2023). Ambidextrous Data and Information mechanisms are very important to direct the success of digital transformation (Mulyana et al., 2024b). In addition, one of the key ambidextrous IT governance mechanisms on digital transformation are related to data and information (Mulyana et al., 2024a). Thus, digital transformation and TKTI are very important for organizations to improve the delivery of IT business value and mitigate IT risks (De Haes et al., 2020).

Prior literature also emphasizes the importance of IT services (Tarbiyatuzzahrah et al., 2023), IT risk management (Dwi et al., n.d.), information security (Rahmadana et al., n.d.), and DevOps practices (Riznawati et al., 2023) as foundational to digital transformation in large banking institutions, drawing from some focus areas of COBIT 2019 framework. Similar research has also been conducted on the governance of information security within other sectors of the financial industry, including insurance companies (Anugerah, 2023)(Viamianni et al., 2023) and fintech firms (Prayudi et al., 2023).

According to Indonesian Law No. 20 Article 1 of 2008 concerning Micro, Small and Medium Enterprises, the definition of SME is a productive economic enterprise that stands alone and is carried out by individuals or business entities that are not subsidiaries or branches of companies that are owned, controlled, or are part of either directly or indirectly from Small Businesses or Large Businesses with the amount of net assets or annual sales results as regulated in the Law (Suci, 2017). Therefore, this study focuses on medium-sized businesses that are part of SME.

Moreover, ISMS is a standard that is often used by companies to implement information system security (Panjaitan et al., 2021). ISO 27001 is an example that emphasizes the standard requirements for ISMS (Muthaiyah & Zaw, 2018). Furthermore, ISO 27001 applies to all businesses that have information security in any form (Hartati, 2017). The focus of ISO 27001 is the planning, implementation, and operation of continuously monitoring and improving the ISMS (Disterer, 2013).

Therefore, TD is very important for organizations in their business processes to improve efficiency and effectiveness. Not only large organizations, but SME can also perform TD journey to increase productivity. However, the implementation of TD also has negative impacts that need to be addressed. Therefore, this research seeks to explore crucial aspects of creating an information security management system specifically designed for DT in SME. The study will focus on two primary questions. 1) How can the implementation of the ISO 27001:2022 standard be identified and adapted to develop an information security management system that emphasizes the annex clauses most pertinent to the digital transformation of SME? 2) What is the extent of the impact that aligning an information security management system with the key clauses of ISO 27001:2022 has on the success of digital transformation in SME?

METHOD

Conceptual Model

This study uses Hevner framework of thought. This conceptual model is very important for research because it aims to help researchers organize problems, find relevant factors, and map the relationships between one and another to find out the main problems that must be solved (Hevner et al., 2004).

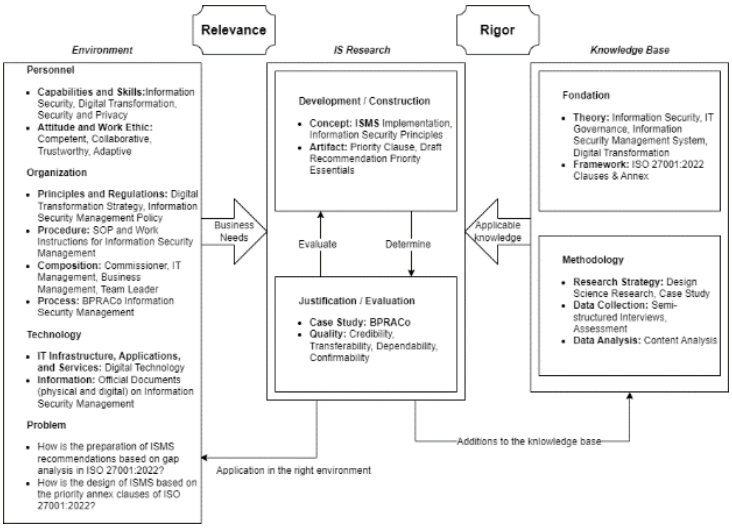

Figure 1. Conceptual Model Of DSR Hevner

Error! Reference source not found. is based on Hevner's framework consisting of three main parts, namely environment, Information System (IS) research, and knowledge base (Hevner et al., 2004). These parts can be used as a reference to define problems, determine relevant factors, and facilitate mapping of the core of the problem. As for the explanation of these three main parts, the first is *1) Environment* divided into four components: Personnel, Organization, Technology, and Problems, *2) IS Research*, Development/Building and Justification/Evaluation, and *3) Knowledge Base,* Foundation and Methodology.

Research Process

The research process are the guiding steps taken to solve problems in research.

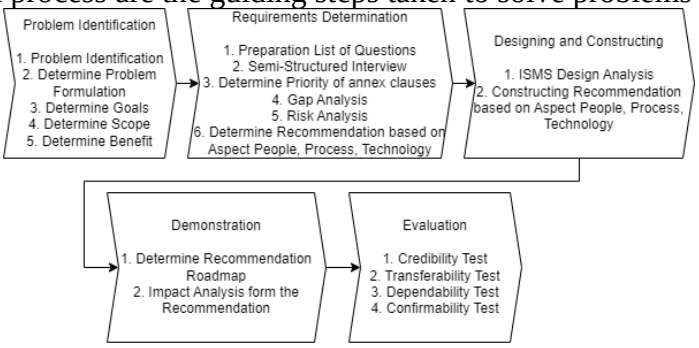

Figure 1 Research Process

Figure 1 Research Process is the systematic problem solving in this study. In the systematic problem-solving stage, there are 5 stages, namely the problem identification stage, the requirements determination stage, the design and constructing, and the evaluation stage.

Data Collection

The data collection process is the process of collecting data that will be processed into information needed in research. In the data collection process, 2 types of data are collected, namely primary data and secondary data with qualitative methods.

Table 1 Interview Activities

No.	Interview Date	Source Person	Topic
1.	14 March 2024	Director of Operations Business Director Director of Compliance Information Technology	Initial visit and introduction regarding the purpose and objectives of the research and request for data required for the ISO 27001:2022 assessment.
2.	15 March 2024	Director of Operations Information Technology	Understand the object's Information Security Management System and perform data analysis required for ISO 27001:2022 assessment.

No.	Interview Date	Source Person	Topic
3..	24 June 2024	Director of Operations Business Director Director of Compliance Information Technology	Online interviews related to data required for the assessment of the main clauses and annexes that have not been completed.

Table 1 Interview Activities explained about semi-structured interviews can provide an opportunity to look deeper into how the organization responds to each question. As long as the previous questions have been answered well, the researcher can add questions that he wants to ask.

Interviews were conducted until no further meaningful data could be obtained, indicating that data saturation had been reached. Multiple interview sessions were held to ensure a thorough exploration of the subject matter (Fuchs & Ness, 2015).

RESULTS AND DISCUSSION

Clauses Prioritization

To conduct an analysis of the current condition of ISO 27001:2022 from BPRCCo, researchers prioritize the clauses and annexes of ISO 27001:2022 to suit digital transformation and SME. Researchers prioritize to suit digital transformation based on POJK and SEOJK regulations No. 75 (OJK 2016), ISMS SME research (Antunes, 2021; Ramadhan, 2022), and Previous Research (Mulyana, 2023 2022 2021). In this first prioritization of the main clauses, each clause will be given a weight of 100 and marked green if it meets the requirements of all assessments.

Table 2 PDCA Clauses Prioritization Results

ISO 27001:2022 Control List	3 TD References	Accumulated Score
4. Context fo the organization		
4.1 Understanding the organization and its context	✓	100
4.2 Understanding the needs and expectations of interested parties	✓	100
6. Planning		
6.1 Actions to address risks and opportunities	✓	100
6.3 Planning of changes.	✓	100
7 Physical controls		
7.1 Resources	✓	100
7.2 Competence	✓	100
7.4 Communication	✓	100
7.5 Documented information	✓	100
8. Operation		
8.1 Operational planning and control	✓	100
9. Performance evaluation		
9.1 Monitoring, measurement, analysis and evaluation	✓	100

Error! Reference source not found. there are 10 main clauses from ISO 27001:2022 that meet the three assessments.

In this first prioritization of Annex A, each Annex A will also be given a weight of 100 and marked green if it meets all the requirements. The following are the results of Annex Clauses Prioritization.

Table 3 Annex Clauses Prioritization Results

ISO 27001:2022 Control List	3 TD References	Accumulated Score
5. Organizational controls		
5.2 Information security roles and responsibilities	✓	100
5.9 Inventory of information and other associated assets	✓	100
5.12 Classification of information	✓	100
5.19 Information security in supplier relationships	✓	100

ISO 27001:2022 Control List	3 TD References	Accumulated Score
5.20 Addressing information security within supplier agreements	✓	100
5.22 Monitoring, review and change management of supplier services	✓	100
5.24 Information security incident management planning and preparation	✓	100
5.30 ICT readiness for business continuity	✓	100
5.31 Legal, statutory, regulatory and contractual requirements	✓	100
6. People controls		
6.2 Terms and conditions of employment	✓	100
6.6 Confidentiality or non-disclosure agreements	✓	100
7 Physical controls		
7.5 Protecting against physical and environmental threats	✓	100
7.11 Supporting utilities	✓	100
8. Technological controls		
8.6 Capacity management	✓	100
8.14 Redundancy of information processing facilities	✓	100
8.16 Monitoring activities	✓	100
8.21 Security of network services	✓	100
8.32 Change management	✓	100
8.34 Protection of information systems during audit testing	✓	100

Error! Reference source not found. there are 19 Annex from ISO 27001:2022 that meet the three assessments.

Gap Assessment

Gap assessment is a step taken to evaluate the identification of differences between current conditions and the standards set by ISO 27001:2022. The purpose of the gap assessment itself is to identify the extent to which BPRCCo has achieved the standards set by ISO 27001:2022 based on three aspects.

Table 4 Gap Assessment First Clause

No	Clause		Number of requirements in this Clause	Number of newly met requirements	Accumulated Score
1.	4	Context the of organization	2	2	100%
2.	6	Planning	2	1	50%
3.	7	Support	4	3	75%
4.	8	Operation	1	1	100%
5.	9	Performance evaluation	1	1	100%
Total			10	8	80%

Based on **Error! Reference source not found.**, The total clauses that have been fulfilled in BPRCCo are 8 out of 10 or around 80%.

Then the researcher also made a gap analysis of Annex A of ISO 27001: 2022 which has and has not met the standards at BPRCCo. the following are the results of the Annex A gap assessment at BPRCCo.

Table 5 Gap Assessment Annex A

No	Annex A		Number of requirements in this Annex A	Number of newly met requirements	Accumulated Score
1.	A.5	Organizational controls	9	8	89%
2.	A.6	People controls	2	2	100%

3.	A.7	Physical controls	2	2	100%
4.	A.8	Technological controls	6	7	86%
	Total		19	17	89%

Based on **Error! Reference source not found.**, the total Annex A that has been fulfilled at BPRCCo is 17 out of 19 or around 89%.

Findings

It is a step to identify findings from the main clauses and Annex A that have not been fulfilled by BPRCCo. This step aims to identify findings in meeting the standards set by ISO 27001:2022.

Table 6 Clause Findings

No	Clause		Finding
1.	6.3	Planning of changes	BPR has no information security change plan
2.	7.4	Communication	The Compliance Work Unit has conducted socialization of the latest information security provisions and refreshed the latest security regulations. however, communication has not been on target and has not been socialized to employees in a timely manner.

Based on **Error! Reference source not found.** In the main clauses, there are two ISO 27001: 2022 standards in BPRCCo that do not meet the standards. namely clauses 6.3 Planning of changes and 7.4 Communication. Then, researchers also get findings from Annex A ISO 27001: 2022 which does not meet the standards at BPRCCo.

Table 7 Annex A Finding

No	Annex A		Finding
1.	A.5.2	Information security roles and responsibilities	BPRCCo distributes roles and responsibilities in the GCG report, but optimization is still needed in improving employee performance, problem solving and responsibility for information security.
2.	A.8.32	Change management	BPR does not have a change plan so BPR does not have information security change management such as policies and procedures and identification and evaluation.

Based on **Error! Reference source not found.** In Annex A, there are two ISO 27001: 2022 Annex standards at BPRCCo that do not meet the standards. namely Annex A.5.2 Information security roles and responsibilities and A.8.32 Change management.

Prioritization Based on Risk Analysis

In the second priority using likelihood and impact analysis, it aims to adjust to SME. Priority of likelihood and impact analysis is used to determine the priority of the main clauses and annexes in making recommendations that are in accordance with SME.

Table 8 Likelihood and Impact Analysis

Impact	likelihood				
	Rare (1)	Unlike (2)	Possible (3)	Likely (4)	Certain (5)
Insignificant (1)	L(1x1)	L(1x2)	L(1x3)	L(1x4)	M(1x5)
Minor (2)	L(2x1)	L(2x2)	M(2x3)	M(2x4)	H(2x5)
Moderate (3)	L(3x1)	M(3x2)	M(3x3)	H(3x4)	H(3x5)
High (4)	L(4x1)	M(4x2)	H(4x3)	H(4x4)	E(4x5)
Major (5)	M(5x1)	H(5x2)	H(5x3)	E(5x4)	E(5x5)

The assessment can be seen in **Error! Reference source not found.**. From the results of this probability and impact analysis, the minimum score that can be obtained is 1 and the maximum is 25. Then, the next step is prioritizing the likelihood and impact analysis of the findings on BPRCCo that have not met the standards of ISO 27001: 2022.

Table 9 Analysis Results

Clause and Annex		Types of Threats	Likelihood score	Impact Score	Score	Risk level
6.3	Planning of changes	Lack of change planning	3	4	12	High
7.4	Communication	Communication is not timely	4	4	16	High
A.5.2	Information security roles and responsibilities	Employee performance is not optimal	4	4	16	High
A..8.32	Change management	Procedure document does not exist	3	4	12	High

In **Error! Reference source not found.** after prioritizing the likelihood and impact analysis, recommendations that are in accordance with SME will be taken from the results of the risk level with a high level and the level above. That way, the four main clauses and annexes will be compiled with recommendations for improvement and change plans in accordance with the ISO 27001:2022 standard.

People Aspect Design

In ISO 27001:2022, the recommendations for the people aspect relate to the recommendations needed to strengthen the human resources factor in order to maintain the ISMS in the company.

1) *Role recommendations*. This study recommends a division responsible for managing information security change management planning at BPRCCo, namely IT Planning & QA.
2) *Communication recommendations*. This study recommends using various communication channels to convey security information, such as email, bulletin boards, and instant messaging applications such as WhatsApp. With the aim of ensuring that security information reaches all employees in the most effective way, and methods by sending routine emails, and notifications via instant messaging applications such as WhatsApp.
3) *Skills & awareness recommendations*. This study recommends holding special training for employees on information security risk management, namely ISO 27001:2022 Lead Implementer Training, ISO 27001:2022 Risk Management and ISO 27001:2022 Certified Lead Implementer ISO 27001:2022 Certified Risk Manager Certification.

Process Aspect Design

In ISO 27001:2022, process aspect recommendations relate to recommendations needed to strengthen the process factors of organizational activities in the ISMS.

1) *Policy recommendations*. This study recommends several policies, namely:
   a. Information Security Management System Change Planning Policy
   b. Policy on the Implementation of Duties and Responsibilities of Company Members.
   c. Information Security Protection Policy when Executing Changes
2) *Procedure recommendations*. This study recommends several procedures, namely:
   a. Information Security Provisions Socialization Procedure
   b. Procedure for Protection of Information Security While Carrying Out Changes
   c. Procedure for Execution of Duties and Responsibilities of Company Members

Technology Aspect Design

In ISO 27001: 2022, the technology aspect recommendations relate to the recommendations needed to strengthen the IT infrastructure factor in order to maintain the ISMS in the company.

1) *Tools recommendations.* BPRCCo needs to improve communication by using various communication channels to convey security information, such as email. BPRCCo can use Microsoft outlook or Zimbra for email.

Implementation Roadmap

At this stage, the researcher will prepare a certification estimate according to the ISO 27001:2022 recommendation clause.

Table 10 Roadmap Recommendation

Activity	Period 2024			
	Sep	Oct	Nov	Dec
People Aspect				
6.3 Planning of Changes				
7.4 Communication				
A.5.2 Information security roles and responsibilities				
A.8.32 Change management				
Process Aspect				
6.3 Planning of Changes				
7.4 Communication				
A.5.2 Information security roles and responsibilities				
A.8.32 Change management				
Technology Aspect				
7.4 Communication				

The recommendation that BPRCCo can do first is to adjust clause 7.4 communication in September. Then it can be continued by adjusting Annex A.5.2 Information security roles and responsibilities in October, after that in November adjust clause 6.3 Planning of Changes, and finally in December adjust Annex A.8.32 Change management.

Research Discussion

Previous research explained that IT Governance mechanisms affect digital transformation (Mulyana et al., 2021b). IT Governance also affects digital transformation in the bank and insurance industry in Indonesia (Artha et al., 2022). In addition, Hybrid IT Governance has an effect on performance in the bank and insurance industry in Indonesia mediated by digital transformation (Mulyana et al., 2023). A landmark case study involving BRI, a leading bank in Indonesia, found seven ambidextrous ITG mechanisms that are important for successful digital transformation (Mulyana et al., 2024b). In addition, the study (Mulyana et al., 2024a) underscores the critical role of information security in achieving digital transformation goals, which reinforces the need for a strong digital and IT strategy to improve performance.

However, research on the use of the latest ISO, namely ISO 27001: 2022 in designing information security for the digital transformation of SME in BPRs does not yet exist. Therefore, the difference between this research and previous research is that this research focuses on the latest framework from ISO 27001: 2022 for digital transformation in BPR SME in Indonesia. Despite limited resources, BPRCCo can improve its information security effectiveness through a balanced approach that combines an agile response to security threats with steadfast traditional practices.

Lastly, the study went through four phases of quality testing to assess the effectiveness of the proposed solution as described in (Shenton, 2004). Credibility was ensured by using data from interviews, surveys, and document analysis, all of which were validated by ISO 27001 experts. Transferability was achieved by offering detailed descriptions of the BPR organization, allowing for assessments of adaptability in similar contexts. Dependability and confirmability were maintained through careful documentation, consistent methodologies, and the use of diverse data sources to minimize bias and uphold objectivity. All results were verified by experts and relevant stakeholders.

CONCLUSION

Based on the gap analysis that has been conducted in this study, it was found that the ISMS at BPRCCo still does not comply with the ISO 27001:2022 standard in its entirety. In the main clause of ISO 27001:2022; Clause 4 (Context of the Organization), Clause 8 (Operation), and Clause 9 (Performance Evaluation) have met the requirements of ISO

27001:2022, while Clause 6 (Planning), and Clause 7 (Support) have not fully met the requirements of ISO 27001:2022. This study also produced a draft ISMS. In the recommendations for the people aspect, there are proposals for new roles, new communication methods, and increased skills & awareness at BPRCCO and in the recommendations for the process aspect there are proposals for new policies and procedures at BPRCCO. This research has limitations only on recommendations for designing an ISMS, not on evaluating the implementation and results of designing an ISMS. The researcher hopes that this study can be used as a reference for implementing the ISO 27001:2022 framework in designing information security, especially for SME for digital transformation and can be used as a guide in designing and implementing new strategies and ISMS in the future.

REFERENCE

Anugerah, M. (2023). Manajemen Keamanan Informasi untuk Transformasi Digital Insurco Berbasis Cobit 2019 Focus Area Information Security. *Jurnal Sistem Informasi*, *5*(3), 452–467. https://doi.org/https://doi.org/10.31849/zn.v5i3.15275

Artha, U., Mulyana, R., & Ramadani, L. (2022). Analisis Kualitatif Pengaruh Tata Kelola TI Terhadap Transformasi Digital dan Kinerja: Studi Kasus Asuransi A. *JURIKOM (Jurnal Riset Komputer)*, *9*(5), 1302–1312. https://doi.org/10.30865/jurikom.v9i5.4797

De Haes, S., Caluwe, L., Huygh, T., & Joshi, A. (2020). *Management for Professionals Governing Digital Transformation*. http://www.springer.com/series/10101

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, *04*(02), 92–100. https://doi.org/10.4236/jis.2013.42011

Dwi, Y. W., Dewi, M., Mulyana, R., & Santoso, A. F. (n.d.). *Penggunaan COBIT 2019 I&T Risk Management untuk Pengelolaan Risiko Transformasi Digital BankCo*.

Gong, Y., Yang, J., & Shi, X. (2020). Towards a comprehensive understanding of digital transformation in government: Analysis of flexibility and enterprise architecture. *Government Information Quarterly*, *37*(3). https://doi.org/10.1016/j.giq.2020.101487

Hadiono, K., Candra, R., & Santi, N. (2020). Menyongsong Transformasi Digital. *Proceeding SENDIU*, 81–84.

Haikal, H., Ananza, R. H., Darmawan, I., & Mulyana, R. (2019). Design of Information Security Governance for E-Government Using ISO 27001:2013 Standard (Case Study: Diskominfotik of West Bandung Regency). *E-Proceeding of Engineering*, *6*(2), 8368–8374.

Halim, A. (2020). Pengaruh Pertumbuhan Usaha Mikro, Kecil dan Menengah Terhadap Pertumbuhan Ekonomi Kabupaten Mamuju. *Jurnal Ilmiah Ekonomi Pembangunan*, *1*(2), 157–172.

Hartati, T. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001:2013. *Jurnal Ilmiah Manajemen Informatika Dan Komputer*, *01*(02), 63–70. https://doi.org/https://doi.org/10.32485/kopertip.v1i02.24

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105. https://www.jstor.org/stable/25148625

Loonam, J., Eaves, S., Kumar, V., & Parry, G. (2018). Towards Digital Transformation: Lessons learned from Traditional Organisations. In *J.E.L. classification codes D83* (Vol. 86). https://doi.org/https://doi.org/10.1002/jsc.2185

Mulyana, R., Rusu, L., & Perjons, E. (2021a). *Association for Information Systems Association for Information Systems IT Governance Mechanisms In7uence on Digital Transformation: IT Governance Mechanisms In7uence on Digital Transformation: A Systematic Literature Review A Systematic Literature Review*. https://aisel.aisnet.org/amcis2021

Mulyana, R., Rusu, L., & Perjons, E. (2021b). IT Governance Mechanisms Infuence on Digital Transformation: A Systematic Literature Review. *Twenty-Seventh Americas Conference on Information Systems*, 1–10. https://aisel.aisnet.org/amcis2021

Mulyana, R., Rusu, L., & Perjons, E. (2023). How Hybrid IT Governance Mechanisms Influence Digital Transformation and Organizational Performance in the Banking and Insurance Industry of Indonesia. *Information Systems Development, Organizational Aspects and Societal Trends (ISD2023 Proceedings)*, 1–12.

Mulyana, R., Rusu, L., & Perjons, E. (2024a). *Association for Information Systems Association for Information Systems Key Ambidextrous IT Governance Mechanisms In>uence on Key Ambidextrous IT Governance Mechanisms In>uence on Digital Transformation and Organizational Performance in Digital Transformation and Organizational Performance in Indonesian Banking and Insurance Indonesian Banking and Insurance*. https://aisel.aisnet.org/pacis2024

Mulyana, R., Rusu, L., & Perjons, E. (2024b). Key ambidextrous IT governance mechanisms for successful digital transformation: A case study of Bank Rakyat Indonesia (BRI). *Digital Business*, *4*(2), 1–19. https://doi.org/10.1016/j.digbus.2024.100083

Muthaiyah, S., & Zaw, T. O. K. (2018). *ISO/IEC 27001 Implementation in SMEs: Investigation on Management of Information Assets*. https://doi.org/10.5958/0976-5506.2018.02112.5

Panggabean, A. (2021). *Memahami dan Mengelola Transformasi Digital*. Trakia University. https://doi.org/https://doi.org/10.31219/osf.io/s36wq

Panjaitan, B., Abdurrahman, L., & Mulyana, R. (2021). The Development of Information Security Management System Implementation Based on ISO 27001: 2013 Using Annex Control : in PT. XYZ Case Study Data Center. *E-Proceeding of Engineering*, *8*(2), 2813–2825.

Patricia, I., Ph, D., & Ness, L. R. (2015). *Are We There Yet? Data Saturation in Qualitative Research*. Walden Faculty and Staff Publications. https://scholarworks.waldenu.edu/facpubs/455

POJK. (2016). Standar Penyelenggaraan Teknologi Informasi bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah. *Nomor 75/POJK.03/2016*.

POJK. (2024). *Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah*.

Prayudi, R. A., Mulyana, R., & Fauzi, R. (2023). SEIKO : Journal of Management & Business Pengendalian Digitalisasi FintechCo Melalui Perancangan Pengelolaan Keamanan Informasi Berbasis COBIT 2019 Information Security Focus Area. *SEIKO : Journal of Management & Business*, *6*(2), 388–406.

Rahmadana, A., Mulyana, R., & Santoso, A. F. (n.d.). *Pemanfaatan COBIT 2019 Information Security Dalam Merancang Manajemen Keamanan Informasi Pada Transformasi BankCo*.

Ramadhani, A. (2018). Keamanan Informasi. *Journal of Information and Library Studies*, *1*(1), 39–51. https://doi.org/10.30999/n-jils.v1i1.249

Riznawati, N., Mulyana, R., & Santoso, A. F. (2023). SEIKO : Journal of Management & Business Pendayagunaan COBIT 2019 DevOps dalam Merancang Manajemen Pengembangan TI Agile pada Transformasi Digital BankCo. *SEIKO : Journal of Management & Business*, *6*(2), 2023–2223.

Shabri, H., Azlina, N., Said, M., Syariah, P., Ekonomi, F., Bisnis, D., Syarif, U., & Jakarta, H. (2020). Transformasi Digital Industri Perbankan Syariah Indonesia. *Journal of Islamic Economics*, *3*(2), 228–234. https://doi.org/https://doi.org/10.58958/elkahfi.v3i02.88

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, *22*(2), 63–75. https://doi.org/10.3233/EFI-2004-22201

Srijani, N. (2020). Peran UMKM (Usaha Mikro Kecil Menengah) Dalam Meningkatkan Kesejahteraan Masyarakat. *Jurnal Ilmiah Ekonomi Dan Pembelajarannya*, *8*(2), 191–201.

Suci, Y. R. (2017). Perkembangan UMKM (Usaha Mikro Kecil dan Menengah) di Indonesia. *Jurnal Ilmiah Cano Ekonomos*, *6*(1), 51–58.

Tarbiyatuzzahrah, Bq. D., Mulyana, R., & Santoso, A. F. (2023). Penggunaan COBIT 2019 GMO dalam Menyusun Pengelolaan Layanan TI Prioritas pada Transformasi Digital BankCo. *JTIM : Jurnal Teknologi Informasi Dan Multimedia*, *5*(3), 218–238. https://doi.org/10.35746/jtim.v5i3.400

Triandi, B. (2019). Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0. In *JURIKOM)* (Vol. 6, Issue 5). http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom|Page477

Viamianni, A., Mulyana, R., & Dewi, F. (2023). COBIT 2019 INFORMATION SECURITY FOCUS AREA IMPLEMENTATION FOR REINSURCO DIGITAL TRANSFORMATION. *JIKO (Jurnal Informatika Dan Komputer)*, *6*(2). https://doi.org/10.33387/jiko.v6i2.6366

Zaoui, F., & Souissi, N. (2020). Roadmap for digital transformation: A literature review. *Procedia Computer Science*, *175*, 621–628. https://doi.org/10.1016/j.procs.2020.07.090