KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 5, No. 4, Oktober (2024), pp. 1824-1835

Utilization of ISO 27001:2022 In Designing Information Security for Digital Transformation at BPRCO SME

Dafa Dinda Bayu Rama Dika[1], Rahmat Mulyana[2], Muharman Lubis[3]
[1]Information Systems, Faculty of Industrial Engineering, Telkom University, Indonesia
[2]Department of Computer and System Sciences, Stockholm University, Sweden
[3]Information Systems, Faculty of Industrial Engineering, Telkom University, Indonesia
E-mail: dbayuu@student.telkomuniversity.ac.id[1], rahmat@dsv.su.se[2], muharmanlubis@telkomuniversity.ac.id[3]

Abstract

Digital transformation has become a priority for SMEs (Micro, Small and Medium Enterprises), including BPRBCo (Bank Perekonomian Rakyat), to remain competitive amidst rapid technological developments. Information security is a critical aspect in this process, which requires a systematic and standardized approach. Previous research emphasizes the importance of ambidextrous (hybrid traditional and agile) information security management for large-scale banks as one of the seven key mechanisms for successful digital transformation, namely data management and information security. However, this approach has not proven effective for small-scale banks such as BPRs. This research aims to design an information security management system (ISMS) based on ISO 27001:2022, with a focus on the readiness of BPRBCo SME in facing digital transformation. This research adopts the five stages of Design Science Research (DSR), namely problem identification, requirement specification, design and development, demonstration, and evaluation. Data was collected through semi-structured interviews and document analysis, then analyzed using the ISO 27001:2022 SMKI framework. After risk analysis and mapping against previous study references, PDCA and Annex controls were found to be prioritized for BPRBCo. The results of this study developed an IMS framework specifically designed to meet the needs of SMEs, with a focus on the SME Focus Area. The DSR method enables the creation of practical solutions, based on an iterative cycle that combines theory and practice to produce optimal results. The resulting ISMS framework is then evaluated to assess the extent to which this design affects BPRBCo's readiness to obtain ISO 27001:2022 certification, as well as its impact on improving information security during the digital transformation process. This research also provides implementation recommendations by integrating three main aspects: people, process, and technology.

Keywords: *BPR, Digital Transformation, Information Security Management System, SMEs, ISO 27001:2022, Design Science Research*

1. Introduction

The rapid development of technology has affected various aspects of life, including how individuals, organizations and governments convey information accurately, effectively and efficiently [1]. In the context of significant technological advancements, digital transformation (DT) has become a major force driving significant changes in various industry sectors [2]. DT is ”A fundamental change that can occur in the application and utilization of digital technology into the resources of an organization with the main objective of improving the performance of an organization and can increase improvements for the organization” [3]. DT involves more than just the application of technology; it includes fundamental

ISSN: 2720-992X

changes in processes, structures, strategies and business models aimed at improving the customer experience [4]. The previous research identified 28 information technology governance mechanisms that influence DT, consisting of 6 structures, 17 processes, and 5 relational mechanisms, with information security and data management as important components within them [5]. The Information Technology (IT) function in business is also required to be able to improve the effectiveness, efficiency, and security of customer data in every service provided [6]. Currently, many companies in various industries, including the banking industry, are driven to implement IT in their digital transformation efforts to maintain data integrity [7]. In other literature, it is stated that digital transformation also has the potential to affect organizational performance [8]. Additionally, previous studies have underscored the critical role of IT services [9], IT risk management [10], information security [11], and DevOps practices [12] in facilitating digital transformation within major banks, incorporating key aspects from the COBIT 2019 framework. Additionally, similar research has been conducted in other sectors of the financial industry, focusing on information security governance in insurance firms [13], [14] and fintech companies [15]. The influence also hypothetically relevant for SMEs in the financial industry, such as rural banks (BPRs). While IT offers great potential in supporting TD, there are also significant risks, especially related to information security [16]. Information security has a very significant role in the running of a company's services, because it involves many aspects such as privacy, integrity, and customer confidentiality [17]. Cyberattacks are now considered one of the most dangerous threats to the world, so companies need to take strategic steps to avoid the impact of possible risks [18]. In a company, the success of digital transformation is not only seen from the application of the latest technology, but also depends on the company's ability to prevent and overcome cyber threats that are increasingly sophisticated and diverse. Findings in previous research indicate that four ambidextrous ISMS mechanisms (board and executives, strategy and architecture, data and information, and internal and external collaboration) greatly affect organizational performance, which is mediated by digital transformation [19]. The potential for strategic implementation of ambidextrous information security management systems (ISMS) in the banking sector, by balancing the exploration and exploitation of digital initiatives, can improve organizational performance and competitiveness in the evolving digital era [20].

ISMS is “A process that is structured based on a business risk approach to plan, implement, review and monitor, and maintain corporate information security“ [21]. ISMS is not enough if it is only done from a technical perspective, but also requires risk analysis and management to get an overview of the various risks that may arise in the organization [22]. SMEs have the potential to be able to adopt information system security in the course of their business.The increased adoption of digital technologies by enterprises has led to a rise in cyberattacks across sectors. one of them, SMEs, which tend to be more vulnerable than large companies due to limited access to digital technology resources and skills[23], [24]. In addition, as business models shift to the online space, many companies and organizations continue to neglect cybersecurity and are continuously viewed as targets, especially SMEs [25]. In OJK Regulation No. 7 of 2024 concerning Rural Banks (BPR), it is stated that BPR or Syariah Rural Banks (BPRS) are established based on changes in the business license of Microfinance Institutions (MFIs) to BPR or BPRS [26].

The ISO/IEC 27000 series is a standard for information security management systems (ISMS) that will help an organization stay up to date and adapt to all changes in the information security environment [27]. This research will focus on the use of ISO/IEC 27001. ISO /IEC 27001 is an international standard prepared for

the implementation, development, monitoring, operation and maintenance of information security management systems that can be used by organizations at large and can certainly protect information assets from various risks [28]. This research discusses the design of an information security management system based on the ISO 27001: 2022 clause prioritized for the digital transformation of SMEs and aims to answer the research questions as follows; "*How is the preparation of recommendations for information security management system solutions based on the results of the assessment gap analysis on the scope of the ISO 27001: 2022 clause prioritized for the digital transformation of SMEs?". How is the design of an information security management system based on the priority ISO 27001: 2022 clauses for the digital transformation of SMEs?*" This research produces a draft recommendation for an information security management system solution that complies with the ISO 27001: 2022 standard for BPRs by considering aspects of applicable financial regulations.

2. Research Methodology

In this research, researchers adopted the Design Science Research (DSR) framework. DSR provides a systematic guide for understanding, conducting, and evaluating research in the context of information system design. With this approach, researchers can effectively define research performance and create innovative solutions that are relevant and practical [29]. Figure 1. Design Science Research adopted from Hevner [29] is a conceptual model in this research.

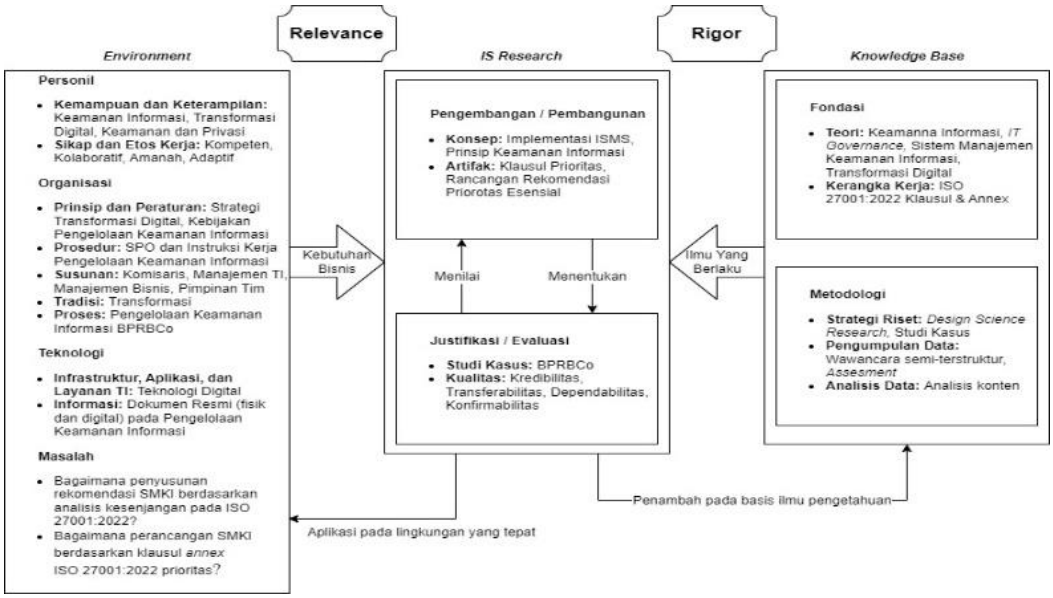

Figure 1. Design Science Research adopted from Hevner [29]

Figure 1. *Design Science Research adopted from Hevner [29]* represents the conceptual model of the framework based on Hevner's concept, which consists of three main elements: environment, Information System (IS), and knowledge base [29]. This model is designed to assist researchers in defining problems, identifying relevant factors, and forming clear relationships to facilitate mapping the core of the problem.

2.1. Research Process

This research applies a systematic process to see and analyze which strategies work best to address the need for a robust information security management system

(ISMS) that is aligned with ISO 27001:2022 and supports the digital transformation of SMEs. The research process consists of a number of several structured steps that are used to find problems, create solutions, and evaluate results to achieve objectives. The following **Figure 2.** Research Processshows the research process.

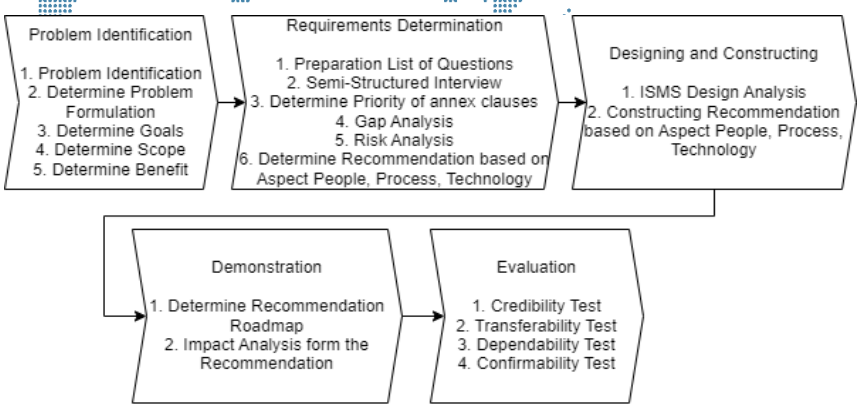

Figure 2. Research Process

This research divides the research design process into 5 stages.

a) Problem Explanation
At to this point, it starts by identifying problems by reading previous research or others regarding the application of ISO 27001: 2022 in organizations, ISO 27001: 2022 as best practice, comparison of international standards COBIT 2019 Information Security Focus Area and NIST SP 800-53, national information security management regulations, and internal BPRBCo company documents. After that, a problem formulation is formed from the researcher, setting objectives, and research limitations. After all stages are completed, verification will be made to the supervisor regarding the activities that will be carried out during this research.

b) Determination of Need
Determine the priority of clauses and annexes based on digital transformation for assessment with organizational conditions then, make a list of questions based on the prioritization of clauses and annex of ISO 27001: 2022 for research needs which will later be used for interview needs to source. After that, a risk analysis assessment is carried out from the results of the selected clauses and annex based on the results of the previous interview and selected to be used as recommendations. The last process is to determine recommendations for selected clauses and annexes according to the types of people, process, and technology aspects.

c) Design and Manufacture
At this stage, the design of the information security management system is carried out in accordance with the clauses and annex selected from the previous assessment results. Improvement recommendations based on three aspects of people, process, and technology

d) Demonstration
The design of the estimated time of implementation of recommendations in accordance with the selected annex clauses and analyzed its effect on certification preparation.

e) Evaluation
There are four stages of testing performed to evaluate how well the offered solution solves the problem. First, testing ensures that the data is valid. Next, the research findings determine how effectively the solution can be implemented and used by the organization. Finally, the findings are used as a basis for the organization to implement a data security management system.

2.2. Data Collection and Processing

The data collection process carried out at the BPRBCo object is one of the stages of research that aims to obtain the information needed to achieve the objectives of the research. The data collection process is carried out in two ways, namely by using related documents and conducting interviews offline and online. In a roadmap that has been prepared by researchers in collecting data at BPRBCo.

Table 1. Primary Data

Date & Duration	Interviewee	Topic
March 21, 2024 (10.00 – 15.00)	head of IT and head of regional office	Introduction to the organization starting from the organizational structure, conditions, information security of the organization, and explaining the purpose and objectives of the research.
March 22, 2024 (10.00 – 15.00)	head of IT and head of regional office	Understand the detailed business processes of the organization as well as retrieve data through documents.
April 3, 2024 (09.00 – 14.00)	head of IT	collecting data through documents and interviews related to the assessment of the annex clause.
June 27, 2024 (09.00 – 12.00)	head of IT	collecting data through documents and interviews related to the assessment of the annex clause.
July 07, 2024 (09.00 – 14.00)	head of IT	interview on risk analysis for the company and draft recommendations.

Secondary data is data collected and published by the subject. This data is obtained directly from research subjects such as Company databases, related documents, and related literature. Researchers use secondary data to assist in the assessment process. The secondary data used in this study consists of the data in

Table 2. Secondary *Data*. Interviews were carried out until no further significant insights emerged, indicating data saturation. This was ensured by performing several iterations of interviews to comprehensively explore the subject matter [30].

Table 2. Secondary Data

Data Type	Data
Secondary Data	Audit Report
	Annual report
	Strategy Plan Document
	Policy Documents and SOP
	Organizational Structure
	Technical Guidance Document

The researcher also used a thematic analysis approach in this study. Thematic analysis provides a more structured framework, which is appropriate for data analysis in case study and design science research [31]. In addition, since it is based on a case study, the case study method is an appropriate choice to use in the research because it uses the main research question of how or why it happened, requires little time to control the events under study, and the research focus is a contemporary phenomenon [32].

3. Result and Discussion

In this section, researchers assessed the prioritization of annex clauses, followed by making risk analysis, designing recommendations, creating a roadmap from the results of

recommendations, the effect of recommendations on ISMS, to the results of trustworthiness evaluation.

3.1. Annex Clause Priority

To analyze the condition of the company using ISO 27001: 2022 clauses and controls, the researchers prioritized the clauses and annex controls using 3 aspects, namely POJK Regulation SEOJK No. 75 [33], and POJK No. 7[26], ISMS Research for SMEs [17], [34], and Previous Research [5], [7]. After analyzing the three aspects, the weight of the three aspects was accumulated. The researcher takes a weight of 100 with clauses that qualify from all three aspects.

3.2. Conformity Assessment with Priority Clauses and Annexes

After prioritizing, then assessed the existing conditions of the clauses and annexes that have been selected, the assessment is carried out from document data that has been obtained previously and the results of interviews from BPRBCo interviewees.

Table 3. Current Grade Level

Value		Description
N/A		This condition is used when a particular annex clause or control is not relevant to the organization's environment or operations.
1	Fully	The organization has fulfilled the requirements of the Clauses and Annexes and has been properly implemented according to ISO 27001:2022 guidelines.
0	None	The organization has not fulfilled the requirements of the Clauses and Annexes and has not been properly implemented according to ISO 27001:2022 guidelines.

The following is the Existing condition of the company based on the main clauses of ISO 27001: 2022 which have been prioritized:

a) *Assessment (1)*. 4.1 understanding the organization and it's context, 4.2 understanding the needs and expectations of interested parties, 6.1 actions to address risks and opportunities, 7.5 documented information, 8.1 operational planning and control, 5.2 information security roles and responsibilities, 5.9 inventory of information and other associated assets, 5.12 classification of information, 5.19 information security in supplier relationships, 5.20 addressing information security within supplier agreements, 5.30 ICT readiness for business continuity, 5.31 legal, statutory, regulatory and contractual requirements, 6.2 terms and conditions of employment, 6.6 confidentiality or non-disclosure agreements, 7.5 protecting against physical and environmental threats, 7.11 supporting utilities, 8.14 Redundancy of information processing facilities, 8.21 security of network services, 8.34 protection of information systems during audit testing

b) *Assessment (0)*. 6.3 planning of changes, 7.1 resources, 7.2 competence, 9.1 monitoring, measurement, analysis and evaluation, 5.22 monitoring, review and change management of supplier services, 8.6 capacity management, 8.16 monitoring activities, 8.32 change management.

3.3. Risk Analysis

After assessing the current condition of the organization based on ISO 27001: 2022, prioritization will be carried out again using probability and impact analysis. This prioritization is carried out to determine the clauses and annex controls that will later be given recommendations. In Table ***4.*** *Probability Criteria*below are the criteria for the probability of risks that will occur in the company.

Table 4. Probability Criteria [35]

Criteria	Description	Value	Frequency of incidence
Certain	Risks are certain to happen	5	< 7 months
Likely	High probability of risk	4	7 - 12 months
Possible	Risks occur sometimes	3	1 – 3 years
Unlikely	Risks are rare	2	3 – 5 years
Rare	Risk is very rare	1	> 5 years

Table ***4.*** *Probability Criteria* explains the criteria of the existing probability, for the frequency criteria are divided into 5, namely, certain, likely, possible, unlikely, rare [35]. Furthermore, in Table 5. Impact Criteria [35] explains the description and criteria of impact.

Table 5. Impact Criteria [35]

Criteria	Description	Value
Critical	Risks that occur are very disruptive to organizational activities and cause the entire business operation to stop.	5
High	The risks that occur begin to disrupt organizational activities and interfere with application operations, leading to obstacles.	4
Medium	The risks that occur begin to disrupt some organizational activities and hinder the smooth operation of the application.	3
Low	Risks that occur slightly disrupt organizational activities and slightly hinder application operations.	2
Very low	Risks that occur do not impact organizational activities and application operations.	1

In Table 5. Impact Criteria [35] explains the criteria for existing impacts, there are 5 impact criteria, namely critical, high, medium, low, very low. In **Error! Reference source not found.**the following is a risk matrix of probability and impact.

Table 6. Risk Matrix

Probability values	Risk impact				
	Very low (1)	Low (2)	Medium (3)	High (4)	Critical (5)
Rare (1)	Low	Low	Low	Low	Medium
Unlikely (2)	Low	Low	Medium	Medium	High
Possible (3)	Low	Medium	Medium	High	High
Likely (4)	Low	Medium	High	High	Extreme
Certain (5)	Medium	High	High	Extreme	Extreme

The lowest score from the calculation of probability and impact is 1 and the spread score is 25. The score from the assessment is calculated by the formula.
Score = probability x impact [35] (1)

Table 6. Risk Matrix calculations obtained values 1 to 4 get low risk values, values 5 to 9 get medium risk values, values 10 to 16 get high risk values, and values 17 to 25 get extreme risk values. In
Table 7. Risk Analysis *Results* using probability and impact indicators based on the results of unmet clauses and controls.

Table 7. Risk Analysis Results

Clause/Annex	Impact level	Probability level	Risk score
6.3 Planning of changes	Medium (3)	Unlikely (2)	Medium (6)
7.1 Resources	High (4)	Likely (4)	High (16)

Clause/Annex	Impact level	Probability level	Risk score
7.2 Competence	High (4)	Likely (4)	High (16)
9.1 Monitoring, measurement, analysis and evaluation	High (4)	Unlikely (2)	Medium (8)
5.22 Monitoring, review and change management of supplier services	High (4)	Likely (4)	High (16)
8.6 Capacity management	High (4)	Unlikely (2)	Medium (8)
8.16 Monitoring activities	Critical (5)	Likely (4)	Extreme (20)
8.32 Change management	Medium (3)	Possible (3)	Medium (9)

The research took high and extreme risk levels to provide recommendations based on 3 aspects (people, process, technology).

3.4. Design of Information Security Management System (ISMS)

Designing an ISMS that aims to improve organizational readiness in the face of digital this design, relevant controls are used as a reference for achieving the ISMS. This design involves three main aspects: people, process, and technology.

Table 8. Recommendation Aspects

Clause/Annex	Aspect
7.1 Resources	People & Process
7.2 Competence	People & process
5.22 Monitoring, review and change management of supplier services	People & Technology
8.16 Monitoring activities	People & Technology

a. *People Aspect Design*. The people aspect provides six recommendations, including one recommendation for roles by adding new roles so that the handling of information system security becomes more specific, two responsibilities to add more specific responsibilities to each role, and three recommendations for skills and awareness to increase competencies owned while increasing awareness of ISMS.
b. *Process Aspect Design*. Produces one recommendation on the process aspect, namely a policy recommendation that can simultaneously handle the recommendations in 2 clauses, making policies so that there are guidelines in the IT team recruitment system.
c. *Technology Aspect Design*. Produce two recommendations, namely one recommendation for tools to be able to assist in the evaluation system in supplier management, and one recommendation for features to be able to assist in the monitoring process to be more effective and efficient.

3.5. Roadmap Recommendations Implementation Design

Roadmap in this context refers to the planned schedule and implementation strategy of the proposed recommendations.

Table 9. Recommendation Roadmap

Activity	Time Period (2024)											
	Q1			Q2			Q3			Q4		
	1	2	3	4	5	6	7	8	9	10	11	12
7.1 Resources	P											
7.2 Competence	P	P										
5.22 Monitoring, review and change management of supplier services		P	P	P	P	P						
8.16 Monitoring activities		P				P	P	P	P			

The design of the schedule started in January and ended in September. The roadmap was created as a guide to direct the steps that need to be taken to effectively implement the recommendations.

3.6. Trustworthiness Evaluation Results

In the final stage, researchers carried out four stages of quality testing to evaluate how effective the solution was in solving the problem [36] The evaluation of this research was carried out in four stages.

a) *Credibility*. The credibility of this research is guaranteed through several important steps taken during the research process related to the implementation of ISO 27001:2022. First, data collection to the object. Second, the validation process. Third, validation by an ISO 27001:2022 expert and supervisor, who provides verification of the suitability and validity of the methods and results obtained.
b) *Transferability*. The transferability of this study was tested by presenting a detailed description of the context of BPRBCo. Data came from document analysis and employee interviews with ISO 27001:2022 guidelines. Risk registers were created to assess the risk of each clause and control. For a structured implementation, a four-quarter recommendation schedule was designed that provides step-by-step guidance for the company.
c) *Dependability*. The research data was collected from employee interviews and analysis of company documents, providing a comprehensive understanding. After analysis, the research was validated by ISO 27001:2022 organizations and experts, in addition to being tested by examiners who provided critical analysis and different perspectives.
d) *Confirmability*. The process began with data collection from credible sources, such as employee interviews and analysis of internal BPRBCo documents, followed by validation by the organization. The research was also validated by ISO 27001:2022 experts and supervisors, who provided valuable assessments and suggestions, as well as examiners who offered additional analysis and perspectives.

3.7. Discussion

Information security for BPR is very important, especially when digital transformation (DT) is taking place. This research contributes to the existing body of work on the banking and insurance industry in Indonesia [7], [20]. Previous studies have shown how traditional and adaptive IT governance mechanisms impact organizational performance and digital transformation in these industries [7]. In addition, a case study on a large Indonesian bank, BRI, found seven ambidextrous ITG mechanisms that are critical for successful digital transformation [20]. An additional study emphasized that information security is critical to successful digital transformation. This study emphasizes that effectively managing digital (exploration) and IT (exploitation) strategies is critical to improving performance in digital transformation projects [19].

This study confirms that effective implementation of information security, especially with the ISO 27001 standard, is critical to the success of digital transformation in SMEs such as BPRs. This is consistent with interview participant 1's statement, “Information security in BPRs is important, especially because it is required by regulation,” [37], which emphasizes the regulatory obligations in its implementation.

BPRBCo faces challenges in implementing hybrid information security due to limited human and financial resources. However, with the right approach, which combines agile methodologies for rapid response and traditional approaches for operational stability, BPRBCo can improve its information security efficiency and resilience. This research shows that a flexible approach based on ISO 27001 can be adapted in organizations with limited resources, making flexibility in information security key to successful digital transformation and improving BPRBCo's competitiveness in the digital era.

4. Conclusion

Based on ISO 27001: 2022 at BPRBCo, the researcher obtained several clauses and annexes selected as information security planning at BPRBCo for digital transformation. Five main clauses were selected in ISO 27001: 2022 which have been prioritized with 3 aspects, after prioritization and risk analysis using probability and impact indicators, resulting in 4 main controls in ISO 27001: 2022. There are People controls and Physical controls that have met the requirements based on ISO 27001:2022, while in Organizational controls and Technology controls there are still some sub-controls that have not met the requirements of ISO 27001:2022. There are clause 4 Context of the Organization and clause 8 Operation that have met the requirements based on ISO 27001: 2022, while clause 6 Planning, clause 7 Support, clause 9 Performance evaluation that have not met the requirements of ISO 27001: 2022. Selected 4 main controls in ISO 27001: 2022 that have been prioritized with 3 aspects. There are People controls and Physical controls that have met the requirements based on ISO 27001: 2022, while in Organizational controls and Technological controls there are still several sub-controls that have not met the ISO 27001: 2022 requirements. There are 4 sub-clauses and 4 sub-controls that are still unqualified, with 1 sub-clause each from Planning, 2 sub-clauses from Support, 1 sub-clause from Performance evaluation, 1 sub-control from Organizational controls, and 3 sub-controls from Technological controls.

After completing the prioritization and producing 4 annex clauses, recommendations will then be made based on 3 aspects. Utilizes 3 aspects of recommendations, namely people, process, and technology. There are types of recommendations in terms of Roles, Responsibility, and Skill and awareness for the people aspect. There are types of policy recommendations for the process aspect. There are types of recommendations for tools and features for the technology aspect. This research only discusses recommendations for designing an ISMS, not an evaluation of its implementation and results. It also increases the knowledge of information security management for DT in small banks and provides practical implications for the management of such organizations.

References

[1] M. F. Safitra, M. Lubis, And A. Widjajarto, “Security Vulnerability Analysis Using Penetration Testing Execution Standard (Ptes): Case Study Of Government’s Website,” In *Acm International Conference Proceeding Series*, 2023. Doi: 10.1145/3592307.3592329.

[2] K. S. R. Warner And M. Wäger, “Building Dynamic Capabilities For Digital Transformation: An Ongoing Process Of Strategic Renewal,” *Long Range Plann*, Vol. 52, No. 3, 2019, Doi: 10.1016/J.Lrp.2018.12.001.

[3] C. Gong And V. Ribiere, “Developing A Unified Definition Of Digital Transformation,” *Technovation*, Vol. 102, 2021, Doi: 10.1016/J.Technovation.2020.102217.

[4] V. Gurbaxani And D. Dunkle, “Gearing Up For Successful Digital Transformation,” *Mis Quarterly Executive*, Vol. 18, No. 3, 2019, Doi: 10.17705/2msqe.00017.

[5] R. Mulyana, L. Rusu, And E. Perjons, “It Governance Mechanisms Influence On Digital Transformation: A Systematic Literature Review,” In *27th Annual Americas Conference On Information Systems, Amcis 2021*, 2021.

[6] N. L. Rinanty, Y. A. Prasetyo, And R. Mulyana, “Analisis Dan Perancangan Tata Kelola Teknologi Informasi Pada Lembaga Keuangan Mikro Menggunakan Framework Cobit 5 Domain Build Acquire And Implement (Bai),” *E-Proceeding Of Engineering*, Vol. 4, No. 2, 2017.

[7] R. Mulyana, L. Rusu, And E. Perjons, “It Governance Mechanisms That Influence Digital Transformation: A Delphi Study In Indonesian Banking And Insurance

Industry," *Pacific Asia Conference On Information Systems (Pacis)*, No. Ai-Is-Asia, 2022.

[8] R. Mulyana, L. Rusu, And E. Perjons, "How Hybrid It Governance Mechanisms Influence Digital Transformation And Organizational Performance In The Banking And Insurance Industry Of Indonesia," In *International Conference On Information Systems Development (Isd)*, 2023.

[9] Bq. D. Tarbiyatuzzahrah, R. Mulyana, And A. F. Santoso, "Penggunaan Cobit 2019 Gmo Dalam Menyusun Pengelolaan Layanan Ti Prioritas Pada Transformasi Digital Bankco," *Jtim : Jurnal Teknologi Informasi Dan Multimedia*, Vol. 5, No. 3, 2023, Doi: 10.35746/Jtim.V5i3.400.

[10] Y. W. D. M. Dewi, R. Mulyana, And A. F. Santoso, "Penggunaan Cobit 2019 I&T Risk Management Untuk Pengelolaan Risiko Transformasi Digital Bankco," *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, Vol. 12, No. 3, 2023.

[11] A. Rahmadana, R. Mulyana, And A. F. Santoso, "Pemanfaatan Cobit 2019 Information Security Dalam Merancang Manajemen Keamanan Informasi Pada Transformasi Bankco," *Jutisi: Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi*, Vol. 12, No. 3, 2023.

[12] N. Riznawati, R. Mulyana, And A. F. Santoso, "Pendayagunaan Cobit 2019 Devops Dalam Merancang Manajemen Pengembangan Ti Agile Pada Transformasi Digital Bankco," *Seiko : Journal Of Management & Business*, Vol. 6, No. 2, 2023.

[13] M. A. Andyas, R. Mulyana, And W. A. Nurtrisha, "Manajemen Keamanan Informasi Untuk Transformasi Digital Insurco Berbasis Cobit 2019 Focus Area Information Security," *Zonasi: Jurnal Sistem Informasi*, Vol. 5, No. 3, 2023, Doi: 10.31849/Zn.V5i3.15275.

[14] 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, 2023, Doi: 10.33387/Jiko.V6i2.6366.

[15] R. A. Prayudi, R. Mulyana, And R. Fauzi, "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*, Vol. 6, No. 2, 2023.

[16] A. F. Utami, I. A. Ekaputra, And A. Japutra, "Adoption Of Fintech Products: A Systematic Literature Review," *Journal Of Creative Communications*, Vol. 16, No. 3, 2021, Doi: 10.1177/09732586211032092.

[17] M. Antunes, M. Maximiano, R. Gomes, And D. Pinto, "Information Security And Cybersecurity Management: A Case Study With Smes In Portugal," *Journal Of Cybersecurity And Privacy*, Vol. 1, No. 2, 2021, Doi: 10.3390/Jcp1020012.

[18] M. F. Safitra, M. Lubis, And M. T. Kurniawan, "Cyber Resilience: Research Opportunities," In *Acm International Conference Proceeding Series*, 2023. Doi: 10.1145/3592307.3592323.

[19] R. Mulyana, L. Rusu, And E. Perjons, "Key Ambidextrous It Governance Mechanisms Influence On Digital Transformation And Organizational Performance In Indonesian Banking And Insurance," 2024.

[20] R. Mulyana, L. Rusu, And E. Perjons, "The Key Ambidextrous It Governance Mechanisms For A Successful Digital Transformation: Case Study Of Bank Rakyat Indonesia (Bri)," *Digital Business*, P. 100083, 2024.

[21] B. Panjaitan, L. Abdurrahman, And R. Mulyana, "Pengembangan Implementasi Sistem Manajemen Keamanan Informasi Berbasis Iso 27001:2013 Menggunakan Kontrol Annex: Studi Kasus Data Center Pt. Xyz," *E-Proceeding Of Engineering*, Vol. 8, No. 2, 2021.

[22] T. S. Putri, N. Mutiah, And D. Prawira, "Analisis Manajemen Risiko Keamanan Informasi Menggunakan Nist Cybersecurity Framework Dan Iso/Iec 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," *Coding : Jurnal Komputer Dan Aplikasi*, Vol. 10, No. 2, Pp. 237–248, 2022.
[23] M. Bada And J. R. C. Nurse, "Developing Cybersecurity Education And Awareness Programmes For Small- And Medium-Sized Enterprises (Smes)," *Information And Computer Security*, Vol. 27, No. 3, 2019, Doi: 10.1108/Ics-07-2018-0080.
[24] R.-P. Classen, M. Garbutt, And J. Njenga, "Factors Influencing The Adoption Of Digital Technologies In South African Smmes," 2021.
[25] M. Varachia, S. Bvuma, And A. Pooe, "Adoption Of Cybersecurity Practices For Smmes," 2022.
[26] "Pojk 7 Tahun 2024 Bank Perekonomian Rakyat Dan Bank Perekonomian Rakyat Syariah".
[27] J. Damian Vasquez, "Iso/Iec 27000," *High Tech-Engineering Journal*, Vol. 3, No. 2, 2023, Doi: 10.46363/High-Tech.V3i2.3.
[28] A. Fathurohman And R. W. Witjaksono, "Analysis And Design Of Information Security Management System Based On Iso 27001: 2013 Using Annex Control (Case Study: District Of Government Of Bandung City)," *Bulletin Of Computer Science And Electrical Engineering*, Vol. 1, No. 1, 2020, Doi: 10.25008/Bcsee.V1i1.2.
[29] A. R. Hevner, S. T. March, J. Park, And S. Ram, "Design Science In Information Systems Research," *Mis Q*, Vol. 28, No. 1, 2004, Doi: 10.2307/25148625.
[30] P. Ness And L. Fusch, "Are We There Yet? Data Saturation In Qualitative Research," *Qualitative Report*, Vol. 20, No. 9, 2015.
[31] M. Denscombe, *The Good Research Guide For Small Scale Research Projects*, Vol. 6, No. 3. 2010.
[32] R. K. Yin, "Discovering The Future Of The Case Study Method In Evaluation Research," *American Journal Of Evaluation*, Vol. 15, No. 3, 1994, Doi: 10.1177/109821409401500309.
[33] Ojk, "Standar Penyelenggaraan Teknologi Informasi Bagi Bank Perkreditan Rakyat Dan Bank Pembiayaan Rakyat Syariah." Ojk.Go.Id. Accessed: Jun. 13, 2024. [Online]. Available: Https://Ojk.Go.Id/Id/Regulasi/Pages/Pojk-7-Tahun-2024-Bank-Perekonomian-Rakyat-Dan-Bank-Perekonomian-Rakyat-Syariah.Aspx
[34] N. Ramadhan And U. Rose, "Adapting Iso/Iec 27001 Information Security Management Standard To Smes," 2022.
[35] W. S. Basri And A. L. Ayu, "Risk Management In Information Systems: Applying Iso 31000: 2018 And Iso/Iec 27001: 2022 Controls At Pmi's Central Clinic," *International Journal For Applied Information Management*, Vol. 4, No. 1, Pp. 1–13, 2024.
[36] A. K. Shenton, "Strategies For Ensuring Trustworthiness In Qualitative Research Projects," *Education For Information*, Vol. 22, No. 2, 2004, Doi: 10.3233/Efi-2004-22201.
[37] Bprbco, "Interview Transcript Of Bprbco." Mar. 2024.