Jurnal Teknologi Dan Sistem Informasi Bisnis
Vol. 6 No. 4 Oktober 2024 Hal. 820-831
http://jurnal.unidha.ac.id/index.php/jteksis

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

Utilizing ISO 27001:2022 to Design Information Security for BPRACo SME Digital Transformation

Raihan Rakan[a], Rahmat Mulyana[b], Muharman Lubis[c]
[a] Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia, raihanrakan@student.telkomuniversity.ac.id
[b] Departement of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden, rahmat@dsv.su.se
[c] Faculty of Industrial Engineering, Telkom University, Bandung, Indonesia, muharmanlubis@telkomuniversity.ac.id

Submitted: 27-08-2024, Reviewed: 06-09-2024, Accepted 18-10-2024
https://doi.org/10.47233/jteksis.v6i4.1621

Abstract
In the digital age of the Industrial Revolution 4.0, organizations like BPRACo must undergo Digital Transformation (DT). A significant challenge is the lack of adequate information security controls, which can lead to DT failure. Smaller banks, such as BPR, face difficulties in adopting effective information security management strategies that are proven for larger institutions. This study aims to identify the application of ISO 27001:2022 standards and develop an information security management system focusing on the most critical annex clauses for SME digital transformation. It also seeks to evaluate and analyze the impact of an information security management system aligned with these key clauses on SME DT success. The research employs a five-stage Design Science Research (DSR). Data were collected through interviews and document analysis, then analyzed using the ISO 27001:2022 framework for Information Security Management Systems (ISMS). The study identified six priority Clause and Annex controls for BPRACo. Based on the gaps, six essential solutions were designed, compiled into an implementation roadmap to enhance BPRACo readiness for full ISMS implementation and certification, supporting DT success in small banks. This research provides valuable insights and practical implications for information security management in small banks.

Keywords: *Digital Transformation, Design Science Research, Information Security, ISO 27001:2022, BPRACo.*

INTRODUCTION

Digital Transformation (DT) has significantly affected various aspects of life, including business [1]. DT is "A fundamental change process, enabled by the innovative use of digital technologies accompanied by the strategic use of core resources and capabilities"[2]. DT aims to strengthen entities through the application of information technology, computing, communication, and connectivity, which drives significant changes in the nature and function of business [3], [4], [5]. DT is becoming an important issue in the banking sector [6], and previous research has shown that agile IT mechanisms have a significant impact on DT [7]. However, traditional IT is also needed to support the DT. A hybrid approach, which combines traditional and agile methods, has proven to be effective in achieving optimal organizational performance [8].

Moreover, previous research has highlighted the significance of IT services [9], IT risk management [10], information security [11], and DevOps practices [12] in supporting digital transformation (DT) in large banks, with a focus area from COBIT 2019 framework. Furthermore, in other financial industry types also existed prior studies with information security governance focus area, such as in insurance companies [13], [14], also in fintech company [15].

The most recent research in large banks and insurance context highlight that data management and information security are key mechanisms for successful DT toward organizational performance achievements [16]. In the context of SME such as BPRACo, the company is considered as an SME because through the latest BPR regulations, it focuses on SME services and according to experts, BPR is an SME when compared to a General Bank (large organization). SME are recognized as having the ability to create jobs, encourage entrepreneurship, and support local economic growth [17], the adoption of the right technology can increase efficiency and productivity, and maintain competitiveness in an increasingly competitive market [18], [19]. Therefore, regulations and policies must be prioritized before implementation, as these decisions directly influence the quality, effectiveness, and efficiency of the outcome [20].

However, DT adoption also brings significant challenges related to information security, such as the risk of data loss, unauthorized access, and infrastructure damage [21], [22]. To address these dangers, it is essential to carry out thorough investigations, pinpoint weaknesses, and reduce existing risks [23]. Therefore, it is important for an SME such as BPRACo to design Information Security Management System (ISMS) using the ISO 27001:2022 standard to manage those risks

[24]. ISMS is one that focuses on how to identify possible and current risks and how to address the impact of these risks [25]. This is in line with Financial Services Authority regulations that require BPRs and BPRSs to implement security measures to prevent security breaches that could harm them and their customers [26]. This research will explore how information security can be implemented in BPRACo using the ISO 27001:2022 framework, ISO 27001:2022 is a framework for information security that can help businesses develop and implement a good information security management system (ISMS). The ISO 27001:2022 standard provides guidelines for establishing, implementing, maintaining, and continually improving an information security management system for companies of all sizes and from all sectors of activity [27], which is flexible and adaptable to the needs of the organization, to improve performance.

Therefore, this study has formulated several research questions to develop an information security management system for digital transformation. The main research questions are: How can the implementation of the ISO 27001:2022 standard be identified and developed to establish an information security management system that focuses on specific annex clauses most relevant to the digital transformation of SME.

Furthermore, to what extent does the application of an information security management system aligned with the key clauses of ISO 27001:2022 impact the success of digital transformation in SME.

This study presents a novel approach by prioritizing key annex clauses of the ISO 27001:2022 standard for the digital transformation of small banks (BPR). Unlike previous research focused on larger institutions, it addresses the unique challenges small banks face in implementing robust information security management systems (ISMS), offering a tailored framework to enhance their readiness and maturity for digital transformation.

RESEARCH METHODOLOGY

2.1. Conceptual Model

A conceptual model is a pictorial representation of the concepts being discussed in the research.

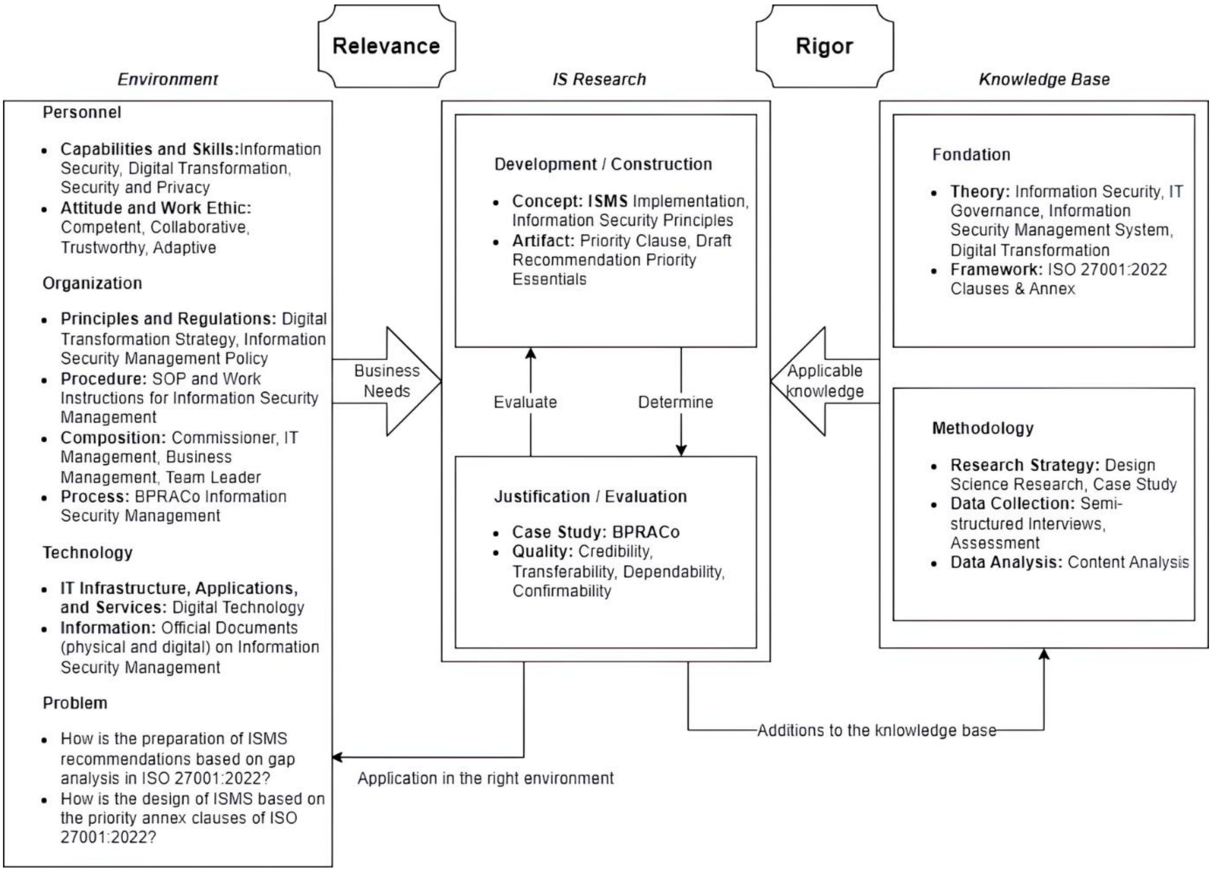
Relevance
Rigor
Environment
IS Research
Knowledge Base
Personnel
Capabilities and Skills:Information Security, Digital Transformation, Security and Privacy
Attitude and Work Ethic: Competent, Collaborative, Trustworthy, Adaptive
Organization
Principles and Regulations: Digital Transformation Strategy, Information Security Management Policy
Procedure: SOP and Work Instructions for Information Security Management
Composition: Commissioner, IT Management, Business Management, Team Leader
Process: BPRACo Information Security Management
Technology
IT Infrastructure, Applications, and Services: Digital Technology
Information: Official Documents (physical and digital) on Information Security Management
Problem
How is the preparation of ISMS recommendations based on gap analysis in ISO 27001:2022?
How is the design of ISMS based on the priority annex clauses of ISO 27001:2022?
Business Needs
Development / Construction
Concept: ISMS Implementation, Information Security Principles
Artifact: Priority Clause, Draft Recommendation Priority Essentials
Evaluate
Determine
Justification / Evaluation
Case Study: BPRACo
Quality: Credibility, Transferability, Dependability, Confirmability
Applicable knowledge
Fondation
Theory: Information Security, IT Governance, Information Security Management System, Digital Transformation
Framework: ISO 27001:2022 Clauses & Annex
Methodology
Research Strategy: Design Science Research, Case Study
Data Collection: Semi-structured Interviews, Assessment
Data Analysis: Content Analysis
Application in the right environment
Additions to the knlowledge base

Figure 1 Conceptual Model

The conceptual framework model consists of three main components: environment, information system (IS) research, and knowledge base [28].

a. Environment
Is the environment used as a means for research. Divided into four parts Personnel whose focus is on abilities and skills, Organization whose focus is on the environment that exists in the organization, Technology whose focus is on infrastructure and information, and problems that become the initial benchmark for research.
b. IS Research
Focus on the development research factor of the research and evaluation conducted in the study.
c. Knowledge Base
It is the knowledge base of the research, such as the foundation of the theories and concepts developed, the methodology for research strategy and analysis.

2.2. Research Process

To address the need for a robust information security management system (ISMS) that aligns with ISO 27001:2022 and supports the digital transformation of SME, this research employs a systematic process to explore and analyze the most effective strategies. A research process involves a series of structured steps designed to identify challenges, develop solutions, and evaluate outcomes to achieve the desired objectives. The research process is illustrated in Figure 2.

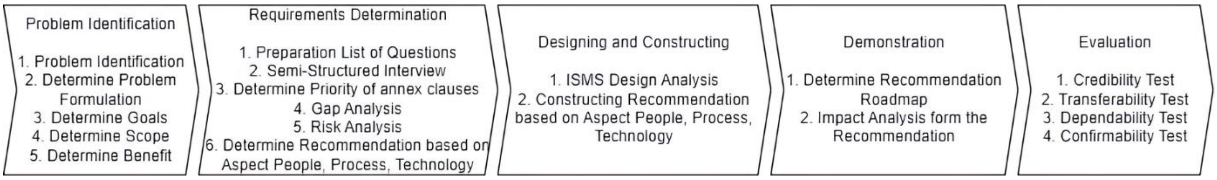
Problem Identification
1. Problem Identification
2. Determine Problem Formulation
3. Determine Goals
4. Determine Scope
5. Determine Benefit
Requirements Determination
1. Preparation List of Questions
2. Semi-Structured Interview
3. Determine Priority of annex clauses
4. Gap Analysis
5. Risk Analysis
6. Determine Recommendation based on Aspect People, Process, Technology
Designing and Constructing
1. ISMS Design Analysis
2. Constructing Recommendation based on Aspect People, Process, Technology
Demonstration
1. Determine Recommendation Roadmap
2. Impact Analysis form the Recommendation
Evaluation
1. Credibility Test
2. Transferability Test
3. Dependability Test
4. Confirmability Test

Figure 2 Research Process

Research Process is the stage of the research design process. In this research, the systematics is divided into 5 stages.

a. Problem Explanation
At this stage, it can be started by looking for problems by reading research on the application of ISO 27001: 2022 in organizations, ISO 27001: 2022 as best practice, international standard comparisons COBIT 2019 Information Security Focus Area and NIST SP 800-53, national information security management regulations, and internal BPRACo company documents. Furthermore, the problem to be discussed will be determined by the researcher, setting objectives, and research limitations. After the entire procedure is complete, verification will be made to the supervisor regarding the activities that will be carried out during this research.
b. Determination of Need
Formulate a list of questions based on the research needs. Next, conduct semi-structured interviews. Then, determine the priority of clauses and annexes based on digital transformation for assessment with organizational conditions. After that, a risk analysis assessment is carried out to determine the selected clauses and annexes for recommendations. The last process is to determine the clauses and annex recommendations following the type of people, process, and technology aspects.
c. Design and Manufacture
At this stage, the design of the information security management system is carried out according to the selected clauses and annexes. Improvement recommendations follow three aspects, namely people, process, and technology.
d. Demonstration
At this stage, after designing recommendations for information security management systems from the aspects of people, process, and technology. Furthermore, time estimation is carried out according to the selected annex clause and its effect on certification preparation is analyzed.
e. Evaluation
Four testing steps are carried out to assess how effective the solution is to solve the problem. Starting from testing to ensure the information data is valid, evaluating the research results to what extent they can be applied and used in the organization, and the research results are used as a basis for the organization to implement an information security management system.

2.3. Data Collection and Processing

In this research, the semi-structured interview method was used because in the interview the interviewer has a clear list of questions and still the interviewer is prepared to be flexible. The interviewee can develop further and open questions. Before conducting the interviews, we sent out a research request letter and received a response in the form of a research approval letter. The interviews were carried out both in-person over two days at the

BPRACo headquarters and virtually via the Microsoft Teams platform. These sessions were recorded for later transcription. Interviews continued until data saturation was reached, meaning no new significant information was emerging [29]. To achieve this, multiple rounds of interviews were conducted to ensure thorough coverage of the topic [29]. We conducted semi-structured interviews with three representatives from BPRACo. Table 1 presents the primary data collected.

Table 1 Primary Data

Date & Duration	Interviewee	Topic
March 14, 2024 (09.00 – 16.00)	Interviewee 1 (IT Manager), Interviewee 2 (IT Staff), Interviewee 3 (IT Staff)	Interview on organizational conditions, general information security, and data retrieval from documents
March 15, 2024 (09.00 – 16.00)	Interviewee 1 (IT Manager), Interviewee 2 (IT Staff), Interviewee 3 (IT Staff)	Interview on annex clauses, and data retrieval from documents
April 26, 2024 (10.00 – 11.00)	Interviewee 2 (IT Staff)	Interview on annex clauses
June 20, 2024 (10.00 – 11.00)	Interviewee 2 (IT Staff)	Interview on annex clauses, analysis methods, and draft recommendations

Regarding the interview findings, interviewee 1 stated, "BPRACo will continually require digital transformation to enhance its banking operational services. Digital transformation will lead to greater operational efficiency, improved customer service, and enable BPRACo to stay competitive in a constantly changing market [30]." This indicates that BPRACo needs to shift some traditional activities to digital formats to enhance customer efficiency.

Secondary data was gathered through a triangulation of internal and public documents to obtain more detailed information and a more comprehensive understanding of the data. Table 2 illustrates the secondary data utilized.

Table 2 Secondary Data

Data Type	Data
Secondary Data	Organizational Structure. Security Information. Annual Report. Strategy Plan. Hardware and software documents. IT Implementation SOP. BPRACo Official Website.

In this study, researchers also used a thematic analysis approach. Thematic analysis provides a more structured framework, suitable for data analysis in the context of case studies and design science research [31].

In addition, conducted based on a case study, the case study method is the right choice to use in research because it uses the main research question how or why, requires little time to control the events under study, and the research focus is a modern phenomenon to follow modern events [32].

RESEARCH RESULTS AND DISCUSSION

3.1. Annex Clause Priority

The priority of the annex clause is assessed based on 3 aspects, namely Regulation POJK SEOJK No. 75 [26] and POJK No. 7 [33] research on information security management systems for SME [34], [24], and previous research on digital transformation in the banking sector [6], [7]. Each aspect has equal weight, and the assessment is done by seeing whether the annex clause is discussed in the three aspects or not. If the annex clause is addressed in the aspect, it is given a plus and if it is not addressed in the aspect it is crossed.

3.2. Conformity Assessment to Priority Clauses and Annex

The Conformance Assessment is carried out to see the current condition of the ISMS at BPRACo in accordance with the priority clauses and annex of the digital transformation that has been carried out.

Table 3 Current Grade Level

Value		Description
N/A		This condition is used when the requirements of a particular clause or control are not relevant for the organization's environment or operations.
0	No	The organization has not implemented the clause or annex at all. This means that in their information security management system, the relevant clause or annex has not been implemented and no steps have been taken to meet those requirements.
0,5	Partially	The organization has not fully implemented the clause or control. Although some steps have been taken in adopting the relevant clause or annex, the

E-ISSN : **2655-8238**
P-ISSN : **2964-2132**

Value		**Description**
		implementation has not reached the overall level or consistency expected in this standard.
1	Fully	The organization has implemented the clause or control well. This indicates that the organization has adopted and implemented appropriate procedures or actions to meet the requirements and achieve an overall level of compliance with the clause or control.

A conformity assessment of the clauses and annexes based on the current state of the organization, with results:

a. Assessment (1)
- 4.1 The organization shall determine the external and internal issues relevant to its objectives
- 4.2 Understand the needs and expectations of interested parties
- Actions to address risks and opportunities
- 7.1 Resources
- 7.4 Communication
- 5.2 Information security roles and responsibilities
- 5.9 Inventory of information and other relevant assets
- 5.12 Classification of information
- 5.24 Information security incident management planning and preparation
- 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 confidentiality agreements
- 7.5 Protecting against physical and environmental threats
- 8.14 Redundancy of information processing facilities
- 8.21 Security of network services
- 8.34 Protection of information systems during audit testing

b. Assessment (0.5)
- 6.3 Change planning
- 7.2 Competence
- 7.5 Documented information
- 8.1 Operational planning and control
- 9.1 Monitoring, measurement, analysis and evaluation
- 5.19 Information security in supplier relationships
- 5.20 Addressing information security in supplier agreements
- 5.22 Monitoring, reviewing and change management of supplier services
- 7.11 Supporting utilities
- 8.32 Change management

c. Assessment (0)
- 8.6 Capacity management
- 8.16 Monitoring activities

3.3. Risk Analysis

Risk analysis is carried out to assess the high to low risks of each annex clause. In this research, risk analysis is assessed based on 3 components, namely:

a. Threat includes the time when a risk is likely to occur, and the actor.
b. Vulnerability or ease of exploitation.
c. Impact includes influences or consequences that can occur and affect the value of the organization.

In the analysis process, researchers determine the criteria for each aspect by considering the condition of the company, risk standards[35], and relevant previous research [36].

Table 4 Threat Vulnerability Criteria

Code	**Threat**	**Vulnerability**
High (3)	- Time of occurrence < 1 year - Performed by experienced or professional people (hackers)	Very easy to exploit, no special ability required
Medium (2)	- Time of occurrence within 1-3 years - Performed by medium-skilled people (competitors, fraudsters)	Exploitable with general technical ability
Low (1)	- Time of occurrence > 3 years - Performed by people who do not have technical skills (employee error)	Very difficult and requires special ability to exploit

Table 5 Impact Criteria

Code	**Impact**
Very High (4)	Influential in all corporate and operational activities
High (3)	Influential in core corporate and operational activities
Medium (2)	Influential in some enterprise and operational activities
Low (1)	Influential for related enterprise activities and operations
Very Low (0)	No influence on enterprise and operational activities

After mapping the priority clauses and annexes from the prioritization and determination of threat, vulnerability, and impact criteria with qualifications following ISO 27005 and organizational needs.

From the analysis results, the minimum score obtained is 0 and the maximum score is 8 [35].

Table 6 Risk Matrix

	Threat	**Low**			**Medium**			**High**		
	Vulnerability	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Impact	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

The analysis was conducted following the criteria of each aspect, the current condition of the organization and the goals of the organization. Clauses and annexes that are continued to this stage are those that have a value of (0) and (0.5) in the assessment process.

Table 7 Risk Analysis Results

Clause/ Annex	**Threat**	**Vulnerability**	**Impact**	**Score**
6.3 Planning of changes	High	Medium	2	5
7.2 Competence	Medium	High	3	6
7.5 Documented information	Medium	Medium	3	5
8.1 Operational planning and control	High	High	4	8
9.1 Monitoring, measurement, analysis and evaluation	High	High	3	7
5.19 Information security in supplier relationships	Medium	High	3	6
5.20 Addressing information security within supplier agreements	Medium	High	3	6
5.22 Monitoring, review and change management of supplier services	Medium	Medium	2	4
7.11 Supporting utilities	High	High	3	7
8.6 Capacity management	Medium	Medium	2	4
8.16 Monitoring activities	Medium	Medium	3	5
8.32 Change management	Medium	Medium	2	4

ISO 27005 assesses the division of the final score into three low, medium, and high with numerical divisions such as:

1. *Low* 0-2
2. *Medium* 3-5
3. *High* 6-8

3.4. Annex Clause Prioritization Result

Based on the results of clause & annex prioritization, assessment, and risk analysis, the following clauses & annexes were selected for digital transformation.

Table 8 Prioritization Result

Clause & Annex	**Priority**	**Assessment**	**Risk**
7.1 Competence	100	0,5	High
8.1 Operational planning and control	100	0,5	High
9.1 Monitoring, measurement, analysis and evaluation	100	0,5	High
5.19 Information security in supplier relationships	100	0,5	High
5.20 Addressing information security within supplier agreements	100	0,5	High
7.11 Supporting utilities	100	0,5	*High*

3.5. Design of Information Security Management System (ISMS)

In the context of BRPACo, the design of the information security management system aims to improve organizational readiness for digital transformation by planning, adjusting, and managing priority information security at BPRACo to comply with the information system security management system based on ISO 27001: 2022 and using the controls in ISO 27001: 2022 as a reference for achieving the information system security management system. This design involves aspects of people, process, and technology.

Table 9 Recommendation Aspects

Clause & Annex	Aspect
7.2 Competence	People
8.1 Operational planning and control	Process
9.1 Monitoring, measurement, analysis and evaluation	Process
5.19 Information security in supplier relationships	Process
5.20 Addressing information security within supplier agreements	Process
7.11 Supporting utilities	Process & Technology

a. People Aspect Design

The design of the people aspect produces two (2) recommendations which are divided into responsibility, and skills and awareness. In responsibility it is recommended to inform all personnel about information security responsibilities so that each personnel know their role in supporting information security. In skill & awareness, it is recommended to standardize knowledge about information security for old and new personnel such as understanding information security, expertise in information security risk management, cyber security and information technology expertise, and data management expertise. To set these standards, training, certification, and socialization can be carried out for old personnel who have joined and apply these standards in recruiting new personnel.

b. Process Aspect Design

The design of the process aspect resulted in seven (7) recommendations, namely the preparation of operational planning and control procedures; procedures for monitoring, measuring, analyzing, and evaluating information security; information security procedures in agreements with suppliers; procedures for regular monitoring and evaluation of supporting utilities; information security policies for relationships with external vendors; policies for determining and documenting information security requirements in agreements with suppliers; work instructions for operational planning and control; and work instructions for operational planning and control.

c. Design of Technology Aspect

Designing in the technology aspect results in one (1) recommendation, namely increasing supporting utilities for information security digital transformation.

3.6. Roadmap Recommendations Implementation Design

The recommended roadmap in Table 10 provides an overview of the steps to be taken and the amount of time required to complete each step. The recommended roadmap outlines the level of need, difficulty, and organizational capabilities.

Table 10 Recommendation Roadmap

Activity	Time Period									
	2024				2025					
	9	10	11	12	1	2	3	4	5	6
7.2 Competence	■	■								
8.1 Operational Planning and Control			■	■						
9.1 Monitoring, measurement, analysis and evaluation									■	■
5.19 Information security in supplier relationships					■	■				
5.20 Addressing information security within supplier agreements							■	■		
7.11 Supporting utilities									■	■

Recommended roadmap for the implementation of the clauses and annexes starting in September 2024 and expected to be completed by June 2025. In the roadmap recommendations:

a. September - October 2024, recommendation 7.11 Competence will be implemented. This recommendation is done early because personnel competence is a very important foundation for the implementation of all aspects of information security and training and competence development is relatively faster to implement compared to other technical procedures.

b. November - December 2024, recommendation 8.1 Operational Planning and Control will be carried out. To ensure that all information security processes go according to plan, operational planning and control is essential at the outset after having competent personnel in place. Having proper documentation in place at the outset helps in organizing and overseeing all information security activities to be implemented.

c. January - February 2025, recommendation 5.19 Information Security in Supplier Relationships will be implemented. After designing operational and subsequent controls, relationship management with suppliers and ensuring they comply with information security requirements is an important first step. The identification and initial assessment of supplier risks requires time and coordination.

d. March - April 2025, recommendation 5.20 Addressing Information Security within Supplier Agreements will be implemented. Once information security in supplier relationships is managed, the next step is to strengthen agreements with suppliers to ensure long-term compliance. This will take time and is required once the initial understanding and management of supplier relationships has been done.

e. May - June 2025 will be carried out recommendation 9.1 Monitoring, Measurement, Analysis and Evaluation is a follow-up step that must be carried out after the main process has been completed. This ensures that all previous steps are working properly and ensures that all recommendations are used correctly and as planned. Simultaneously, recommendation 7.11 Supporting Utilities is carried out because it is very important to ensure stability and reliability after all the main processes are well underway. Supporting utilities should be ensured after all the main operational processes have been stabilized.

3.7. Effect of Annex Clause Recommendations

The results of the information security management system recommendations, if implemented by BPRACo, will have effects such as:

a. 7.2 Competence
By implementing the recommendation to improve competence, BPRACo will ensure that personnel have the necessary skills and knowledge to carry out their responsibilities related to information security. This will ensure BPRACo meets control 7.2 in full, as all key personnel will have the appropriate competencies to effectively protect information in the context of digital transformation.

b. 8.1 Operational Planning and Control
Implementation of the recommendation will help BPR ensure that all information security-related processes are properly planned and controlled, including the handling of operational changes and risks. By doing so, BPRACo will meet control 8.1 in full, keeping critical processes aligned with information security objectives in the digital transformation process.

c. 9.1 Monitoring, Measurement, Analysis, and Evaluation
By implementing this recommendation, BPR will be able to conduct effective monitoring of its Information Security Management System (ISMS) performance and ensure the results are valid and reliable. This will fulfill control 9.1 in full, enabling BPRACo to proactively manage and improve information security performance.

d. A.5.19 Information Security in Supplier Relationships
By managing information security risks throughout the supply chain, BPR will ensure that relationships with suppliers do not pose additional risks to information security. This will help BPRACo meet control 5.19 in full by maintaining the integrity and security of information when interacting with third parties.

e. A.5.20 Addressing Information Security within Supplier Agreements
Implementation of this recommendation will ensure that all agreements with suppliers include clear and agreed requirements regarding information security. This will enable BPRACo to meet control 5.20 in full, protecting critical data and information in all external interactions with suppliers.

f. A.7.11 Supporting Utilities
By ensuring that all supporting facilities are properly managed and maintained, BPR will be able to prevent operational disruptions that could threaten information security. This will help BPRACo meet control 7.11 in full, maintaining operational continuity and information security throughout the digital transformation process.

Implementation of the recommendations of each annex clause above will bring BPRACo closer to full compliance with ISO 27001:2022, which is the global standard for information security. Each step taken to meet the ISO 27001:2022 controls will ease the certification process, as BPRACo will be able to demonstrate consistent and ongoing compliance with the requirements of this standard. By focusing on high-risk areas and ensuring that medium-risk areas remain stable, BPRACo is not only reducing risk, but also strengthening their information security structure, which is essential in digital transformation.

3.8. Trustworthiness Evaluation Results

In the final stage, researchers run four stages of quality testing to evaluate how effective the solution is in solving the problem [37].The evaluation of this research was conducted in four stages:

a. Credibility: To ensure credibility, the research used data triangulation from multiple sources such as interviews, surveys, and document analysis to verify the consistency of findings. Interim results were shared with participants for validation, and ISO 27001 experts, including the supervisor, provided feedback to ensure the depth and accuracy of the research.
b. Transferability: A detailed description of the research context was provided, such as the characteristics of the BPR organization, to enable readers to assess the applicability of the research results in other similar contexts. Discussions with supervisors and ISO 27001 experts helped explore the adaptability of the research results to various organizations.
c. Dependability: Dependability was ensured by documenting the entire research process in detail, enabling review by others. Consistency of methodology and research results was ensured through data triangulation and reviewed by supervisors and ISO 27001 experts.
d. Confirmability: Confirmability was evaluated by triangulating data from multiple sources to minimize bias. The researcher's personal reflections and discussions with the supervisor also helped maintain objectivity, while validation by the company and the examining lecturer ensured that the findings were objective and based on valid data.

3.9. Research Discussion

This research emphasizes the importance of information security for BPR, especially during ongoing digital transformation (DT). This research contributes to the existing body of work on the banking and insurance industry in Indonesia [6], [16], [38]. Previous studies have demonstrated the impact of agile-adaptive and traditional IT governance (ITG) mechanisms on digital transformation and organizational performance within this sector [6]. Additionally, a case study on BRI, a major bank in Indonesia, identified seven ambidextrous ITG mechanisms crucial for successful digital transformation [16]. Subsequent research [38], highlighted the significance of information security as key elements for achieving digital transformation success. This body of work underscores the broader importance of effectively managing both digital (exploration) and IT (exploitation) strategies to enhance performance during digital transformation initiatives.

This study confirms that effective information security implementation is critical to the success of digital transformation in SMEs such as BPR, particularly using the ISO 27001 standard. This is in line with the statement of one interview 2 participant who mentioned, “Yes, information security for BPRs is important, especially as it is required by regulations” [30], emphasizing that regulations also require the implementation of information security in BPR.

BPRACo faces challenges in implementing ambidextrous or hybrid information security, mainly due to limited human and financial resources. However, with the right approach, which combines agile methodologies for rapid response to security threats and traditional approaches to maintain operational stability, BPRACo can improve its information security efficiency and resilience. The results of this study provide important insights into how a flexible, ISO 27001-based information security approach can be adapted and implemented in organizations with limited resources.

As such, this research confirms that flexibility in information security approaches, in accordance with the ISO 27001 standard, is key to meeting the challenges of digital transformation. It paves the way for BPRACo to adopt more effective information security strategies, maximize the use of existing resources, and improve competitiveness in the digital age.

CONCLUSION

To answer the research questions, we first rely on the results from designing an information security management system based on ISO 27001: 2022 at BPRACo, it is concluded that although the priority steps of regulation and digital transformation have been carried out, there are still several clauses and annexes that have not been fulfilled or are only in the early stages of development. The six annex clauses that are top priorities are: 7.2 Competence, 8.1 Operational planning and control, 9.1 Monitoring, measurement, analysis, and evaluation, A.5.19 Information security in relationships with suppliers, A.5.20 Information security handling in agreements with suppliers, and A.7.11 Support utilities. Second, the recommendation process for this clause utilizes an appropriate people, process, and technology approach, which will strengthen BPRACo resilience in the face of digital transformation. These recommendations ensure that human resources have the right competencies, operational processes and controls are effective, and technology infrastructure and supplier relationships are secure and reliable. This research has limitations only on recommendations for designing an ISMS, not on evaluating the implementation and results of designing an ISMS. This research contributes to the development of knowledge in the field of information security management for TD in small banks and provides practical implications for the management of similar organizations.

BIBLIOGRAPHY

[1] K. Schwertner, “Digital transformation of business,” *Trakia Journal of Science*, vol. 15, no. Suppl.1, pp. 388–393, 2017, doi: 10.15547/tjs.2017.s.01.065.

[2] C. Gong and V. Ribiere, “Developing a unified definition of digital transformation,” *Technovation*, vol. 102, p. 102217, Dec. 2020, doi: 10.1016/j.technovation.2020.102217.

[3] G. Vial, “Understanding digital transformation: A review and a research agenda,” *The Journal of Strategic Information Systems*, vol. 28, no. 2, pp. 118–144, Jun. 2019, doi: 10.1016/j.jsis.2019.01.003.

[4] N. Mamuriyah, S. E. Prasetyo, and A. O. Sijabat, “Rancangan Sistem Keamanan Jaringan dari serangan DDoS Menggunakan Metode Pengujian Penetrasi,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 6, no. 1, pp. 162–167, Jan. 2024, doi: 10.47233/jteksis.v6i1.1124.

[5] A. Faidlatul Habibah and I. Irwansyah, “Era Masyarakat Informasi sebagai Dampak Media Baru,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 3, no. 2, pp. 350–363, Jul. 2021, doi: 10.47233/jteksis.v3i2.255.

[6] R. Mulyana, L. Rusu, and E. Perjons, “IT Governance Mechanisms that Influence Digital Transformation: A Delphi Study in Indonesian Banking and Insurance Industry,” in *Association for Information Systems (AIS)*, Pacific Asia Conference on Information Systems (PACIS), AI-IS-ASIA (Artificial Intelligence, Information Systems, in Pacific Asia), Jul. 2022.

[7] R. Mulyana, L. Rusu, and E. Perjons, “IT Governance Mechanisms Influence on Digital Transformation: A Systematic Literature Review,” in *Association for Information Systems*, AIS Electronic Library (AISeL), Aug. 2021. [Online]. Available: https://aisel.aisnet.org/amcis2021

[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 *Association for Information Systems*, Lisbon: International Conference on Information Systems Development, 2023, pp. 1–12.

[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, pp. 218–238, Oct. 2023, doi: 10.35746/jtim.v5i3.400.

[10] Y. W. Dwi, 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, pp. 1366–1380, 2023, doi: 10.35889/jutisi.v12i3.1488.

[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, pp. 1226–1229, 2023, doi: 10.35889/jutisi.v12i3.1513.

[12] N. Riznawati, R. Mulyana, and A. F. Santoso, “SEIKO : Journal of Management & Business Pendayagunaan COBIT 2019 DevOps dalam Merancang Manajemen Pengembangan TI Agile pada Transformasi Digital BankCo,” *SEIKO : Journal of Management & Business*, vol. 6, no. 2, pp. 2023–223, 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, pp. 452–467, Oct. 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, Aug. 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, pp. 388–406, 2023.

[16] R. Mulyana, L. Rusu, and E. Perjons, "Key ambidextrous IT governance mechanisms for successful digital transformation: A case study of Bank Rakyat Indonesia (BRI)," *Digital Business*, vol. 4, no. 2, p. 100083, 2024, doi: https://doi.org/10.1016/j.digbus.2024.100083.

[17] R. Siregar and E. Sudarmanto, "Beyond Traditional Boundaries: Embracing Digital Transformation for Enhanced Management Efficiency at Micro and Small Business Enterprises," *West Science Interdisciplinary Studies*, vol. 01, no. 06, pp. 267–279, 2023, doi: http://dx.doi.org/10.58812/wsis.v1i6.99.

[18] T. Hess, C. Matt, A. Benlian, and F. Wiesböck, "Options for Formulating a Digital Transformation Strategy," *MIS Quarterly Executive*, vol. 15, no. 2, pp. 103–119, 2016.

[19] S. Riyanto and E. Ariyanto, "Digital Transformation in the Indonesian Banking Industry: Impact on Employee Engagement," vol. 12, no. 4, 2020, [Online]. Available: www.ijicc.net

[20] M. Lubis, M. Kartiwi, and S. Zulhuda, "Current State of Personal Data Protection in Electronic Voting: Criteria and Indicator for Effective Implementation," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 16, no. 1, p. 290, Feb. 2018, doi: 10.12928/telkomnika.v16i1.7718.

[21] H. Haikal, R. H. Ananza, I. Darmawan, and R. Mulyana, "Perancangan Tata Kelola Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik (SPBE) Menggunakan Standar ISO 27001:2013 (Studi Kasus: Diskominfotik Kabupaten Bandung Barat)," 2019.

[22] S. M. T. Situmeang, "Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber," *SASI*, vol. 27, no. 1, p. 38, Mar. 2021, doi: 10.47268/sasi.v27i1.394.

[23] M. F. Safitra, M. Lubis, and A. Widjajarto, "Security Vulnerability Analysis using Penetration Testing Execution Standard (PTES): Case Study of Government's Website," in *Proceedings of the 2023 6th International Conference on Electronics, Communications and Control Engineering*, New York, NY, USA: ACM, Mar. 2023, pp. 139–145. doi: 10.1145/3592307.3592329.

[24] R. Ndegeya and R. Uwase, "Adapting ISO/IEC 27001 Information Security Management Standard to SMEs," Luleå University of Technology, Department of Computer Science, Electrical and Space Engineering, 2022.

[25] 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," in *eProceedings of Engineering*, eProceedings of Engineering, 2021.

[26] OJK, "Standar Penyelenggaraan Teknologi Informasi Bagi Bank Perkreditan Rakyat Dan Bank Pembiayaan Rakyat Syariah," Otoritas Jasa Keuangan. Accessed: Nov. 15, 2023. [Online]. Available: https://ojk.go.id/id/regulasi/Pages/POJK-tentang-Standar-Penyelenggaraan-Teknologi-Informasi-bagi-Bank-Perkreditan-Rakyat-dan-Bank-Pembiayaan-Rakyat-Syariah.aspx

[27] "ISO/IEC 27001:2022," ISO. Accessed: Jan. 06, 2024. [Online]. Available: https://www.iso.org/standard/27001

[28] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," Minnesota: Management Information Systems Research Center, University of Minnesota, Mar. 2004, pp. 75–105.

[29] I. Patricia, D. Ph, and L. R. Ness, "Are We There Yet? Data Saturation in Qualitative Research," Walden Faculty and Staff Publications, 2015. [Online]. Available: https://scholarworks.waldenu.edu/facpubs/455

[30] BPRACo, "Transkrip Interview BPRACo," Jun. 2024.

[31] M. Denscombe, *The Good Research Guide for Small Scale Research Projects*, Fourth. New York: Open University Press, 2010.

[32] R. K. Yin, "Discovering the Future of the Case Study. Method in Evaluation Research," *Eval Pract*, vol. 15, no. 3, pp. 283–290, Oct. 1994, doi: 10.1177/109821409401500309.

[33] OJK, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 7 Tahun 2024,"

ojk.go.id. Accessed: Jul. 05, 2024. [Online]. Available: https://ojk.go.id/id/regulasi/Pages/POJK-7-Tahun-2024-Bank-Perekonomian-Rakyat-dan-Bank-Perekonomian-Rakyat-Syariah.aspx

[34] 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, pp. 219–238, 2021, doi: 10.3390/jcp1020012.

[35] ISO 27005, “Information technology-Security techniques-Information security risk management,” 2018.

[36] 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, Apr. 2024, doi: 10.47738/ijaim.v4i1.70.

[37] A. K. Shenton, “Strategies for ensuring trustworthiness in qualitative research projects,” *Education for Information*, vol. 22, pp. 63–75, 2004, doi: 10.3233/EFI-2004-22201.

[38] R. Mulyana, L. Rusu, and E. Perjons, “Key Ambidextrous IT Governance Mechanisms Influence on Digital Transformation and Organizational Performance in Indonesian Banking and Insurance,” in *Pacific Asia Confefence on Information Systems*, Ho Chi Minh , Jul. 2024.