Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)

Journal Homepage: http://journal.lembagakita.org/index.php/jtik

Designing Information Security for BPRDCo SME Digital Transformation Using ISO 27001:2022

Ignatius Christ Surya [1*], Rahmat Mulyana [2], Ryan Adhitya Nugraha [3]

[1*] *Information Systems Study Program, Universitas Telkom, Bandung City, West Java Province, Indonesia.*
[2,3] *Department of Computer and Systems Science, Stockholm University, Frescativägen 54, Frescati, Stockholm, Sweden.*

a r t i c l e i n f o

Article history:
Received 30 Agustus 2024
Received in revised form
7 September 2024
Accepted 10 September 2024
Available online October
2024.

DOI:
https://doi.org/10.35870/jtik.v8i4.3148.

Keywords:
Digital Transformation;
Design Science Research;
Information Security; ISO
27001:2022; BPR.

Kata Kunci:
Transformasi Digital; Design
Science Research; Keamanan
Informasi; ISO 27001:2022,
BPR.

a b s t r a c t

In the digital era of the Industrial Revolution 4.0, organizations such as BPRDCo must undergo Digital Transformation (DT) to remain competitive. A significant challenge in this process is often the need for more information security controls, which can lead to DT failure. Previous studies emphasize the necessity of ambidextrous information security management—integrating both traditional and agile approaches—as a critical factor for DT success in large banks, especially in data management and information security. However, this strategy has not yet proven effective for smaller banks like BPRDCo. Therefore, this study aims to develop and propose priority information security management solutions specifically designed for SMEs while estimating the improvement in maturity levels to support DT success. The research adopts a five-stage Design Science Research (DSR) methodology: problem identification, requirements specification, design and development, demonstration, and evaluation. Data were gathered through interviews and document analysis using the ISO 27001:2022 Information Security Management System (ISMS) framework. Six priority PDCA and Annex controls were identified for BPRDCo as a case study. Six essential solutions were formulated using ISMS controls based on the identified gaps. These recommendations were compiled into an implementation roadmap to improve BPRDCo's readiness for full ISMS implementation and certification. This study provides valuable contributions to the knowledge base and offers practical implications for information security management in a small banks.

a b s t r a k

Dalam era digital Revolusi Industri 4.0, organisasi seperti BPRDCo harus menjalani Transformasi Digital (TD) untuk tetap kompetitif. Tantangan utama dalam proses ini sering kali adalah ketidakcukupan pengendalian keamanan informasi, yang dapat menyebabkan kegagalan TD. Penelitian sebelumnya menekankan pentingnya manajemen keamanan informasi ambidextrous—menggabungkan pendekatan tradisional dan agile—sebagai faktor kunci keberhasilan TD pada bank besar, terutama dalam manajemen data dan keamanan informasi. Namun, strategi ini belum terbukti efektif untuk bank yang lebih kecil seperti BPRDCo. Oleh karena itu, studi ini bertujuan untuk mengembangkan dan mengusulkan solusi manajemen keamanan informasi prioritas yang dirancang khusus untuk UKM, sambil memperkirakan peningkatan tingkat kematangan untuk mendukung keberhasilan TD. Penelitian ini menggunakan metodologi Design Science Research (DSR) dengan lima tahap: identifikasi masalah, spesifikasi persyaratan, desain dan pengembangan, demonstrasi, dan evaluasi. Data dikumpulkan melalui wawancara dan analisis dokumen, serta dianalisis menggunakan kerangka kerja Sistem Manajemen Keamanan Informasi (ISMS) ISO 27001:2022. Enam pengendalian prioritas PDCA dan Annex diidentifikasi untuk BPRDCo sebagai studi kasus. Berdasarkan kesenjangan yang teridentifikasi, enam solusi utama dirancang menggunakan kontrol ISMS. Rekomendasi ini disusun dalam bentuk peta implementasi untuk meningkatkan kesiapan BPRDCo dalam implementasi penuh ISMS dan sertifikasi. Penelitian ini memberikan kontribusi penting bagi basis pengetahuan dan implikasi praktis untuk manajemen keamanan informasi di bank kecil.

Corresponding Author. Email: ignchrist@student.telkomuniversity.ac.id [1].

ACM Computing Classification System (CCS)
EBSCOhost
Communication and Mass Media Complete (CMMC)

© E-ISSN: 2580-1643.

1. Introduction

Digital Transformation (DT) has significantly impacted various aspects of life, including the business world [1]. TD has become an inevitable phenomenon with the growing use of digital technology [2]. Digital transformation is a process of fundamental change caused by the innovative use of digital technology accompanied by strategic influence, resources, and critical capabilities to radically increase the value of an entity 3. DT can support organisations in creating new business models that are more effective and efficient, improve operations, and provide better and innovative customer experiences. It also aims to strengthen organisations through information technology [4][5]. DT is increasingly becoming a significant concern in the banking sector[6], with previous research suggesting that agile IT mechanisms have a considerable influence on DT [7]]. However, traditional IT is still necessary to support TD. A hybrid approach, which integrates traditional and agile methods, has proven effective in achieving optimal organisational performance [8].

In a previous study, a systematic literature review identified 28 IT governance mechanisms that affect TD. Integration of these mechanisms with Information Security Management Systems (ISMS) is essential to support TD while ensuring data security and compliance[7]. The traditional SMKI remains crucial to ensure information security and compliance, especially in implementing an SMKI that supports TD and protects digital assets [6]. The survey results show the importance of hybrid TKTI mechanisms, both traditional and agile, for organisational TD and performance achievement, especially in the context of SMKI, to ensure data security and compliance[9]. Research [10] on the BRI case study discusses how the dimensions of digital transformation impact organisational performance by implementing ambidextrous TKTI mechanisms as a critical influencer of digital transformation and organisational performance. This is followed by further research explaining that TD has significantly impacted organisational performance, showing that effective TKTI is the key to success in the digital era in the banking context [11], including the People's Economic Bank.

In addition, previous research has highlighted the critical function of IT services[12], IT risk management[13], information security[14], and DevOps practices [15] in driving digital transformation in large banks can be done by integrating essential elements of the COBIT 2019 framework. Similar research has also been conducted in various parts of the financial sector, with a focus on information security governance in insurance companies [4], [16] and fintech companies [17]. (BPR), which is on the scale of Micro, Small, and Medium Enterprises (SMEs). Since BPRs face digitalisation, fierce competition, and changes in customer behaviour, they need to implement SMKI to ensure that the data and information managed during the transformation process remain secure and maintain integrity.

According to [18], BPRs are conventional banks whose activities do not directly provide services in chiral traffic. BPR is an MSME-scale organisation because it is much more limited than commercial banks. After all,. BPRs cannot accept current account deposits, conduct foreign exchange transactions, or offer insurance products [19]. Research [20] shows that banks must keep up with technological development in digital-based services. This necessity is further strengthened by the Financial Services Authority (OJK) through the issuance of POJK No. 75/POJK.03/2016 and SEOJK No.15/SEOJK.03/2017, which requires BPR to adopt digitalisation to improve operational efficiency and customer service [21]. These changes enable BPRs to improve operational efficiency, meet customer expectations for faster and more accessible services, and maintain customer data security in the face of increasing cyber threats, one of which is implementing the ISO 27001:2022 standard. Previous Research Version 2013

However, DT adoption also brings significant challenges related to information security, such as the risk of data loss, unauthorised access, and infrastructure damage [22]. SMKI focuses on identifying possible and ongoing risks and handling the impact of these risks[23]. This imperative is further reinforced by the Financial Services Authority, which requires BPR to adopt digitalisation to improve operational efficiency and customer service [21]. A Financial Services Authority regulation requiring

BPRs and BPRSs to implement security measures to prevent security breaches that could harm them and their customers [24].

Small and medium-sized institutions such as BPRs can be categorised as being on the MSME scale, as explained in [25]. The SME sector is the backbone of the economy. SMEs play a vital role in the economy, representing most of the worldwide wealth [26]. SMKI can be used in the banking sector to develop security policies and risk management strategies that suit their scale and business needs. Thus, SMEs can improve protection against cyber threats and ensure business continuity in the digital era.

This research will explore how information security can be implemented at BPRDCo using the ISO 27001:2022 framework, a framework for information security that can help businesses develop and implement a sound information security management system (ISMS). The ISO 27001:2022 standard provides guidelines for establishing, implementing, maintaining and continuously improving an information security management system for enterprises of any size and sector [27], which is flexible and can be adapted to the organisation's needs to improve performance. ISO/IEC 27001:2022 is a global standard that outlines guidelines for managing information security in the enterprise. This specification enables organisations to protect the security of various data types, including employee information, financial records, intellectual property, and data shared with third-party entities [28]. ISO/IEC 27001:2022 is a global standard that outlines guidelines for managing information security in the enterprise. This specification enables organisations to protect the security of various data types, including employee information, financial records, intellectual property, and data shared with third-party entities [28].[27]. In this study, the application used for information security management at BPRDCO is ISO 27001: 2022.

The latest developments in ISO 27001:2022 that differentiate it from previous versions:

1) ISO 27001:2022 also accommodates the latest regulations related to information security. ISO 27001:2022 focuses on Information Security, Cybersecurity, and Privacy Protection. At this Privacy Protection point, Law Number 27 of 2022 concerning Personal Data Protection is accommodated.
2) Other updates include existing controls in ISO 27001:2013. ISO 27001:2013 has 114 controls, while ISO 27001:2022 only has 93 controls. The 93 controls in ISO 27001:2022 include 11 new controls, 24 combinations of several controls, and 58 updated controls.

Research Questions. Therefore, this study has developed several research questions to develop an information security management system in digital transformation. The main questions raised are: How can implementing the ISO 27001:2022 standard be recognised and designed to create an information security management system that focuses on the annexe clauses most relevant to the digital transformation of SMEs? In addition, to what extent does implementing an information security management system that complies with the main provisions of ISO 27001:2022 influence the success of digital transformation in SMEs?.

2. Research Methods

Conceptual Model

The conceptual model is a framework that can describe the identification of data elements in the research process and explain the involvement of a science's individuals, groups, and events. In this research, the framework used is Design Science Research (DSR), which can explain the performance of research using design science in information systems concisely and has clear guidelines for understanding, conducting, and evaluating research through a conceptual framework [29]. Researchers chose the ISO 27001:2022 type because the information security management system implemented according to this standard is a tool for better risk management, cyber resilience and operational excellence.

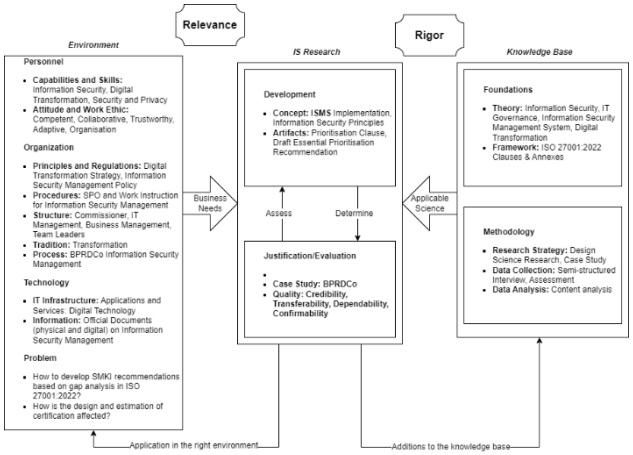

Figure 1. Hevner's DSR Conceptual Model [29]

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

1) Environment
   Refers to the context used for research, divided into four key areas: Personnel, which focuses on skills and capabilities; Organization, which examines the internal environment of the organization; Technology, which centers on infrastructure and information; and Problems, which serve as the initial indicators for the research.
2) IS Research
   Concentrates on the factors influencing research development and the evaluation processes involved in the study.
3) Knowledge Base
   Represents the foundational knowledge for the research, including the underlying theories and concepts, as well as the methodologies used for research strategies and analysis.

Research Process

The stages carried out by in this research as a guide to develop recommendations for optimising the objectives of ISO 27001: 2022 certification at BPRDCo, based on BPRDCo's current maturity level and what will be achieved. The method used is Johannesson's DSR which refers to Hevner's DSR. This method was chosen because the results of this research focus on essential improvements to the ISO 27001:2022 certification objectives that can be implemented by the organisation.

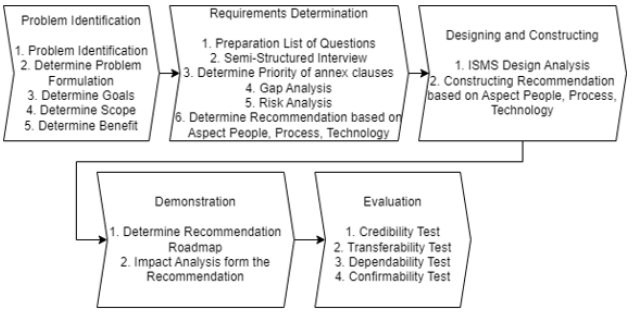

Figure 2. Systematic Problem Solving

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

1) Problem Explanation
   This stage begins with identifying problems by reviewing research on the application of ISO 27001:2022 within organizations, understanding ISO 27001:2022 as a best practice, comparing it with international standards such as COBIT 2019's Information Security Focus Area and NIST SP 800-53, considering national regulations on information security management, and examining internal documents of BPRACo. The researcher will then define the specific problem to be addressed, set the objectives, and establish the research boundaries. Once these steps are completed, verification will be sought from the supervisor regarding the planned research activities.
2) Determination of Needs
   In this stage, a list of questions is formulated based on the research needs, followed by semi-structured interviews. The next step is to prioritize clauses and annexes relevant to digital transformation, considering the organizational context. A risk analysis is then performed to select the appropriate clauses and annexes for recommendations. Finally, the chosen clauses and annexes are aligned with the aspects of people, processes, and technology.
3) Design and Manufacture
   This stage involves designing the information security management system according to the selected clauses and annexes. Recommendations for improvements are then made, focusing on the three key aspects: people, processes, and technology.

4) Demonstration
After designing the recommendations for the information security management system, a time estimation is carried out based on the selected clauses and annexes, and their impact on certification preparation is analyzed.
5) Evaluation
This stage involves conducting four testing steps to assess the effectiveness of the solution in addressing the problem. These steps include validating information data, evaluating how applicable the research results are within the organization, and using the findings as a basis for the organization to implement the information security management system.

Data Collection and Processing

The data collection process is the process of collecting data that will be the information needed in the research. Data collection was carried out using qualitative methods through semi-structured interviews and document triangulation to obtain two types of data, namely primary data and secondary data.

Table 1. Interview Activities

No	Interview	Date	Topic
1.	Deputy Head of IT Division Head of Information Security	15-03-2024	Initial visit for introductions and discussing plans during the research related to BPRDCo information security
2.	Deputy Head of IT Division Head of Information Security Section Head of IT Development	18-03-2024	Interviews and borrowing documents for research purposes
3.	Deputy Head of IT Division Head of Information Security Section Head of IT Development	21-03-2034	Interviews related to clauses and annexes
4.	Deputy Head of IT Division Head of Information Security Section Head of IT Development	16-05-2024	Interviews related to Digital Transformation and ISO 27001:2022 implementation
5.	Deputy Head of IT Division Head of Information Security Section Head of IT Development	14-06-2024	Interviews related to ISO 27001 controls, discussing ISO 27001:2022 certification plans, borrowing documents and being given explanations related to business processes in IT Development.

The findings of this research reveal that the current state highlights the importance of information security at BPRDCo. The digital transformation achievements at BPRDCo have shown significant progress. Additionally, the company's performance, when compared before and after obtaining ISO 27001 certification for information security, indicates a marked improvement. Interviews were conducted until no additional meaningful findings emerged, indicating that data saturation had been achieved. This was confirmed through several rounds of interviews to thoroughly examine the topic [30].

3. Results and Discussion

Results

Annex Clause Priority

The priority of the annexe clause is assessed based on three aspects, namely Regulation POJK No. 75 and SEOJK No. 15 research on information security management systems for SMEs and previous research

on digital transformation in the banking sector. Each aspect has equal weight, and the assessment is done by seeing whether the annexe clause is discussed in the three aspects. If the annexe clause is addressed in the element, it is given a plus; if it is not discussed in the aspect, it is crossed.

Conformity Assessment to Priority Clauses and Annex

This assessment aims to evaluate the effectiveness of the Information Security Management System (ISMS) that has been implemented in managing the company's information security.

Table 2. Current Grade Level

Value		Description
0	No	The organization has not implemented the annex clauses and controls. Indicates that the ISMS in the organization has not implemented and does not meet the requirements of the annex clauses and controls.
1	Fully	The organization has implemented the annex clauses and controls appropriately. Demonstrates that the organization has implemented appropriate procedures to meet the requirements of the annex clauses and controls.

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

1) Assessment (1)
   a) 4.1 Understanding the organization and its context
   b) 4.2 Understanding the needs and expectations of interested parties.
   c) 6.1 Actions to address risks and opportunities.
   d) 7.1 Resources.
   e) 7.4 Communication.
   f) 7.5 Documented information.
   g) 8.1 Operational planning and control.
   h) 9.1 Monitoring, measurement, analysis and evaluation.
   i) 5.2 Information security roles and responsibilities
   j) 5.19 Information security in supplier relationships
   k) 5.20 Addressing information security within supplier agreements
   l) 5.22 Monitoring, review and change management of supplier services
   m) 5.24 Information security incident management planning and preparation
   n) 5.31 Legal, statutory, regulatory and contractual requirements
   o) 6.2 Terms and conditions of employment
   p) 6.6 Confidentiality or non-disclosure agreements
   q) 7.5 Protecting against physical and environmental threats
   r) 7.11 Supporting utilities
   s) 8.6 Capacity management
   t) 8.14 Redundancy of information processing facilities
   u) 8.21 Security of network services
   v) 8.32 Change management
   w) 8.34 Protection of information systems during audit testing
2) Assessment (0)
   a) 6.3 Planning of changes
   b) 7.2 Competence.
   c) 5.9 Inventory of information and other associated assets
   d) 5.12 Classification of information
   e) 5.30 ICT readiness for business continuity
   f) 8.16 Monitoring activities.

Risk Analysis

At this stage, the level of possible risk (Probability) and the risk impact (Impact) of the clause and annex requirements that have not been met will be determined using the risk analysis standard in ISO 27005 [31].

Table 3. Probability Criteria

Probability	Level	Description
Rare	1	The risk probability is very rare or not yet known to occur.
Low	2	The risk probability is rare with a frequency of < 1 time per year.
Medium	3	The risk probability definitely occurs with a frequency of 1 time per 3 months.

Probability	Level	Description
High	4	The risk probability often occurs with a frequency of > 1 time per 3 months.
Very High	5	The risk probability very often occurs with a frequency of > 1 time per month.

Table 4. Impact Criteria

Value	Level	Description
Very Low	1	The impact that occurs does not disrupt organizational activities and the smoothness of its business processes.
Low	2	The impact that occurs slightly disrupts organizational activities and the smoothness of business processes is slightly disrupted.
Medium	3	The impact that occurs is quite disruptive to organizational activities and the smoothness of business processes is disrupted.
High	4	The impact that occurs disrupts organizational activities and the smoothness of business processes is disrupted.
Very High	5	The impact that occurs is very disruptive to organizational activities and business processes are stopped.

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 25.

Table 5. Risk Matrix

Probability	Impact				
	Very Low (1)	*Low* (2)	*Medium* (3)	*High* (4)	*Very High (5)*
Rare (1)	1	2	3	4	5
Low (2)	2	4	6	8	10
Medium (3)	3	6	9	12	15
High (4)	4	8	12	16	20
Very High (5)	5	10	15	20	25

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) in the assessment process

Table 6. Risk Analysis Result

Clause/Annex	Probability	Impact	Score	Risk Level
6.3 Planning of changes.	3	4	12	High
7.2 Competence	3	4	12	High
5.9 Inventory of information and other associated assets	3	3	9	Medium
5.12 Classification of information	3	4	12	High
5.30 ICT readiness for business continuity	2	5	10	High
8.16 Monitoring Activities	3	3	9	Medium

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

1) Low 1-4
2) Medium 5-9
3) High 10-16
4) Extreme 20-25

Annex Clauses Prioritization Result

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

Table 7. Prioritazion Result

Clauses & Annex	Priority	Assessment	Risk
6.3 Planning of changes.	100	0	High
7.2 Competence	100	0	High

5.9 Inventory of information and other associated assets	100	0	Medium
5.12 Classification of information	100	0	High
5.30 ICT readiness for business continuity	100	0	High
8.16 Monitoring Activities	100	0	Medium

Design of Information Security Management System (ISMS)
By planning, modifying, and managing priority information security at BPRDCo 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, the information security management system design at BRPDCo aims to improve organizational readiness for digital transformation. This design involves aspects of people, process, and technology.

Table 8. Recommendation Aspect

Clause & Annex	Aspect
6.3 Planning of changes.	*People, Process*
7.2 Competence	*People, Process*
5.9 Inventory of information and other associated assets	*People*, *Process*
5.12 Classification of information	*People, Process*
5.30 ICT readiness for business continuity	*People, Process, Technology*
8.16 Monitoring Activities	*Process*

1) People Aspect Design

In an effort to improve information security, the people aspect recommendations in the ISO 27001 standard on information security relate to recommendations covering responsibility, skills, awareness, and communication.

a) Responsibility Recommendations, this research aims to identify key roles in managing changes to the Information Security Management System (ISMS) in accordance with the ISO 27001:2022 standard and the skills needed to carry out these responsibilities. Within the organisation, these roles include the Head of IT Operations & Security, Deputy Head of IT, Head of IT Development, Head of IT Helpdesk, IT Librarian/Asset Manager, and IT Operations Staff. The results show that each role has specific responsibilities related to aspects of information security, change management, training, and asset management. In addition, skills such as information security, risk analysis, change management, and communication are necessary to perform these tasks effectively. This research emphasises the importance of an in-depth understanding of ISO 27001:2022 and its application in change management in IT environments.

b) Skill & Awareness recommendations, Skills in change management were also identified as essential, particularly in managing change in accordance with information security standards. In addition, the study identified gaps in ICT readiness, particularly in disaster recovery management, application security, network security and handling system integration. Personnel need to develop capabilities in planning comprehensive recovery strategies, protecting applications during recovery, restoring networks after disruptions, as well as optimising recovery processes to improve efficiency and reduce errors. This research recommends training and certifications such as ISO 27001:2022, CISSP, CISM, as well as ITIL 4 Foundation, to close the skills gap, ensuring that personnel have the necessary competencies to maintain effective information security and business continuity.

2) Process Aspect Design

The process aspect involves developing and implementing effective policies, procedures and work instructions. Well-documented and consistently followed processes help reduce risk and ensure compliance with security standards.

a) Procedure Recommendation, below is a draft solution in the form of a policy that can be a procedure recommendation:
   1. Change Management SOP.
   2. Employee Competency Development SOP.
   3. Information and Asset Inventory SOP.

4. Information Classification SOP.
5. Prevention and Readiness SOP.
6. Monitoring Activities SOP.

b) Recommendation Record, here is a solution design in the form of a record or working paper that the company can use as a recommendation:
1. Change Management Record Report.
2. Employee Competency Document.
3. Inventory and Asset Documents.
4. Information Classification Documents and Working Papers.
5. DRP Working Paper.
6. Monitoring Activities Document.

3) Technology Aspect Design

In an effort to improve information security, it is important for organizations to pay attention to the technological aspects that involve the use of tools and features that support information security. Implementing the right technology, such as security monitoring tools and recovery plan simulations, helps organizations detect and respond to threats quickly and effectively. Providing recommendations for supporting tools that can be used that are expected to help companies improve ICT readiness for business continuity.

Roadmap Recommendations Implementation Design

Roadmap refers to the planned schedule and implementation strategy of the proposed recommendations. This roadmap serves as a guide to direct the steps needed to implement the recommendations effectively.

Table 9. Roadmap Recommendations

Activity	Period			
	2024			
	Sep	Okt	Nov	Dec
Aspek People				
6.3 Planning of changes.				
7.2 Competence				
5.9 Inventory of information and other associated assets				
5.12 Classification of information				
5.30 ICT readiness for business continuity				
Aspek Process				
6.3 Planning of changes.				
7.2 Competence				
5.9 Inventory of information and other associated assets				
5.12 Classification of information				
5.30 ICT readiness for business continuity				
8.16 Monitoring activities				
Aspek Technology				
5.30 ICT readiness for business continuity				

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

1) In September, the implementation of recommendations from clause 6.3 Planning of Changes, 7.2 Competence, and annex 8.16 Monitoring Activities will be carried out. Starting with the determination of the Responsibility and Skill & Awareness recommendations that will support 6.3 and 7.2, then continued with the implementation of the Procedure and Record recommendations that will update existing procedures and working papers to meet the requirements of clause 6.3, 7.2, and annex 8.16.
2) In October, the implementation of recommendations from annex 5.9 Inventory of information and other associated assets and 5.12 Classification of information will be carried out. Starting with the determination of recommendations for Responsibility and Skill & Awareness which will support 5.9 and 5.12. Then continued with the implementation of recommendations for Procedures and Records which will update existing procedures and working papers to meet the requirements of annex 5.9 and 5.12.
3) In November, the implementation of annex 5.30 ICT readiness for business continuity will be carried out which has three aspects of recommendations. Starting with Responsibility and Skill & Awareness, then continued with the implementation of recommendations for

Procedures and Records which will update procedures and working papers, and recommendations for Tools to support technology-based readiness to meet the requirements of annex 5.30.

4) December can be used for recap and can immediately carry out ISMS certification for BPRDco.

Research Quality

Trustworthiness Evaluation Results

The research was assessed through four quality testing stages to gauge the effectiveness of the proposed solution according to [32]. Credibility was established using data from interviews, surveys, and document analysis, validated by ISO 27001 experts. Transferability involved detailed descriptions of the BPR organization to allow for adaptability assessments in similar settings. Dependability and confirmability were achieved through detailed documentation, consistent methodologies, and multiple data sources to minimize bias and ensure objectivity, with all findings being validated by experts and relevant stakeholders.

Discussion

This research highlights the crucial role of information security for BPR, especially during the ongoing digital transformation (DT). It contributes to the existing body of knowledge on the banking and insurance industry in Indonesia [6], [10], [11]. Prior studies have shown how agile-adaptive and traditional IT governance (ITG) mechanisms influence digital transformation and organizational performance in this sector [6]. A case study on BRI, a leading bank in Indonesia, identified seven ambidextrous ITG mechanisms essential for successful digital transformation [10]. Further research [11] emphasized the importance of information security as a key element in achieving digital transformation success. This body of work underscores the broader significance of effectively managing both digital (exploration) and IT (exploitation) strategies to enhance performance during digital transformation initiatives.

This study confirms that effective implementation of information security is critical to the success of digital transformation in SMEs like BPR, particularly using the ISO 27001 standard. This aligns with the statement of one interview participant who noted, "Information security for BPRs is important, especially as it is required by regulations," highlighting the regulatory requirement for information security implementation in BPRs.

BPRDCo faces challenges in implementing ambidextrous or hybrid information security approaches, primarily due to limited human and financial resources. However, with the right strategy, which combines agile methodologies for rapid response to security threats and traditional approaches to maintain operational stability, BPRDCo can enhance its information security efficiency and resilience. The findings of this study offer valuable insights into how a flexible, ISO 27001-based information security approach can be adapted and applied in organizations with limited resources.

This research confirms that flexibility in information security approaches, aligned with the ISO 27001 standard, is crucial for addressing the challenges of digital transformation. It paves the way for BPRDCo to adopt more effective information security strategies, optimize the use of existing resources, and improve competitiveness in the digital era.

4. Conclusions

To answer the research questions, we first rely on the results from designing an information security management system based on ISO 27001: 2022 at BPRDCo; 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 annexe clauses that are top priorities are 6.3 Planning of Changes, 7.2 Competence, A.5.9 Inventory Of Information and Other Associated Assets, and A.5.12. Classification Of Information, A.5.30 ICT Readiness for Business Continuity, and A.8.16 Monitoring Activities. Second, the recommendation process for this clause utilizes an appropriate people, process, and technology approach, which will strengthen BPRDCo's resilience in the face of digital transformation. To improve information security in an organization, it is necessary to assign clear responsibilities to specific roles, which should be accompanied by relevant training programs to enhance employee skills and awareness. In

addition, developing six new procedures and six records or worksheets is essential to strengthen operational security practices and ensure existence and traceability. Challenges faced by users of ISO 27001:2022 include developing a comprehensive set of controls to cover all potential security, cybersecurity and privacy obligations, which are complex.

Finally, recommendations for supporting tools are also needed to improve the company's ICT readiness, which will help maintain business continuity in facing digital challenges. This research has limitations only on recommendations for designing an ISMS, not on evaluating the implementation and results of creating 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.

5. References

[1] Schwertner, K. (2017). Digital transformation of business. *Trakia Journal of Science, 15*(Suppl. 1), 388–393. https://doi.org/10.15547/tjs.2017.s.01.065

[2] Hadiono, K., Candra, R., & Santi, N. (2020). *Menyongsong Transformasi Digital.*

[3] Gong, C., & Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation, 102*. https://doi.org/10.1016/j.technovation.2020.102217

[4] 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

[5] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *Elsevier B.V.* https://doi.org/10.1016/j.jsis.2019.01.003

[6] Mulyana, R., Rusu, L., & Perjons, E. (2022). IT Governance mechanisms that influence digital transformation: a delphi study in indonesian banking and insurance industry. In *Pacific Asia Conference on Information Systems (PACIS), AI-IS-ASIA (Artificial Intelligence, Information Systems, in Pacific Asia), Virtual Conference, July 5-9, 2022*. Association for Information Systems (AIS).

[7] Mulyana, R., Rusu, L., & Perjons, E. (2021). IT governance mechanisms influence on digital transformation: A systematic literature review. In *Twenty-Seventh Americas' Conference on Information Systems (AMCIS), Digital Innovation and Entrepreneurship, Virtual Conference, August 9-13, 2021* (pp. 1-10). Association for Information Systems (AIS).

[8] Mulyana, R., Rusu, L., & Perjons, E. (2023). How Hybrid IT Governance Mechanisms Influence Digital Transformation and Organizational Performance in the Banking and Insurance Industry in Indonesia. In *The International Conference on Information Systems Development (ISD)* (pp. 1-12). Association for Information Systems (AIS).

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

[10] Mulyana, R., Rusu, L., & Perjons, E. (2024). The influence of key ambidextrous IT governance mechanisms on digital transformation and organizational performance in the Indonesian banking and insurance industry. *PACIS 2024 Proceedings*. https://aisel.aisnet.org/pacis2024

[11] Tarbiyatuzzahrah, B. 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

[12] Dwi, Y. W., Dewi, M., Mulyana, R., & Santoso, A. F. (2023). Penggunaan COBIT 2019 I&T risk management untuk pengelolaan risiko transformasi digital BankCo.

[13] Rahmadana, A., Mulyana, R., & Santoso, A. F. (2023). Pemanfaatan COBIT 2019 information security dalam merancang manajemen keamanan informasi pada transformasi BankCo.

[14] Riznawati, N., Mulyana, R., & Santoso, A. F. (2023). Pendayagunaan COBIT 2019 DevOps dalam merancang manajemen pengembangan TI Agile pada transformasi digital BankCo. *SEIKO: Journal of Management & Business, 6*(2), 2023–223.

[15] Anugerah, M. R. A. W. (2023). Manajemen keamanan informasi untuk transformasi digital Insurco berbasis COBIT 2019 focus area information security.

[16] Prayudi, R. A., Mulyana, R., & Fauzi, R. (2023). Pengendalian digitalisasi FintechCo melalui perancangan pengelolaan keamanan informasi berbasis COBIT 2019 information security focus area. *SEIKO: Journal of Management & Business, 6*(2), 388–406.

[17] POJK 7. (2024). *POJK 7 Tahun 2024 Bank Perekonomian Rakyat dan Bank Perekonomian Rakyat Syariah.*

[18] POJK 20. (2014). *POJK 20. Bank Perkeditan Rakyat.*

[19] Shabri, H., et al. (2020). Transformasi digital industri perbankan syariah Indonesia. *Jurnal Ekonomi dan Keuangan Syariah, 3*(2).

[20] POJK75. (2016). *Peraturan Otoritas Jasa Keuangan (PP Nomor 75 Tahun 2016).*

[21] Haikal, H., Ananza, R. H., Darmawan, I., & Mulyana, R. (2019). Perancangan tata kelola keamanan informasi sistem pemerintahan berbasis elektronik (SPBE) menggunakan standar ISO 27001:2013 (studi kasus: Diskominfotik Kabupaten Bandung Barat).

[22] Panjaitan, B., Abdurrahman, L., & Mulyana, R. (2021). Pengembangan implementasi sistem manajemen keamanan informasi berbasis ISO 27001:2013 menggunakan kontrol Annex: Studi kasus data center PT. XYZ.

[23] SEOJK15. (2017). *SAL SEOJK 15 - SPTI BPR BPRS_240115_203306*.

[24] Moeti. (2022). Information security framework adoption for South African SME.

[25] Nistotskaya, M., Charron, N., & Lapuente, V. (2014). The wealth of regions: quality of government and SMEs in 172 European regions. *Environment and Planning C: Government and Policy, 0*(0), 0–0. https://doi.org/10.1068/c13224r

[26] ISO 27001. (2022). *Information security, cybersecurity, and privacy protection-Information security management systems-Requirements*.

[27] Obuh, D. (2023). The structure of the ISMS documentation in accordance with updates to ISO 27001:2022, 27002:2022.

[28] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research.

[29] 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

[30] ISO 2018. (2018). *Information technology-Security techniques-Information security risk management*.

[31] 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.