 p-ISSN 2827-8585
e-ISSN 2827-8062

International Journal of Multidisciplinary Research and Literature
IJOMRAL
Vol. 4, No. 4, July 2025 pp. 771-783
Journal Page is available at http://ijomral.esc-id.org/index.php/home

ANALYSIS OF THE IMPLEMENTATION OF ISO/IEC 27001:2013 STANDARDS IN PT. SULSELBAR BANK

Kristian Gala[1*], Rahman Suwandaru[2], Muh. Ashary Anshar[3]
[1.2,3]Nitro Institute of Business and Finance, Indonesia
Corresponden Email: *Kristian.gala@yahoo.co.id*[1]

Abstract

This study aims to examine the implementation of the ISO/IEC 27001:2013 standard in optimizing the information security system at PT. Bank Sulselbar. This international standard is the main reference in information security management which includes structured policies, procedures, and technical controls to protect the confidentiality, integrity, and *availability of data. This study uses a descriptive qualitative approach with a focus on analyzing the implementation and effectiveness of the ISO/IEC 27001:2013 standard and identifying potential weaknesses in the company's information security system. The main object of the study is how the information security management system (ISMS) based on ISO/IEC 27001:2013 has been implemented in the operational environment of Bank Sulselbar. Data were collected through interviews, observations, and documentation studies of work units relevant to information security.*

The results of the study indicate that PT. Bank Sulselbar has implemented an ISO/IEC 27001:2013-based ISMS in a systematic and structured manner, which includes security policies, risk assessments, access control, and continuous monitoring and evaluation of the system. This implementation has been proven to increase the level of company information protection and strengthen resilience to cyber threats. However, this study also identified several weaknesses, including aspects of human resource awareness of the importance of information security and the need for increased periodic training. Thus, the implementation of ISO/IEC 27001:2013 has made a significant contribution in optimizing the information security system at PT. Bank Sulselbar, but continuous improvement is still needed in several aspects to achieve optimal effectiveness.

Keywords: *STANDARDISO/IEC* 27001:2013

INTRODUCTION

In today's competitive business era, and in the current digital era, it is important for companies to not only focus on product development, but also on improving the quality of their product services. PT. Bank Sulselbar with a vision to become a proud and leading bank to develop the eastern region of Indonesia and a mission to provide innovative financial service solutions to the government and the community based on excellent service and the principle of prudence, is one of the banking companies that provides conventional and sharia services with strengthening digitalization to improve the quality of services and product and service features. Therefore, guaranteeing the availability and security of the managed information systems and technology is a top priority for Bank Sulselbar in the current digitalization era.

In carrying out its business activities, PT. Bank Sulselbar, hereinafter referred to as the company, stores and manages various types of information, financial transactions, reports, and other information as an essential part of its operational activities. Information security threats in the current digital era, such as leaks, damage, inaccuracies, or other disruptions to information, can have detrimental financial and non-financial impacts on the company.

Given that information is a critical asset for a company, it must be protected and secured from the risk of leakage, damage, inaccuracy, loss, and misuse, whether intentional or unintentional. The level of information protection and security will depend on the sensitivity and criticality of the information.

Adequate information security management will protect information from various security threats and can improve the efficiency, effectiveness, and overall operational performance of a company, which means increased productivity, competitiveness, profits, reputation, and compliance with rules and regulations. In an effort to improve adequate security for company information, it is deemed necessary to implement standards or controls and systems to monitor information security management. This has been regulated by the regulator through the Financial Services Authority circular letter number 21/SEOJK.03/2017 concerning the implementation of risk management in the use of information technology and POJK Number 11/POJK.03/2022 concerning the implementation of information technology by commercial banks.

In this case, PT. Bank Sulselbar has implemented a standard or control called*ISO/IEC 27001:2013* which is considered important and useful to help organizations/companies manage the security of information assets such as financial information. Given that information is a very important asset for a company, it must be protected or secured from the risk of leakage, damage, inaccuracy, loss, and misuse, whether intentional or not.

*ISO/IEC 27001*is an international standard that regulates information security management systems*(Information Security Managemen System/ISMS)*, which was released by*international organization for standardization (ISO) dan international electrotechnical commission (IEC).*By implementing standards*ISO/IEC 27001*Since 2020, PT. Bank Sulselbar has committed to ensuring that all data and information received and processed is secure and used only by authorized parties with full responsibility.

In implementing the ISO/IEC 27001:2013 standard at PT. Bank Sulselbar, several obstacles hampered the optimization of the information security management system. One of the main obstacles identified was limited human resources. This limitation was reflected in the lack of technical expertise and in-depth understanding of the information security management system among employees. This caused the ISO implementation process to proceed slower than planned. Therefore, the company's management is expected to provide relevant training and capacity building to ensure more effective and efficient implementation of this system.

In addition to limited human resources, another obstacle is the company's limited funds. The ISO certification process requires significant costs, from document preparation and consultation to training and external audits. If the company does not have adequate budget allocation, the certification process can be delayed or not run optimally. In this context, it is important for PT. Bank Sulselbar to have a definite budget plan to support all stages of certification. Other obstacles include the implementation of work procedures that are not fully in accordance with established standard operating procedures (SOPs), as well as a lack of commitment from some employees. In fact, the core of implementing ISO/IEC 27001:2013 is continuous improvement efforts (*continuous improvement*). Organizations are required to

implement the PDCA cycle (*Plan–Do–Check–Action*) comprehensively and consistently across all lines.

Based on the background discussion above, the author is interested in conducting research with the title*"Analysis of the Implementation of ISO/IEC 27001:2013 Standard at PT. Bank Sulselbar."*This research has novelty in the context of the focus of the study which not only analyzes the extent to which the ISO/IEC 27001:2013 standard has been implemented in the regional banking environment, but also identifies in depth the internal and external barriers that hinder the implementation process, and provides a critical analysis of the readiness of organizational culture in supporting the sustainability of the information security management system. Different from previous studies that generally focus on large-scale national companies, this study provides a scientific contribution by highlighting the implementation of international standards in regional-level financial institutions, which have different resource challenges and managerial structures. The findings of this study are expected to be the basis for strategic decision-making for the management of PT. Bank Sulselbar, as well as being a practical reference for similar financial institutions that are trying to strengthen their information security through the ISO/IEC 27001:2013 standard.

LITERATURE REVIEW

ISO/IEC 27001

ISO/IEC 27001 is an information security management system standard designed to systematically establish, implement, monitor, and improve information protection (ISO/IEC, 2005). Its latest version, ISO/IEC 27001:2013, serves as an essential guideline for organizations in implementing a comprehensive information security concept. Implementing this standard enables companies to effectively manage risks, enhance customer trust, and ensure compliance with applicable regulations. Furthermore, ISO 27001 supports business continuity and strengthens information security management within the supply chain, making it a strategic tool for maintaining the integrity and confidentiality of an organization's information.

Strategic Management

Strategic management is the grand theory in this study because it provides a comprehensive framework for guiding an organization toward its goals. Management is defined as a series of processes encompassing planning, organizing, implementing, monitoring, and controlling organizational resources to achieve specific goals (Riyadi, 2019). Meanwhile, strategy is the art of effectively utilizing organizational skills and resources in response to changing environmental conditions (Budio et al., 2019). Strategy is also a tool for achieving an organization's long-term goals through appropriate actions and resource allocation (Persari et al., 2018). Antariksa et al. (2017) added that strategic management is the art and science of formulating, implementing, and evaluating cross-functional decisions to optimally achieve organizational goals.

Banking Digitalization

According to Wike, digital technology represents a shift from manual work systems to automated, computer-based systems, enabling more sophisticated and efficient operations. This technological development is marked by the emergence of various modern communication tools that enable the sending and receiving of information without the constraints of space and time. In the current digital era, nearly all sectors, including banking, have utilized information technology to improve the effectiveness and efficiency of their business processes. In the banking context, digitalization encompasses services such as ATMs, EDCs, internet banking, SMS banking, and phone banking, which are considered capable of facilitating transactions while strengthening relationships with customers (Wike, 2021).

Information Technology

Technology is a process that increases added value through the use or production of interconnected products in a system (Miarso, 2007). Castells (2004) adds that technology is a collection of tools, rules, and procedures resulting from the application of scientific knowledge that allows for the repetition of functions in certain jobs. Based on these two views, it can be concluded that technology was created to facilitate human activities repeatedly and systematically. Meanwhile, information is the result of processing data into a form that is useful for decision-making (Jogiyanto, 1999; Sidharta, 1995). Information technology itself is the application of technology to manage information quickly, precisely, and efficiently (Nuryanto, 2012; Lucas, 2000; Loudon, 2004).

Thinking Framework

A conceptual framework is a theoretical basis for research that explains the relationships between variables to answer the research problem. According to Barlian (2018:32), a conceptual framework describes and clarifies the relationships between relevant variables in a study. Sugiyono (2017:60) adds that a conceptual framework is a conceptual model that illustrates the relationship between theory and important factors in a study. This framework explains the relationships between independent, dependent, and moderator or intervening variables, which are then formulated in the form of a research paradigm. Based on the strategic theory used, the research conceptual framework can be described as follows.

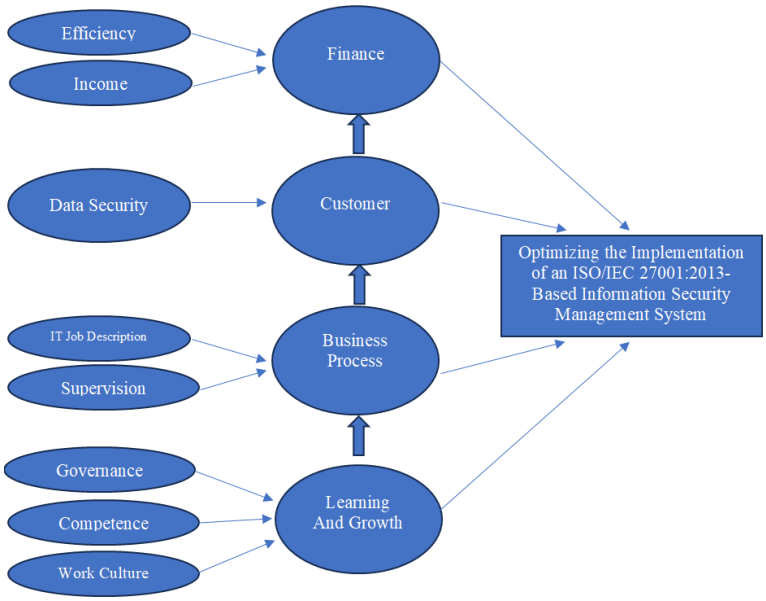

Figure 1 Conceptual Framework

METHOD

Research methods

A research method is a systematic procedure used to obtain data and knowledge in a structured manner in a study (Sugiyono, 2017). Methodology is the study of the rules within a research method. In this study, the researcher used a qualitative method with primary data sources from interviews and direct observation of informants regarding the implementation of ISO/IEC 27001:2013 at PT. Bank Sulselbar.

Location and Time of Research

The research was conducted at PT. Bank Sulselbar for approximately four months, from January to May 2025. The selection of this location and time was aimed at ensuring optimal and comprehensive data collection, so that the research results could reflect the actual conditions in the field.

Data Types and Sources

The type of data collected was qualitative, in the form of statements, experiences, and observations related to the implementation of information security systems. Primary data was the primary source, obtained directly from interviews and observations, providing an in-depth overview of ongoing practices (Creswell, 2014).

Data Collection Methods and Techniques

Data collection was conducted using two main methods: interviews and observation. In-depth interviews were conducted with five purposively selected key informants: the head of the IT Division of PT. Bank Sulselbar, IT Support of PT. Bank Panin Makassar, the

committee/supervisory board of PT. Bank Sulselbar, the OJK supervisor, and an ISO/IEC 27001:2013 expert. The objective was to obtain information on security governance, constraints, oversight, and customer and regulator perspectives. Direct observations were conducted to observe the implementation of the security system and its dynamics in the field (Sugiyono, 2017).

Data collection techniques included verbal data (informants' words), non-verbal data (attitudes and reactions), and photographic documentation. Interviews used semi-structured instruments to ensure a natural flow of conversation, supported by the use of cameras, voice recorders, and field notes.

Research Informants and Research Instruments

Informants were selected using purposive sampling techniques, based on relevance criteria and research needs (Sugiyono, 2017). The five main informants were considered to have sufficient knowledge and experience to provide valid and in-depth data on the implementation of ISO/IEC 27001:2013 at PT. Bank Sulselbar. The instrument consisted of a list of open-ended questions aimed at exploring aspects of policy, implementation, evaluation, and obstacles in implementing the ISO/IEC 27001:2013 information security management system at the company (Creswell, 2014).

Data analysis

Data analysis was conducted using a qualitative approach based on post-positivism and interpretive philosophies. Data collection utilized triangulation techniques between interviews, observation, and documentation to increase data validity (Sugiyono, 2017). A narrative approach was also used by compiling a chronological report of the informants' experiences and information.

The analysis process includes:

1. Data reduction, which is the process of filtering and simplifying raw data into more focused and meaningful information, is carried out continuously during data collection.
2. Data presentation, namely the systematic arrangement of data to facilitate understanding and analysis.
3. Drawing conclusions and verification, where data is analyzed to find patterns and themes and cross-checking is carried out to ensure the accuracy of the results.

RESEARCH RESULTS AND DISCUSSION

Research result'

This study uses a qualitative method with data collection through open and in-depth interviews to support the analysis of the implementation of the ISO/IEC 27001:2013 standard at PT. Bank Sulselbar. The implementation of this standard aims to improve customer data security and customer trust to support the company's growth. The interviews involved five informants:

the head of the IT division of PT. Bank Sulselbar, Makassar technical support, representatives of the audit committee, OJK supervisors, and senior consultants from PT. Aplikanusa Lintasarta.

1. First Informant

   The first informant was Mr. Mawardi, S.E., Head of the Information Technology Division of PT. Bank Sulselbar. The interview was conducted on March 4, 2025, and revealed that since the implementation of the ISO/IEC 27001:2013 Information Security Management System (ISMS) in 2020, Bank Sulselbar has established a clear organizational structure with defined duties and responsibilities, approved by the board of directors. All IT staff are actively involved according to their respective duties, from information security officers, risk management, to internal auditors. Internal policies and standards are outlined in the Company Manual (BPP) and SOPs that support governance that runs according to procedures, supported by continuous evaluation and training to improve team competency.

   In terms of oversight, Bank Sulselbar conducts periodic internal audits and external audits through certification bodies to ensure compliance with ISO standards. The learning and growth process is carried out through internal training and customer education regarding information security, as well as regular monitoring of bank branches. Management is strongly committed to ensuring information security to build customer trust, in accordance with OJK regulations and related laws. Management's efforts in managing the costs and benefits of implementing an ISMS ensure spending efficiency and increased customer trust, which leads to growth in the bank's customer base.

2. Second Informant

   The second informant was Mr. Ardhiansyah Putra, S.Kom, as the Technical Support Region (TSR) of Bank Panin KCU Makassar. In an interview on February 28, 2025, he explained that the organizational structure and job descriptions specifically for TSR and IT Support at the branch are already in place, with clear department heads and IT heads. All IT staff, including TSR, are actively involved in the implementation of the information security management system, responsible for safeguarding customer and company data in accordance with work procedures that are always revised and periodically socialized via zoom or email to branches. Supervision is carried out through routine audits in accordance with central policies that regulate all branches, both internally and externally.

   Regarding learning and growth, education and guidelines related to the ISMS are delivered by the head office and serve as a reference for branches, with active coordination provided for any unclear matters. Management is highly concerned about customer data security, considering that data breaches are a serious matter with strict sanctions for violators. The implementation of the ISMS has been socialized to customers, who have responded positively due to a sense of security and comfort. Management is also strict in maintaining data confidentiality, such as prohibiting photos or data distribution, and fully supports the costs of implementing an information security system to protect customer data.

3. Third Informant

The third informant, Mr. Faisal, S.T., MPP, a representative of the Commissioner/Audit Committee of PT. Bank Sulselbar, stated that the organizational structure related to the information security management system has been officially regulated in a board of directors' decree and follows the established criteria. All IT staff are involved in the implementation of the ISMS, but primary oversight is carried out by top management. Adequate policies and procedures that comply with ISO 27001 standards form the basis of governance, and oversight is carried out actively by the board of directors, internal audit, and external supervisors. Although IT audits are already underway, specific ISMS audits need to be improved. Learning and growth processes are important to improve the competency of IT employees, in accordance with Bank Indonesia's recommendation that IT risks are still moderate.

Management fully supports IT development and information security, particularly in the digital era. Although there have been complaints related to customer incidents, this has become a serious concern for strengthening the security system. Bank Sulselbar also complies with regulations, such as POJK No. 11 and SE OJK, with clear policies and SOPs. Efforts to improve the competency of IT staff so they can manage their ISMS independently are expected to reduce reliance on vendors and optimize costs, while maintaining the bank's reputation and readiness to face digital challenges.

4. Fourth Informant

The fourth informant, Mr. Laode Rusly Ibrachim, an OJK supervisor, explained that according to POJK 11 of 2022, banks are required to establish a structure or unit responsible for managing information security systems, including cyber resilience, tailored to the complexity of the bank's needs. All IT staff must be involved in implementation, with distinct roles according to their respective duties and functions, such as a development team ensuring system security, an operational team maintaining infrastructure, and a security team establishing incident response policies. Written policies and standards related to the ISMS are also required as part of IT governance and risk management. For effective governance, banks must have a clear organizational structure, conduct regular training and monitoring, and align work standards with frameworks such as ISO 27001.

Furthermore, comprehensive internal oversight is necessary to ensure compliance and effectiveness of the ISMS, and the Financial Services Authority (OJK) encourages audits and continuous improvement. Learning and growth are supported through regular training, security awareness, benchmarking, and seminars to update the IT team's knowledge in line with the development of digitalization. Management plays a crucial role in establishing policies, providing human resources, and overseeing the implementation of the ISMS. To improve customer satisfaction, banks routinely conduct data security education and outreach through social media and provide a complaint channel. Management also manages the costs and benefits of implementing the ISMS using a risk-based investment approach, budget efficiency, and continuous evaluation to ensure that security investments are commensurate with the results achieved.

5. Fifth Informant

The fourth informant, Mr. Laode Rusly Ibrachim, an OJK Supervisor, stated that based on POJK 11 of 2022, banks are required to establish an organizational structure or dedicated unit to manage their information security management systems, including cybersecurity and resilience. Adjustments to this structure must take into account the complexity and needs of each bank, and banks are required to conduct independent assessments of their cybersecurity maturity levels. In implementing an information security system, all IT staff are involved according to their respective responsibilities and functions, such as the development team that ensures security when creating the system, the operational team that monitors and maintains the infrastructure, and the security team that establishes incident response policies. Furthermore, banks are required to have written policies and standards that support IT governance and risk management as a reference for implementing the ISMS.

To ensure effective IT governance, in accordance with its mandate, banks must establish a clear organizational structure, conduct regular dissemination and training, and conduct regular monitoring and evaluation. Thorough internal oversight is essential to ensure compliance and the effectiveness of ISMS implementation. Learning and growth processes are also crucial through training, certification, security awareness, benchmarking, and seminars to update knowledge related to information system security and the latest technology. Management plays a crucial role in establishing formal policies, providing human resources, and overseeing and evaluating ISMS implementation. To address customer satisfaction, banks actively conduct data security education and outreach, provide complaint channels, and implement transparent data protection mechanisms. Management also manages the costs and benefits of ISMS implementation through risk-based investment, budget efficiency, appropriate technology utilization, and ongoing evaluation to ensure security investments deliver optimal results.

Discussion

The implementation of ISO 27001:2013 at Bank Sulselbar reflects an appropriate strategy for strengthening information security systems, enhancing risk management, and strengthening customer trust. Research conducted by Srivastava, Rizvi, and Priya (2023) shows that the implementation of ISO 27001 in the banking sector significantly improves information security risk governance and enhances response to cyber incidents. Furthermore, the implementation of this standard creates a more security-conscious work culture among employees, supporting a more structured internal control system.

Regarding corporate performance, Martí-Calatayud et al. (2022) revealed a positive relationship between ISO 27001 certification and improved financial performance, productivity efficiency, and corporate reputation. This study demonstrates that the benefits of ISO 27001 implementation extend beyond strengthening information security and have a broad impact on the overall operational and strategic aspects of a company.

Another study conducted in the energy sector by the SCIRP study team (2023) demonstrated the effectiveness of ISO 27001 in reducing the number of cyber incidents and mitigating their reputational impact. The study also confirmed that a systematic approach to information security management enables companies to respond to risks more quickly and measurably, making the standard an effective mitigation tool even in industries with high risk exposure.

Culot, Nassimbeni, Podrecca, and Sartor (2021) highlight the importance of ISO 27001 in meeting stakeholder expectations through a comprehensive ISMS framework. They state that implementing this standard can balance regulatory and business interests, particularly in the context of data protection and legal compliance.

These four studies strengthen the argument that Bank Sulselbar's implementation of ISO 27001 is on track to align with global best practices. As a pioneer among regional development banks, certified since 2020, Bank Sulselbar demonstrates a strong commitment to building a robust information security system. However, challenges remain, particularly in strengthening internal training, regular monitoring, and improving security literacy for all stakeholders.

Table 1 Conceptual Framework for the Implementation of the Bank Sulselbar Information Security Management System

No	Question	Balanced Scorecard Perspective	Keyword	Theoretical References
1	Is there an organizational structure that regulates the job description of the information security management system?	Internal Business Processes	Organizational Structure and Job Description	Organization Theory (Jay Galbraith)
2	Are all IT staff involved in the information security management system implementation process?	Internal Business Processes	Position and Responsibilities	Organizational Theory (Stephen P. Robbins)
3	Are there policies or standards for implementing an information security management system?	Learning and Growth	Internal Policy	Management Theory (Peter Drucker)
4	How can we ensure that governance runs according to the employees' duties and functions?	Learning and Growth	Training and Evaluation	COBIT, ITIL
5	Is there supervision of the ISMS process and implementation?	Internal Business Processes	Internal and External Supervision	COSO

6	How is the monitoring process for the implementation of the information security management system?	Internal Business Processes	Internal and External Supervision	COSO
7	How is the learning and growth process for implementing an information security management system?	Learning and Growth	Provision and Training	Balance Scorecard (Kaplan & Norton)
8	What is the role of management in the process of implementing an information security management system?	Financial	Commitment and Compliance	Organizational Commitment Theory (Meyer & Allen)
9	How do customers respond to the implementation of an information security management system?	Customer	Customer Reviews	Customer Satisfaction Theory (Kotler)
10	How does management strive to provide customer satisfaction?	Customer	Education and Socialization	Customer Satisfaction Theory (Kotler)
11	Are there any regulations/laws governing the implementation of information security management systems?	Internal Business Processes	Risk Management	COSO
12	How does management relate to the costs and benefits of implementing an information security management system?	Financial	Efficiency and Strategy	Teori Return on Investment (ROI)

Financial Services Authority (OJK) Perspective

The Financial Services Authority (OJK) plays a key role in regulating and overseeing information security in the financial services sector. Through regulations such as POJK No. 11/POJK.03/2022 and OJK Circular Letter No. 29/SEOJK.03/2022, the OJK establishes standards for customer data protection, IT system security, risk management, and the establishment of cyber resilience units in banks. The OJK's primary focus is ensuring customer data confidentiality, system security, including asset and threat identification, and preparedness for cyber incidents. This role provides a regulatory framework that serves as a foundation for banks like those in South Sulawesi and West Sulawesi to build and develop robust information security management systems.

Thus, Bank Sulselbar's implementation of ISO 27001:2013 has had a significant positive impact on information security, customer satisfaction, and overall bank performance. However, ongoing development in training, supervision, and customer understanding remains a key challenge that must be addressed to ensure the benefits of this information security system are optimal and sustainable.

CONCLUSION

Based on the results of the research that has been conducted, it can be concluded that the implementation of the ISO/IEC 27001:2013 standard at PT. Bank Sulselbar can be an effective way to improve information security in the organization. Therefore, organizations need to consider implementing this standard in improving information security. Another thing that can be seen directly from the implementation of ISO 27001 is the existence of a very significant positive change in terms of work culture where the existence of a structured process and standards that must be applied in the office environment will inevitably and slowly lead each employee to what is called awareness (*Awareness*) about the importance of information security.

Other positive impacts obtained from the implementation of information security standards include: Improving quality or service, increasing efficiency, reducing security risks, improving reputation, increasing trust and credibility of the organization in the eyes of customers/clients, partners and other stakeholders. The results of this study can be used as a reference for organizations that want to improve information security and reduce security risks whereCybercrime or cybercrime is an undeniable phenomenon, invisible but real and various cybercrime problems continue to increase every day.

REFERENCES

Antariksa, H., Nugroho, L., & Fadillah, R. (2017). *Manajemen Strategis dalam Organisasi*. Jakarta: Mitra Wacana Media

Budio, R., Saputra, A., & Widodo, T. (2019). *Strategi Bisnis dan Pengambilan Keputusan*. Yogyakarta: Graha Ilmu

Castells, M. (2004). *The network society: A cross-cultural perspective*. Edward Elgar Publishing

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). Thousand Oaks, CA: SAGE Publications

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda. *Information Systems Frontiers*

Jogiyanto, H. M. (1999). *Analisis dan desain sistem informasi: pendekatan terstruktur teori dan praktek aplikasi bisnis*. Andi Offset

Loudon, K. C., & Loudon, J. P. (2004). *Management information systems: Managing the digital firm* (9th ed.). Pearson Education

Lucas, H. C. (2000). *Information technology and the productivity paradox: Assessing the value of investing in IT*. Oxford University Press

Martí-Calatayud, M. C., et al. (2022). Research on the Impact of Information Security Certification and Concealment on Financial Performance. *Journal of Global Information Management*.

Miarso, Y. (2007). *Menyemai benih teknologi pendidikan*. Kencana Prenada Media Group

Nuryanto, E. (2012). *Teknologi informasi dan komunikasi dalam organisasi*. Graha Ilmu

Peraturan Jasa Keuangan (POJK) Nomor 11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum

Persari, D., Utomo, B., & Ramadhan, F. (2018). *Formulasi Strategi dan Keunggulan Bersaing*. Surabaya: Laksana Ilmu

Riyadi, S. (2019). *Manajemen Umum: Konsep dan Aplikasi*. Bandung: Alfabeta

SCIRP (2023). Study the Effectiveness of ISO 27001 to Mitigate the Cyber Security Threat. *SCIRP Journal*

Sidharta, I. (1995). *Sistem informasi manajemen*. Informatika Bandung

Srivastava, A., Rizvi, S., & Priya, K. (2023). *ISO 27001 in Banking: An Evaluation of Its Implementation and Effectiveness in Enhancing Information Security*. Finance & Accounting Research Journal, 5(12), 405–425. DOI: 10.51594/farj.v5i12.684

Sugiyono. (2017). *Metode Penelitian Kualitatif, Kuantitatif dan R&D*. Bandung: Alfabeta

Surat Edaran OJK Nomor 29/SEOJK.03/2022 Tentang Ketahanan dan Keamanan Siber Bagi Bank Umum.

Wike, R. (2021). *Digitalisasi Layanan Perbankan di Era Modern*. Jakarta: Prenada Media.