JPPIPA 11(10) (2025)

Jurnal Penelitian Pendidikan IPA

http://jppipa.unram.ac.id/index.php/jppipa/index

Bank Indonesia's It Audit Guidelines for Payment Service Providers in The SME Category: An Integrated ISO 27001:2022 Annex A, and Cloud-Based Solution Architecture Design

Suarjan[1*], Moh. A. Amin Soetomo[1], Heru Purnomo Ipung[1]

[1] Data Science Cyber Security - Master of Information Technology, Faculty of Engineering and Information Technology, Swiss German University, Indonesia.

Received: August 14, 2025
Revised: September 19, 2025
Accepted: October 25, 2025
Published: October 31, 2025

Corresponding Author:
Suarjan
arjan.20@gmail.com

DOI: 10.29303/jppipa.v11i10.12899

Abstract: Small and Medium Enterprises (SMEs) in Indonesia face significant challenges in complying with Bank Indonesia's (BI) stringent Payment Service Provider (PJPP) licensing requirements, including cybersecurity mandates (BI 23/6/PBI/2021). This study addresses these challenges by designing a cost-effective, cloud-based solution architecture aligned with ISO 27001:2022 Annex A, simplifying compliance for resource-constrained SMEs. This framework helps SMEs prepare for IT audits with guidelines aligned with Bank Indonesia requirements and the ISO 27001:2022 Annex A standard, and replaces complex enterprise architectures with lightweight, cloud-centric models that leverage Indonesian cloud providers while still meeting Bank Indonesia requirements. Validation through a pilot study with SMEs demonstrated lower compliance costs compared to traditional approaches, achieved through open source tools and hybrid cloud deployments. The combination of IT audit guidelines and solution architecture impacted the results of the IT audit, with only a few findings identified by the external auditor and PT XYZ passing the IT audit. This suggests that the conclusions drawn from the results and discussion indicate that this framework has a significant impact on PSPs, particularly at the SME level. The novelty of this research contributes to practical implementation guidelines for SMEs and the design of cloud-based solution architectures that meet Bank Indonesia requirements.

Keywords: Bank Indonesia regulations; ISO/IEC 27001: 2022 annex A controls; Payment Service Providers (PSPs); Small-Medium Enterprises (SMEs); Solution architecture design

Introduction

A recorded history of significant changes and significant patterns over time may be found by looking at the development and evolution of Indonesian SMEs. According to preliminary research, SMEs are crucial to Indonesia's economy, especially in terms of job generation and regional economic growth. Researchers started looking into how government policies and funding availability affected the expansion of SMEs after economic liberalization in the 1990s (Agote-Garrido et al., 2023). The focus shifted in the 2000s as researchers looked at the challenges SMEs face, particularly with regard to market rivalry and financial access. Even though SMEs' significance was becoming more widely recognized, many of them continued to face underlying issues that limited their long-term survival and growth. The impact of globalization and technology on SMEs has been the subject of more recent research, which suggests that innovation and adaptation are critical for survival

How to Cite:
Suarjan, Soetomo, M. A. A., & Ipung, H. P. (2025). Bank Indonesia's It Audit Guidelines for Payment Service Providers in The SME Category: An Integrated ISO 27001:2022 Annex A, and Cloud-Based Solution Architecture Design. *Jurnal Penelitian Pendidikan IPA*, *11*(10), 121–134. https://doi.org/10.29303/jppipa.v11i10.12899

in a market that is continuously changing. Technology integration has become a hot topic, showing a big shift in SMEs' ability to compete both domestically and internationally (Setyoso et al., 2024).

Payment Service Providers (PSPs) are pivotal to the global digital economy, facilitating seamless transactions between merchants, consumers, and financial institutions. The market for digital payments is expected to reach a total transaction value of US$20.09 trillion by 2025 due to the growth of e-commerce, mobile wallets, and cross-border payments. Leading global PSPs like PayPal, Stripe, and Adyen emphasize secure, scalable architectures and compliance with regional regulations such as the EU’s PSD2 (Payment Services Directive) and the PCI DSS (Payment Card Industry Data Security Standard). However, smaller players, particularly in emerging economies, struggle with balancing innovation, cybersecurity, and regulatory compliance, often lacking resources to implement frameworks like ISO 27001:2022 (Al-Okaily, 2021). With mobile phones becoming a widespread tool for financial transactions, the rise of mobile payments has been an important development in the fintech era. However, as demonstrated by the case studies of M-PESA in Kenya, TCASH in Indonesia, and Oi Paggo in Brazil, several mobile payment projects have encountered difficulties. These systems compete on the basis of common infrastructures and function within intricate networks, which are frequently controlled by international operators such as telecom companies (Darmawan et al., 2023).

Bank Indonesia, the central bank of Indonesia, plays a pivotal role in the country's financial and economic stability. Established in 1953, following Indonesia's independence, it became a key institution in constructing the nation’s monetary and economic framework. Bank Indonesia’s mandate has evolved over the years, but its primary responsibilities have remained consistent: achieving and maintaining the stability of the Indonesian rupiah. This includes managing inflation rates, ensuring a stable exchange rate, and monitoring the overall financial system's health. The institution serves as the guardian of Indonesia's monetary policy, deploying tools such as interest rates adjustments, open market operations, and the setting of reserve requirements to bolster economic stability. Through these mechanisms, Bank Indonesia not only supervises the financial system’s health but also facilitates sustainable economic growth. Moreover, Bank Indonesia has embraced significant transformation, especially in recent decades, to address the challenges brought by globalization and technological advancements (Antunes et al., 2022). This transformation is evident in the adoption of more sophisticated financial regulations and supervisory frameworks aimed at preserving both national financial stability and protecting consumers. Additionally, with the rise of digital banking and fintech innovations, Bank Indonesia has expanded its focus on developing regulatory guidelines and improving cybersecurity measures to mitigate the heightened risks associated with digital finance. The adoption of these progressive strategies underscores Bank Indonesia’s commitment to remain resilient and responsive to the ever-evolving financial landscape, ensuring that it continues to perform its role effectively as a cornerstone of Indonesia's financial system (Aravik et al., 2025).

Bank Indonesia offers a wide array of services aimed at maintaining financial stability and supporting the economic infrastructure of the country. Among its critical services, the central bank oversees payment systems and ensures their efficiency and security as part of its broader mission to provide a stable and robust financial environment. One significant aspect of these services is the regulation and oversight of Penyedia Jasa Pembayaran (PSP), or Payment Service Providers. PSPs play an essential role in the daily financial transactions across Indonesia, facilitating everything from individual remittances to large-scale corporate payments. With the rapid rise of digital transactions and mobile banking, Bank Indonesia has been instrumental in developing regulatory frameworks that support innovation while ensuring security and efficiency within the payment system. This involves licensing PSPs and enforcing compliance with regulatory standards to safeguard consumer interests and maintain trust in the financial system. By promoting a secure and efficient payment infrastructure, Bank Indonesia enhances financial inclusion and supports the nation's economic growth, ensuring that even the most remote areas can access modern financial services (Angganegara et al., 2025).

Technology breakthroughs and legislative developments have had a major impact on the evolution of payment service providers (PSPs) in Indonesia. Early on, the sector was mostly defined by conventional banking practices, which provided few choices for online transactions. According to research, this started to change around 2010, when the financial industry started to become more competitive due to the emergence of alternative payment methods sparked by mobile banking. According to multiple studies, by 2015, advancements in mobile payment applications further sped up the adoption of PSPs, driven by rising smartphone penetration and the expanding middle class (Setyoso et al., 2024).

Regulatory frameworks changed together with the market to accommodate the quickly shifting environment. The Indonesian government strengthened public confidence in digital payment systems by enacting rules in 2016 to improve their security and usability. Innovative fintech businesses were able to thrive because to this regulatory backing, which also significantly increased the number of local startups joining the PSP industry. According to recent estimates, by 2020, a wide range of payment solutions—from peer-to-peer transfers to e-wallets—had developed to meet the needs of different consumer segments, indicating the market's dynamic nature (Indonesia, 1953).

Becoming a Penyedia Jasa Pembayaran (PSP), or Payment Service Provider, in Indonesia involves meeting a set of stringent criteria set by Bank Indonesia, aimed at ensuring the integrity and security of the country's payment systems. Bank Indonesia has several regulations for Payment Service Providers, namely PBI No. 23/6/PBI/2021. Then an explanation of the technology security system framework is included in the Payment Service Provider Licensing Document Requirements (PSP) document for institutions other than Banks. One of the pivotal requirements is providing detailed IT Audit reports from external, independent auditors. These reports are crucial as they offer an unbiased assessment of the PSP's information technology systems, focusing on aspects such as security, data integrity, and system reliability. The IT Audit helps ascertain that the PSP's technological infrastructure is robust enough to handle transactions securely and efficiently, minimizing risks such as data breaches or system failures. This audit is an integral part of both the initial licensing process and the ongoing annual reporting requirements mandated by Bank Indonesia. The external IT audit provides an independent assessment of a company's technological infrastructure, focusing on key areas such as cybersecurity, system integrity, and compliance with regulatory standards (Indonesia, 2021b). These audits are essential because they help ensure that PSPs maintain a high level of operational security and efficiency, critical for safeguarding consumer transactions and data. Moreover, the annual submission of these IT audit reports to Bank Indonesia serves as a continual validation that the PSPs adhere to the evolving regulatory requirements and can effectively manage new and existing risks in the fast-paced digital financial environment. By leveraging these external IT audits, Bank Indonesia can more effectively oversee the stability and security of the nation's payment systems, fostering a trustworthy and reliable financial ecosystem for businesses and consumers alike (Indonesia, 2022).

ISO/IEC 27001:2022 certification represents a global standard for information security management systems (ISMS) and stands as one of the optional yet highly advantageous credentials for a Payment Service Provider (PSP) seeking registration in Indonesia. This certification demonstrates a company's commitment to systematically managing sensitive information, ensuring the confidentiality, integrity, and availability of data. For PSPs, aiming to strengthen their market position and build trust with consumers and regulatory bodies alike, obtaining ISO/IEC 27001:2022 offers a structured framework for implementing robust security controls that align with international best practices. While not mandatory, the certification can significantly enhance a PSP's credentials by showing that it has undergone rigorous audits and assessments by certified bodies. This external validation underscores the PSP's dedication to proactively managing and mitigating information security risks, which is critical in today's digital landscape where cyber threats are continually evolving. Ultimately, having ISO/IEC 27001 certification not only aids in regulatory compliance but also elevates the institution's reassurance to stakeholders that critical financial data is handled with the utmost care and security (Indonesia, 2021a).

The progression of ISO 27001:2022, especially concerning Payment Service Providers (PSPs), shows how security standards have gotten better to fit the digital financial world. Early on, conversations about ISO 27001 mainly focused on the basic ways to manage information security systems (ISMS), stressing the need for well-organized systems to safeguard important data in various fields, including finance as the digital economy grew, the rise of online payment systems made it necessary to have a more detailed understanding of security measures that could handle the particular weaknesses PSPs faced. Later writings pointed out how ISO 27001 changed to meet these new dangers, adding stricter rules that directly matched the complex details of digital payment processes.

The 2022 update is a key point in this development. It not only strengthened basic security steps but also gave specific advice for handling risks from the cyber threats PSPs face. Studies suggest that the updated standards encourage a more forward-thinking approach, pushing organizations to use constant monitoring and improvement methods, which are crucial in a field that changes quickly with technology.

The progress of system analysis and design in solution architecture has seen major turning points, showing how things have changed and technology has gotten better. Initial structures, as pointed out by, established the basics for understanding the key parts and ways to do effective system design. These early ideas stressed how important user needs and getting people involved in the design process were, things that became more and more important later on. As technology developed, so did the ways of doing things. For example, mentions how Agile methods came about in the early 2000s and caused a big shift, making solution architecture more iterative and collaborative. This evolution suggests a response to the growing difficulty of system needs and what users want (Barati & Rana, 2022).

To obtain a PSP license from Bank Indonesia, the PSP must meet Bank Indonesia's requirements, both administrative and technical. One obstacle to meeting these requirements, particularly for SMEs, is the capability system, which will be audited by an external institution. These SMEs lack a clear understanding of what they must prepare and fulfill, given limited resources, competencies, and implementation guidelines. Therefore, this thesis was created to assist PSPs in the SME category in facing IT audit preparations from external institutions for reporting to Bank Indonesia so that the implementation carried out is in accordance with PSP requirements from Bank Indonesia, thereby minimizing major findings that could disrupt the licensing process or annual reporting (Daousis et al., 2024).

Method

This chapter explains the study framework, which includes comparison of standards and frameworks, gap analysis, creation of IT audit guidelines, designing solution architecture, monitoring implementation, and validating with feedback and validation from experts (Budisantoso & Sumarwan, 2022).

Research Framework

This research will be conducted by mapping each aspect within the Bank Indonesia IT audit framework into the ISO/IEC 27001:2022 Annex Control and solution architecture design using System Analysis and Design (SAD) according to the identification of each aspect and designing technology architecture based on cloud, as illustrated in Figure 1.

This research will be conducted by mapping each aspect within the Bank Indonesia IT audit framework into the ISO/IEC 27001:2022 Annex Control and solution architecture design using System Analysis and Design (SAD) according to the identification of each aspect and designing technology architecture based on cloud (Digital Payments - Worldwide | Statista Market Forecast, 2025).

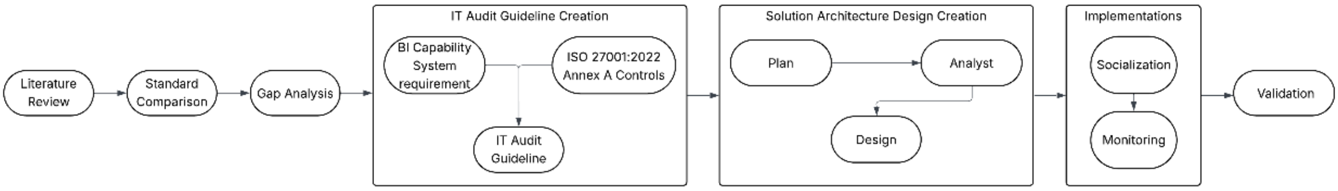

Figure 1. Research framework

Literature Review

Literature review offers a thorough grasp of current frameworks, standards, and best practices pertaining to cloud computing, governance, information security, and regulatory compliance, particularly as they relate to SMEs and payment service providers. In order to ensure that the suggested solutions are based on tried-and-true theories and up-to-date best practices, the researcher finds pertinent concepts, technologies, and gaps by methodically reviewing academic publications, industry reports, and legislation (Gheorghe, 2010).

Standard Comparison

The initial research was conducted by comparing several standards commonly used by payment service providers, to determine which standards could clearly assist clients in preparing for external IT audits while also complying with regulations. Some of the standards compared are ISO 27001:2022, COBIT, ITIL and PCI DSS. For the solution architecture, the framework compared are System Analysis & Design (SAD) and TOGAF (Hadjarati et al., 2025).

Gap Analysis

For the gap analysis, we conduct interviews with PT XYZ IT Manager combine with gap analysis checklist from ISO 27001:2022 Annex A Controls in exploring the organization's current implementation. These discussions also examined the organization's current state, specifically related to Bank Indonesia and ISO 27001:2022 requirements. The purpose of this analysis was to identify differences between the existing implementation process and the desired state of the company's objectives to meet Bank Indonesia requirements. In doing so, we aimed to uncover gaps and opportunities for improvement, ensuring that the organization's implementation practices align with Bank Indonesia regulations (Ajayi & Udeh, 2024).

IT Audit Guideline Creation

Each point in the IT Audit framework contained in the Payment Service Provider regulation at Bank Indonesia will be mapped into ISO 27001:2022 Annex A Controls as shown at Table 1. A total of 60 of the total 93 Annex A Controls will be used as guidelines.

Solution Architecture Design Creation

To create a cloud-based solution architecture design, we first sampled the infrastructure architecture from PT XYZ which is SME in PSP category 3, including their technology stacks. We then used a systematic method for creating and enhancing systems that incorporates both technical and management elements is called system analysis and design, or SAD. It entails evaluating current systems, pinpointing areas in need of development, and creating new or improved systems to achieve predetermined goals to comply with Bank Indonesia capability system requirement. SAD is essentially the process of determining what a system must perform (analysis) and then how it will accomplish it (design). The SAD framework can be seen in Figure 2.

Planning
Analysis
Design
Implementation

Figure 2. SAD framework

Determining the project's boundaries and assessing its viability are the main goals of the planning phase. It starts with determining the main issue that the system is meant to address and evaluating the viability of a solution from a technological, financial, and operational standpoint.

Understanding what the system needs to do becomes the main focus throughout the analysis phase. Users, stakeholders, and current procedures are consulted to obtain specific requirements. This stage produces a thorough needs definition by identifying opportunities, limitations, and gaps. Before design starts, it guarantees that all parties involved are in agreement about the system's goal (Hossain et al., 2024).

Requirements are converted into a technical blueprint for the system's construction during the design phase.Physical design includes infrastructure, security protocols, interfaces, and performance criteria in addition to choosing specific technologies (such as databases and cloud services). Before development begins, this stage makes that the solution is effective, scalable, and maintainable (Hidayatullah et al., 2023).

Through construction, testing, deployment, and end-user transfer, the implementation phase turns the proposed system into a working reality. In this phase, the implementation phase is in PT XYZ side, the author only monitoring the implementations and receive feedback from them.

Implementation

Implementation was carried out at PT XYZ which is included in the SME in PSP category 3. After they agree, conduct a socialization on the use of the IT audit guidelines. Monitor the implementation carried out by the company. And finally ensure that all controls have been carried out by the company. Afterward, PT XYZ will conduct an IT audit with a third party registered with ASPI, under the auspices of Bank Indonesia. The audit report will determine whether the implemented framework successfully assists PT XYZ in facing the IT audit. If an external auditor concludes that the company has sufficient system capabilities in compliance with Bank Indonesia's standards, the framework's success criterion is met. By fulfilling this requirement, businesses can make sure that audit reports can be sent to Bank Indonesia with any non-conformities already fixed (Hasibovic & Tanovic, 2024).

Results and Discussion

Standard Comparison

Several standards and frameworks are used as a comparison to determine which one will be used for the IT audit guideline. The standards to be compared are ISO 27001:2022, COBIT, ITIL 4 and PCI DSS. To determine the most important category in determining standards in a service is when it is required by regulation to be MT (Fauzi & Suryani, 2019). The following comparison is explained in Table 1.

Table 1. Standard and framework comparison

Criteria	ISO 27001:2022	COBIT 2019	ITIL 4	PCI DSS v4.0
Primary Focus	Information Security Management System (ISMS)	IT Governance & Risk Control	IT Service Management	Payment Card Data Security
Regulation Alignment	Mention on Peraturan Bank Indonesia No. 23/6/PBI/2021; Mention on Peraturan Badan Siber dan Sandi Negara No. 8 Tahun 2020	No mention on regulation	No mention on regulation	Mention on Peraturan Bank Indonesia No. 23/6/PBI/2021 regulation
Certification	Globally recognized certification	No formal certification	Individual certifications	Merchant/processor validation
Bank Indonesia Alignment	Align	Not Align	Not Align	Not Align to PSP category 3

Based on the comparison above with the category that is the main reference is related to regulations and Bank Indonesia alignment, therefore the ISO 27001:2022 standard was chosen in this thesis so that the implementation carried out by SMEs in PSP category 3 is in line with regulations from Bank Indonesia and BSSN. For cloud-based solutions architecture, several frameworks will be compared, such as System Analysis & Design (SAD), and TOGAF. Several categories will be used for the comparison, as shown in Table 2.

Table 2. Framework comparison

Criteria	SAD	TOGAF
Core Purpose	Design deployable systems	Enterprise transformation (business-IT alignment)
Scope	Solution-focused (single system/application)	Enterprise-wide
Complexity	Low-moderate (practical for SMEs).	High (organization-wide).
SME Suitability	Agile, outcome-focused	Overkill

Based on the comparison of the frameworks above, SAD was chosen because it has a low level of complexity and can focus on solutions that lead to a single system or application only.

Gap Analysis

The author interviewed the PT XYZ IT Manager to learn more about the company's present implementation in order to perform the gap analysis. The organization's current status was also discussed, with particular attention on Bank Indonesia and ISO 27001:2022 criteria. Also, the author used gap analysis checklist for ISO 27001:2022. Finding discrepancies between the company's goals and the current execution process in order to satisfy Bank Indonesia's standards was the aim of this investigation. In order to make sure that the organization's implementation procedures comply with Bank Indonesia rules, we set out to identify any gaps and areas that may use improvement.

Based on the results of the gap analysis, a gap was found within PT XYZ as seen in Table 3 which is their main concern in facing IT audit preparations from external institutions (Roghanian et al., 2012).

Table 3. Gap analysis results

ISO 27001:2022 Annex A	Current State	Desired State	Gap Identified
A.5.31 Legal, statutory, regulatory and contractual requirements	No specific compliance guideline to face Bank Indonesia IT audit from external party.	Ensure that the systems, infrastructure and supporting documents required for IT audits comply with Bank Indonesia requirements.	Inadequate guidelines for fulfilling Bank Indonesia requirements.

The lack of clear guidelines for implementing system capabilities required by Bank Indonesia is a major concern for PT XYZ in facing IT audits. Therefore, they need clear guidelines regarding these requirements to avoid poor audit results and failure to proceed to the licensing stage for Bank Indonesia (Greuning & Bratanovic, 2020).

IT Audit Guideline Creation

To create the IT Audit Guidelines for Payment Service Providers in the SME category, we mapped the Payment Service Provider capability system requirements by Bank Indonesia against the system capability framework of ISO 27001:2022 Annex A Controls to determine the appropriate controls for each aspect. Each aspect will provide guidance on what the company, especially SME needs, both technically and non-technically (Rahi et al., 2020).

Data Confidentiality

The purpose of data confidentiality is to ensure that sensitive or private information is protected from unauthorized access, disclosure, or exposure. Confidentiality ensures that data is accessible only to authorized individuals or systems and remains private from anyone who is not explicitly permitted to view or handle it. Several guidelines can be seen on Table 4.

Inventory of information and other associated assets: It is necessary to create and keep an inventory of the data and other related resources, including the owners: Policy and procedures related to inventory of information and other associated assets as documented information. Conduct a data collection of primary assets and supporting assets (Laptop, PC, Mobile Phone, Router, etc.). Conduct asset reviews and updates regularly (every three months, every six months, etc.)

Return of assets: When their employment, contract, or agreement changes or is terminated, employees and other interested parties should return any assets owned by the organization (Harmening, 2018). Policy and procedures related to inventory of information and other associated assets as documented information. All company-loan assets must be returned by departing or resigning employees.

Classification of information: Information should be categorized in accordance with the organization's information security requirements, taking into account requirements for confidentiality, availability, integrity, and pertinent interested parties. Policy and procedures related to information classifications as documented information. Information can be classified based on legal requirements, value, criticality and sensitivity to unauthorized exposure or modification. For example, Confidential, Internal and Public.

Labelling of information: The organization's chosen information classification strategy should guide the development and application of a suitable set of information labeling methods. Policy and procedures related to information labelling as documented information. Labeling method that can be used is attaching information to assets with content such as information classification, asset ID numbers, owner name, division name, acquisition date, etc.

Examples of labelling techniques include: physical labels, headers and footers, metadata, watermarking, rubber-stamps.

Access controls: Based on business and information security needs, rules should be developed and put into place to regulate logical and physical access to data and other related assets. Policy and procedures related to access controls as documented information. Role determination can be done, by providing different roles with different activities for each account registered in a system (Example: Admin, Supervisor, User, etc.). Identifying the organizations that need access to the data and any related resources.

Access rights: The organization's topic-specific policy and access control guidelines should be followed when allocating, reviewing, modifying, and removing access rights to information and other related assets. Policy and procedures related to access rights as documented information. Making changes to access rights for employees who resign, migrate or terminate their contracts. When an employee resigns or terminated, an exit clearance process is required, including the removal of access rights to company systems. Coordination is usually carried out between the IT and HR teams. Conduct user access reviews periodically at specified intervals (once a year, once every two years, etc.)

System and Data Integrity

Integrity in information security relates to the correctness, consistency, and reliability of data, making sure it hasn't been illegally changed or destroyed. It's about ensuring that data is accurate and comprehensive during transmission and storage. Guidelines for integrity aspects can be seen in (Gheorghe, 2010).

Protection against malware: Adequate user awareness should be used to support and implement malware protection. Policy and procedures related to protection against malware as documented information. Install and update malware detection/antivirus and repair software on a regular basis. Scan computers and electronic storage devices on a regular basis.

Management of technical vulnerabilities: It is important to gather information on the technological weaknesses of the information systems that are being used, assess the organization's vulnerability to these weaknesses, and take the necessary precautions. Policy and procedures related to management of technical vulnerabilities as documented information. Perform vulnerability assessment and/or penetration testing (VAPT) to application, infrastructure, etc. on a regular basis (Ex. minimum once a year) by internal or using third party.

Configuration management: Hardware, software, services, and network configurations—including security configurations—should be planned, recorded, put into use, tracked, and evaluated. Policy and procedures related to configuration management as documented information. Manual configurations carried out by the IT team need to be recorded in detail in documentation (network devices, servers, user devices, etc. (Logie & Maroun, 2021) be guidelines (such as pre-made templates from independent security organizations and vendors).

System and Data Two-Factor Authentication

Two-factor authentication (2FA) is implemented to ensure an additional layer of security in the authentication process. 2FA can also serve as an alert to users that their primary authentication credentials have been compromised (Naji, 2020). The guidelines of 2FA can be seen in Table 6.

Authentication information: A management procedure should oversee the distribution and administration of authentication data, including informing staff members about how to handle it properly. Policy and procedures related to authentication information as documented information. Personal identifying numbers (PINs), which are produced automatically during enrollment processes as temporary secret authentication information, are unique to each individual and cannot be guessed. Users must change them after their first usage. Determine the criteria for creating a password, such as the minimum password length and the combination used (uppercase letters, lowercase letters, numbers and special characters).

Secure authentication: Information access limitations and the topic-specific access control policy should serve as the foundation for the implementation of secure authentication methods and processes. Policy and procedures related to secure authentication as documented information. Authentication information requires the addition of additional authentication factors such as multi-factor authentication (MFA) or two-way authentication (2FA) to applications developed or used internally.

System Availability

The availability aspect focuses on ensuring that information is always available when needed. Some guidelines for this aspect can be seen in Damanik et al. (2021).

Security of assets off-premises: Off-site assets need to be safeguarded. Policy and procedures related to security of assets off-premises as documented information. Any device used to store or process data outside of the organization's physical location (such as a mobile device), including both privately owned and organization-owned devices utilized on the organization's behalf (bring your own device, or BYOD) requires defense. Not leaving removed equipment and storage media in unattended, public, or unprotected areas. Preventing the dangers of shoulder surfing and using a gadget (such as a laptop or cell phone) to browse information while on public transit.

Storage media: Storage media should be handled in compliance with the organization's handling guidelines and categorization system throughout its life cycle of purchase, usage, transportation, and destruction. Policy and procedures related to storage media as documented information. Following the manufacturer's instructions for keeping all storage media in a safe, secure environment in compliance with its information categorization and safeguarding them from environmental hazards (such as heat, moisture, humidity, electronic fields, or aging). Information on removable storage media can be protected using cryptographic approaches if information integrity or secrecy are crucial factors (Pimentel et al., 2023).

Cabling security: Power, data, and auxiliary information service cables should be shielded from damage, interference, and interception. Policy and procedures related to cabling security as documented information. Separate the power and communication cables, differentiate their paths and try to ensure that the two cables do not touch each other. Labeling cables with enough source and destination information at each end to allow for physical identification and inspection.

Equipment maintenance: To guarantee information availability, integrity, and secrecy, equipment needs to be properly maintained. Policy and procedures related to equipment maintenance as documented information. Keeping equipment maintained in compliance with the specifications and suggested servicing frequency provided by the supplier. Equipment repairs and maintenance are only performed by authorized maintenance professionals.

Secure disposal or re-use of equipment: Before being disposed of or used again, equipment that contains storage media should be checked to make sure that any licensed software and sensitive data have been safely overwritten or deleted. Policy and procedures related to secure disposal or re-use of equipment as documented information. Instead of utilizing the usual delete function, storage media containing private or copyrighted material should be physically destroyed, or the information should be erased, overwritten, or destroyed using methods that render the original data unretrievable. Re-check the equipment that will be destroyed or reused and ensure that there is no confidential data there.

Table 5. System availability

BI Aspect	ISO 27001:2022 Annex A
System Availability	A.7.9 Security of assets off-premises A.7.10 Storage media A.7.12 Cabling security A.7.13 Equipment maintenance A.7.14 Secure disposal or re-use of equipment A.8.6 Capacity management A.8.13 Information backup A.8.14 Redundancy of information processing facilities A.8.31 Separation of development, test and production environments

The Existence of Systems and Procedures for Conducting Audit Trails

Both system and application processes as well as user activity on systems and applications are tracked by audit trails. Audit trails can help identify security breaches, performance issues, and application defects when used in conjunction with the proper tools and processes. Several guidelines can be seen in Table.

Logging: It is necessary to create, store, safeguard, and analyze logs that document actions, exceptions, errors, and other pertinent occurrences (Octaviani & Ekasari, 2021). Policy and procedures related to logging as documented information. An event log must be included in each event (user IDs, system activity, date, time, details, etc.).

When logging, the following events should be taken into account: successful and unsuccessful attempts to gain access to the system, successful and unsuccessful attempts to gain access to data and other resources. modifications to the system configuration, privilege usage, utility program and application use, files accessed and the type of access, including the deletion of crucial data files, alerts generated by the access control system., activation and deactivation of security systems, such as intrusion detection and antivirus software, identity creation, modification, or deletion, user transactions in applications. In certain instances, the applications are third-party services or products.

The Existence of Internal Policies and Procedures for the Operation of Information Systems and Human Resources

This aspect serves to ensure that the company's policies and procedures are documented, including the availability of human resources. Several guidelines that can be implemented from this aspect.

Policies for information security: A management-approved information security policy and topic-specific policies should be created, publicized, acknowledged by the appropriate staff and interested parties, and reviewed on a regular basis and whenever there are major changes. Create an information security policy document including the required procedures based on the implemented Annex A Controls. Security policy should contain statements concerning: an explanation of information security, guidelines for all information security-related operations.

Segregation of duties: To lower the possibility of fraud, mistakes, and information security control circumvention. Policy and procedures related to segregation of duties as documented information. Each person in the company has different duties to avoid conflicts of interest: proposing, approving, and carrying out a change, asking for, approving, and implementing access rights, creating, planning, and evaluating code, creating software and managing production systems., utilizing and managing applications, utilizing applications and managing databases, creating, auditing, and guaranteeing.

The Fulfilment of Aspects of Security and Reliability of the System and/or Network Including Networks Provided by Other Parties

In this aspect, relationships with third parties need to be monitored and evaluated so that the services used are in accordance with the agreed service level agreement (SLA). Guidelines for this aspect can be seen in Table (Kusmayasari et al., 2023).

Monitoring, review and change management of supplier services: Changes in supplier information security procedures and service delivery should be routinely observed, reviewed, assessed, and managed by the company. Policy and procedures related to monitoring, review and change management of supplier services as documented information. The company is obliged to evaluate the performance results of third parties as a reference for continuing or terminating the cooperation contract.

Information security for use of cloud services: Procedures for purchasing, utilizing, managing, and terminating cloud services ought to be set up in compliance with the information security needs of the company. Policy and procedures related to information security for use of cloud services as documented information. The IT team must determine tasks and duties pertaining to cloud service management and use. Define its methodology for tracking, analyzing, and assessing continuous cloud service use to control information security threats.

Table 5. The fulfilment of aspects of security and reliability of the system and/or network including networks provided by other parties

BI Aspect	ISO 27001:2022 Annex A
The Fulfillment of Aspects of Security and Reliability of The System and/or Network Including Networks Provided by Other Parties	A.5.22 Monitoring, review and change management of supplier services; A.5.23 Information security for use of cloud services

The existence of a Business Continuity Plan (BCP) that can guarantee the continuity of the implementation of fund management activities. The BCP includes preventive measures and disaster recovery plans in the event of an emergency or disruption that results in the main system for implementing fund management activities being unusable.

This aspect is implemented to ensure that business operations can continue in the event of a disaster in one of the environments, the guidelines for which can be seen in the Table. With a BCP, business operations can continue in a backup/other environment.

Information security incident management planning and preparation: By defining, developing, and disseminating information security incident management procedures, roles, and duties, the company may plan and get ready to handle information security incidents. Policy and procedures related to information security incident management planning and preparation as documented information. Putting in place an incident management procedure to give the company the ability to handle the administration, documentation, detection, triage, prioritizing, analysis, communication, and coordination of interested parties involved in information security incidents. Putting in place an incident response procedure that enable the company to evaluate, address, and gain knowledge from information security occurrences.

Solution Architecture Design Creation

To create a cloud-based solution architecture design, we first sampled the infrastructure architecture from PT XYZ which is SME in PSP category 3, including their technology stacks. We then used a systematic method for creating and enhancing systems that incorporates both technical and management elements is called system analysis and design, or SAD. It entails evaluating current systems, pinpointing areas in need of development, and creating new or improved systems to achieve predetermined goals to comply with Bank

Indonesia capability system requirement. SAD is essentially the process of determining what a system must perform (analysis) and then how it will accomplish it (design) (Rijal & Bakri, 2023).

Planning

The planning phase is the essential step in figuring out why an information system should be constructed and how the project team will approach its development. The purpose of this planning phase is to determine whether the project is feasible and worth continuing (Hubais et al., 2023).

The plan is to improve the current cloud infrastructure design to meet Bank Indonesia's requirements (Francis, 2023).

Analysis

Analyzing the current cloud infrastructure and its constituent parts is the next stage. Finding existing systems, identifying areas for improvement, and creating concepts for new systems are the objectives of this investigation. The following Figure 3 shows a diagram of the existing cloud infrastructure at PT XYZ.

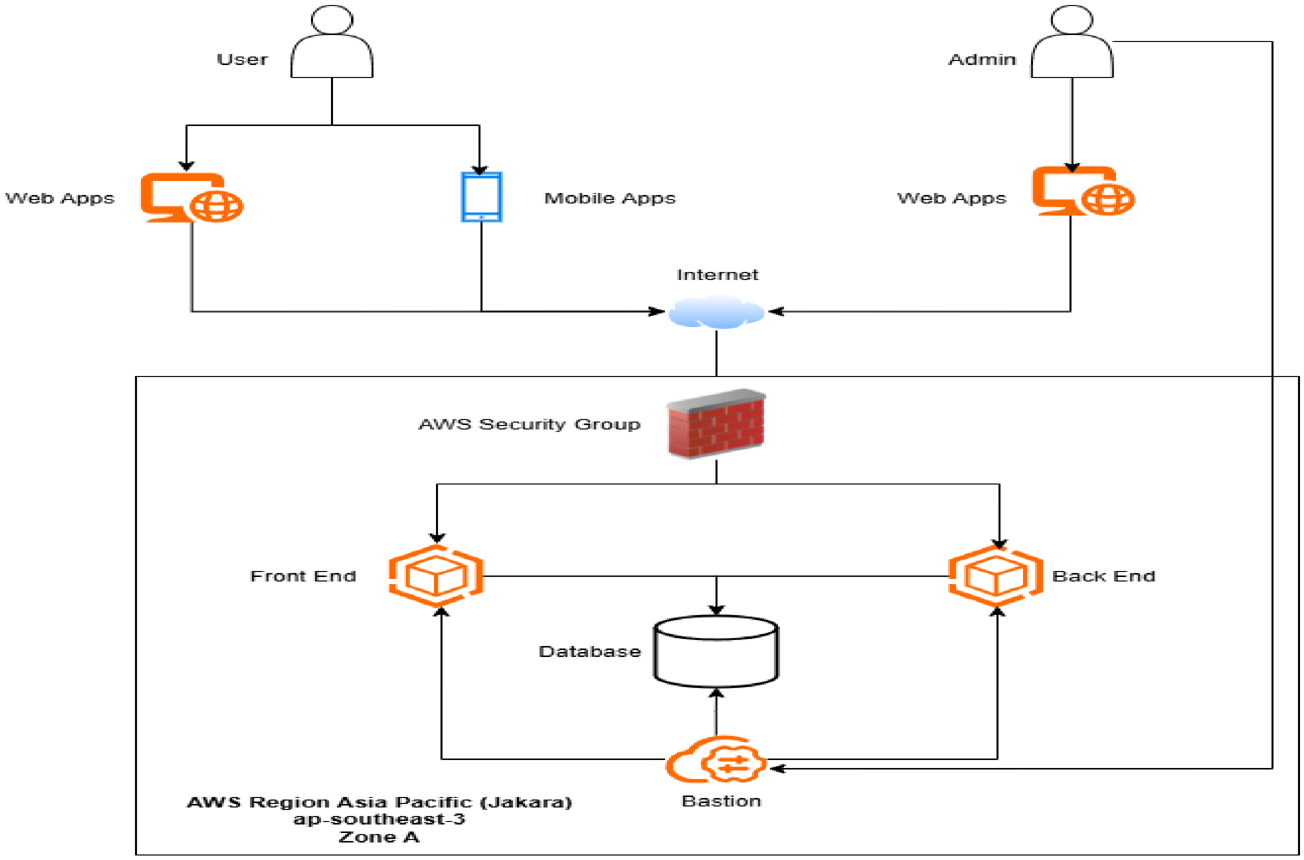

Figure 3. PT XYZ cloud infrastructure diagram

From the infrastructure diagram above, analyze the cloud components used which can be seen in Table 5. The results of the component analysis above revealed gaps in Bank Indonesia's requirements, namely having a disaster recovery center/secondary zone as part of the Business Continuity Plan and implementing redundancy to maintain high system availability. Furthermore, business continuity will be implemented in the cloud infrastructure by planning to deploy systems in more than one zone and high availability will be ensured by implementing redundancy across multiple zones.

Design

The next phase is to improvise the existing infrastructure design by adding gaps that were previously identified in the analysis phase can be seen at and the new design adapted to the improvements needed can be seen in Figure 4.

In the Figure 4, it can be seen that the architectural design of PT XYZ has implemented a disaster recovery center using Zone B in the same region and redundancy in each Zone to ensure business continuity and maintain high system availability when an incident occurs in one of the Zones.

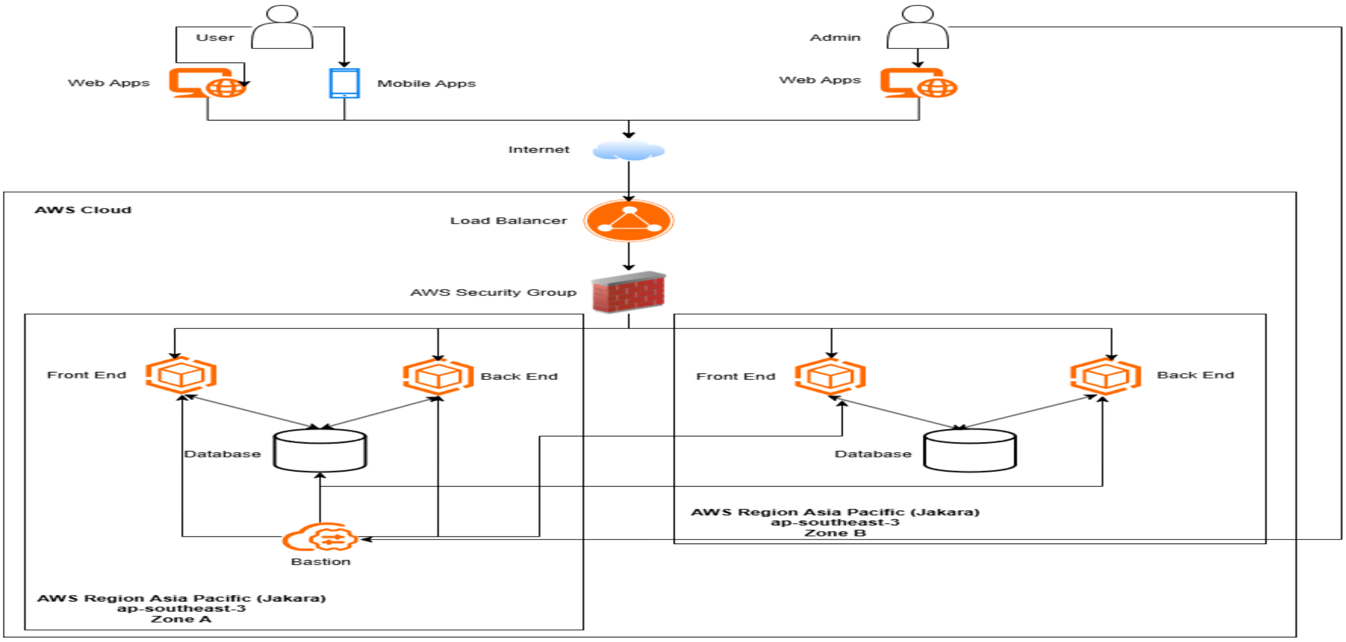

Figure 4. PT XYZ improvement design

Implementation

In this phase, implementation is carried out by PT XYZ, the author only conducting socialization and give solution architecture design.

Socialization

The author first conducted socialization to the PT XYZ regarding the IT guidelines. The outreach is carried out so that the internal team can understand the points contained in the IT guidelines and why they need to be implemented. In addition, this outreach session also serves as a form of question and answer forum if there are still unclear points related to the IT guidelines (Ton, 2023). For documented policies and procedures, several are already in place by PT XYZ. It is hoped that with this IT guideline, PT XYZ, can prepare the points required by the system capability requirements of Bank Indonesia and successfully face IT audits from external parties. For cloud-based architectural designs, outreach is also conducted, particularly for IT teams, to enable them to implement them within their cloud service providers. This also ensures smooth implementation and stable system operation without interruption.

Monitoring

The authors then monitored the implementation of the guidelines and the new infrastructure design to ensure proper implementation. Discussions continued throughout this monitoring period.

Once everything is ready, PT XYZ conduct an IT audit with an external party within the specified timeframe. After the audit, PT XYZ found several inconsistencies, but they were not significant and have been corrected by PT XYZ and verified by the auditor, as seen in Figure 4.3. The final result of the IT audit report was stated by the auditor, that the system implemented by PT XYZ is appropriate and in accordance with Bank Indonesia's requirements, as seen in the Figure 4.4. With this, PT XYZ has passed the IT audit and will then submit the IT audit report to Bank Indonesia along with other required documents (Sulaiman, 2023).

Validation

The main objective in conducting the validation process is to confirm that this framework provides IT audit guidelines that are sufficiently detailed and comprehensive, equipped with a solution architecture that is sufficient for SMEs while still meeting the requirements of Bank Indonesia.

Participants Selected for the Validation

Three experts were asked to interview and assess the framework as part of this validation. Their knowledge and expertise can be used to evaluate the framework's advantages and disadvantages, point out areas that need development, and provide suggestions for future framework optimization.

Riki Andi Nugraha. Role: Senior Auditor at TUV Rheinland Indonesia Relevant Criteria: Riki is a senior auditor with a wealth of experience in information security management systems and IT audits, especially in the fintech sector. He has conducted IT audits for Bank Indonesia and holds several certifications, including Lead Auditor ISO 27001. Riki has the expertise and understanding required to validate this thesis because of his background and skill set.

Sri Hardianti Abdullah. Role: Director and Senior Auditor at PT Mega Global Solusindo. Relevant Criteria: Anti is a director and auditor with a long background working in the internal audit division of a well-known category 1 PSP fintech company in Indonesia. He resigned from that position and founded PT Mega Global Solusindo where his company focuses on IT audit services for the needs of Bank Indonesia (BI) and the Financial Services Authority (OJK), vulnerability assessment and penetration testing (VAPT) and ISO 27001 assistance consultants. With a wealth of experience, especially in handling IT audits for Bank Indonesia, it is hoped that the validation carried out will provide much enlightenment and improvement as expected by the author.

Aditya Rangga Putra. Role: Solution Architect at PT Data Sinergitama Jaya Tbk (Elitery). Relevant Criteria: Adit currently works as a solution architect for a large IT managed services provider and system integrator. He has a background as a cloud engineer and architect before reaching his current position. With his competence and experience, he is expected to provide broad and comprehensive feedback and insight into this thesis.

Questions

In conducting validation, the author has created several sets of questions that will be asked to participants which can be seen in the Table 6.

Table 6. Questions

Topic	Question
Assessment and compliance	What do you think about this framework in relation to BI regulation?
	Can it comply with BI regulation?
	Can this framework help SME success pass the IT audit from external parties?
Difficulties and solutions	What are the challenges of this framework?
	How can we mitigate this?
Insights derived from experience	Based on your experiences, what aspects should SME focus on to comply with BI regulation?
Optimization	What steps we can take to optimize this framework in the future?
Relevance with the industry	What modifications are required to bring this framework into compliance with the industry's present demands?

Only the most important questions are included in this list. Further follow-up questions may be asked during the actual interview if necessary to elucidate answers and obtain more in-depth understanding (Tumwebaze et al., 2022). Based on validation from the participants, mapping the capability requirements of Bank Indonesia's system to ISO 27001:2022 Annex A Control provides guidance in implementation, which helps SMEs in PSP category 3. It can provide a great opportunity for SMEs to pass IT audits from external parties with satisfactory results and can be provided to Bank Indonesia (Panjaitan et al., 2023).

Conclusion

Based on the experimental results, several conclusions can be drawn: Mapping controls from Bank Indonesia's system capability framework for payment services to ISO 27001:2022 Annex A controls make it easier for PSPs to implement all required aspects as determined by Bank Indonesia. This IT Audit Guideline provides a clear overview of each required aspect, a situation that previously faced a lack of detailed understanding among PSPs in the SME sector. The selection of ISO 27001:2022 Annex A Controls and solution architecture tailored for SMEs makes it easier for them to implement them without requiring high effort and costs while still meeting Bank Indonesia's requirements. The combination of IT audit guideline and solution architecture has an impact on the results of IT audit that have been carried out with only a few findings found by external auditors and the result PT XYZ pass the IT audit, which means that this framework has a very good impact on PSP, especially at the SME level.

Acknowledgments

The researcher would like to express his deepest gratitude to the entire IT audit team of Bank Indonesia who have provided support to me so that the research I conducted can be carried out well, especially his gratitude to PT XYZ IT who has participated earnestly in the activities during the research.

Author Contributions

This article was written by three individuals, S., M.A.A.S., and H.P.I. who have read and approved the published version of this manuscript. S., M.A.A.S., and H.P.I. designed the study and analyzed the data, performed the laboratory work, and wrote the manuscript. They drafted the original manuscript, prepared the introduction, results, discussion, methodology, and conclusion. S.S., M.A.A.S., and H.P.I. also contributed ideas to the research process, data processing, translation into English, review, and editing. All members of the research team collaborated at every stage until this article was completed.

Funding

Funding in this research is supported by the institution, the amount of which is adjusted to the applicable regulations on campus.

Conflicts of Interest

This research is conducted to provide information to the public regarding the research that has been conducted so that it can be used for educational purposes. in addition, this research is used by researchers for lecturer performance loads and accreditation needs of study programmes and institutions.

References

Agote-Garrido, A., Martín-Gómez, A. M., & Lama-Ruiz, J. R. (2023). Manufacturing System Design in Industry 5.0: Incorporating Sociotechnical Systems and Social Metabolism for Human-Centered, Sustainable, and Resilient Production. *Systems*, *11*(11), 537. https://doi.org/10.3390/systems11110537

Ajayi, F. A., & Udeh, C. A. (2024). Review of Workforce Upskilling Initiatives for Emerging Technologies in IT. *International Journal of Management & Entrepreneurship Research*, *6*(4), 1119–1137. https://doi.org/10.51594/ijmer.v6i4.1003

Al-Okaily, M. (2021). Assessing the Effectiveness of Accounting Information Systems in the Era of Covid-19 Pandemic. *Vine Journal of Information and Knowledge Management Systems*, *54*(1), 157–175. https://doi.org/10.1108/vjikms-08-2021-0148

Angganegara, M. A., Mukti, I. Y., & Fathinnuddin, M. (2025). Integration of Stride and Mitre Att&Ck Frameworks for Enhanced Cyber Threat Modeling: A Case Study of Digital Merchant Banking Application. *2025 International Conference on Advancement in Data Science, E-Learning and Information System (ICADEIS)*, 1–6. https://doi.org/10.1109/icadeis65852.2025.10933223

Antunes, M., Maximiano, M., & Gomes, R. (2022). A Client-Centered Information Security and Cybersecurity Auditing Framework. *Applied Sciences*, *12*(9), 4102. https://doi.org/10.3390/app12094102

Aravik, H., Hamzani, A. I., & Khasanah, N. (2025). Women Entrepreneurship in Indonesia: Opportunities and Challenges. *Islamic Banking: Jurnal Pemikiran dan Pengembangan Perbankan Syariah*, *10*(2), 327–348. https://doi.org/10.36908/isbank.v10i2.1422

Barati, M., & Rana, O. (2022). Tracking GDPR Compliance in Cloud-Based Service Delivery. *IEEE Transactions on Services Computing*, *15*(3), 1498–1511. https://doi.org/10.1109/tsc.2020.2999559

Budisantoso, R. I. N., & Sumarwan, A. (2022). Entrepreneurial Modes Towards Information Technology Applications in Business During Pandemic Covid-19 Based on Indonesia SMEs' Stories. *Indonesian Journal of Information Systems*, *4*(2). https://doi.org/10.24002/ijis.v4i2.4840

Damanik, D. P. P., Hutagalung, G., & Ginting, R. R. (2021). Analysis of the Effect of Auditor Independence, and Auditor Ethics on Audit Quality at A Public Accounting Firm in Medan City with Auditor Experience as A Moderating Variable. *Journal of Economics, Finance and Management Studies*, *4*(8), 1499–1508. https://doi.org/10.47191/jefms/v4-i8-28

Daousis, S., Peladarinos, N., Cheimaras, V., Papageorgas, P., Piromalis, D. D., & Munteanu, R. A. (2024). Overview of Protocols and Standards for Wireless Sensor Networks in Critical Infrastructures. *Future Internet*, *16*(1), 33. https://doi.org/10.3390/fi16010033

Darmawan, A. P., Erlando, A., & Santoso, D. B. (2023). Examining an Islamic Financial Inclusivity and Its Impact on Fundamental Economic Variables in Indonesia (An Approach of Static Panel Data Analysis). *Jurnal Ekonomi Syariah Teori dan Terapan*, *10*(4), 337–351. https://doi.org/10.20473/vol10iss20234pp337-351

Digital Payments - Worldwide | Statista Market Forecast. (2025). Retrieved from http://frontend.xmo.prod.aws.statista.com/outlook/fmo/payments/digital-payments/worldwide?

Fauzi, A. A., & Suryani, T. (2019). Measuring the Effects of Service Quality By Using Carter Model Towards Customer Satisfaction, Trust and Loyalty in Indonesian Islamic Banking. *Journal of Islamic Marketing*, *10*(1), 269–289. https://doi.org/10.1108/jima-04-2017-0048

Francis, J. R. (2023). Going Big, Going Small: A Perspective on Strategies for Researching Audit Quality. *The British Accounting Review*, *55*(2), 101167. https://doi.org/10.1016/j.bar.2022.101167

Gheorghe, M. (2010). Audit Methodology for IT Governance. *Informatica Economica*, *14*(1), 32-42. Retrieved from https://www.researchgate.net/publication/43121541

Greuning, H. V., & Bratanovic, S. B. (2020). *Analyzing Banking Risk: A Framework for Assessing Corporate Governance and Risk Management*. World Bank Publications. https://doi.org/10.1016/j.jclepro.2018.10.120

Hadjarati, P. R. Y. P., Widodo, A. M., & Tjahjono, B. (2025). Comparative Analysis of Enterprise Architecture Frameworks Using Togaf ADM and SPBE Architecture Based on Presidential Regulation No. 132 of 2022. *EDUVEST - Journal of Universal Studies*, *5*(3), 2766–2773. https://doi.org/10.59188/eduvest.v5i3.1772

Harmening, D. M. (2018). *Modern Blood Banking & Transfusion Practices*. Fa Davis.

Hasibovic, A. C., & Tanovic, A. (2024). Review of ISO 9001:2015 and ISO 27001:2013 Implementation in Financial Institution – Case Study. *2024 47th Mipro ICT and Electronics Convention (MIPRO)*, 1520–1525. https://doi.org/10.1109/mipro60963.2024.10569415

Hidayatullah, M. F., Irawan, B., Roziq, A., & Ma'mun, S. (2023). Enhancing Customer in Islamic Banking: A Case Study of Bank Syariah Indonesia's Marketing Strategy. *International Journal of Islamic Business and Economics (IJIBEC)*, *7*(2), 128–138. https://doi.org/10.28918/ijibec.v7i2.1966

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework. *Applied Sciences*, *14*(13), 5501. https://doi.org/10.3390/app14135501

Hubais, A. S. A., Kadir, M. R. A., Bilal, Z. O., & Alam, M. N. (2023). The Impact of Auditor Integrity to Audit Quality: An Exploratory Studies from the Middle East. *International Journal of Professional Business Review*, *8*(1), E01254–E01254. https://doi.org/10.26668/businessreview/2023.v8i1.1254

Indonesia, B. (1953). *Sejarah Bank Indonesia*. Retrieved from https://www.bi.go.id/id/tentang-bi/sejarah-bi/default.aspx

Indonesia, B. (2021a). *PBI_230621 Penyedia Jasa Pembayaran*. Retrieved from https://www.bi.go.id/elicensing/helps/pbi_230621 penyedia jasa pembayaran.pdf

Indonesia, B. (2021b). *Perizinan Penyelenggara Jasa Sistem Pembayaran*. Retrieved from https://www.bi.go.id/id/fungsi-utama/sistem-pembayaran/perizinan/default.aspx

Indonesia, B. (2022). *Dokumen Persyaratan Izin Penyedia Jasa Pembayaran (PJP) - Lembaga Selain Bank*. Retrieved from https://www.bi.go.id/elicensing/helps/dokumen

Kusmayasari, D., Bilgies, A. F., Damayanti, D., & Suharsono, J. (2023). The Influence of Audit Fee, Independence, and Competency on Audit Quality. *Journal of Governance, Taxation and Auditing*, *1*(4), 425–433. https://doi.org/10.38142/jogta.v1i4.653

Logie, J., & Maroun, W. (2021). Evaluating Audit Quality Using the Results of Inspection Processes Performed By An Independent Regulator. *Australian Accounting Review*, *31*(2), 128–149. https://doi.org/10.1111/auar.12328

Naji, R. N. (2020). Auditing Vehicle Insurance Contracts Compensation Under Civil Liability Insurance; Applied Research In The National Insurance Company.

Octaviani, D., & Ekasari, K. (2021). The Effect of Due Professional Care, Integrity, Confidentiality, and Independence on Audit Quality. *2nd Annual Management, Business and Economic Conference (AMBEC 2020)*, 106–110. https://doi.org/10.2991/aebmr.k.210717.022

Panjaitan, V. O., Tambuna, J., & Sirait, E. (2023). Pengaruh Model Pembelajaran Somatic, Auditory, Visualization, Intellectually (SAVI) Terhadap Hasil Belajar Siswa Kelas V Pada Subtema 1 Organ Gerak Hewan SD Negeri 095552 Pematang Siantar. *Innovative: Journal of Social Science Research*, *3*(6), 7601–7610. https://doi.org/10.31004/innovative.v3i6.5826

Pimentel, E., Lesage, C., & Ali, S. B. H. (2023). Auditor Independence in Kinship Economies: A Macintyrian Perspective. *Journal of Business Ethics*, *183*(2), 365–381. https://doi.org/10.1007/s10551-022-05073-6

Rahi, S., Ghani, M. A., & Ngah, A. H. (2020). Factors Propelling the Adoption of Internet Banking: The Role of E-Customer Service, Website Design, Brand Image and Customer Satisfaction. *International Journal of Business Information Systems*, *33*(4), 549. https://doi.org/10.1504/ijbis.2020.105870

Rijal, S., & Bakri, A. A. (2023). Effect of Auditor Specialization, Auditor Characteristics, Board Independence on Audit Quality Through Intellectual Capital: Study on Service Companies. *The Es Accounting and Finance*, *1*(02), 95–103. org/https://doi.org/10.58812/esaf.v1i02.66

Roghanian, P., Rasli, A., & Gheysari, H. (2012). Productivity Through Effectiveness and Efficiency in the Banking Industry. *Procedia - Social and Behavioral Sciences*, *40*, 550–556. https://doi.org/10.1016/j.sbspro.2012.03.229

Setyoso, F. A. A., Mulyana, R., & Nugraha, R. A. (2024). Utilizing ISO 27001:2022 in Information Security Design for BPRCCO SME Digital Transformation. *Ranah Research: Journal of Multidisciplinary Research and Development*, *6*(6), 2544–2553. https://doi.org/10.38035/rrj.v6i6.1121

Sulaiman, N. A. (2023). External Audit Quality: Its Meaning, Representations and Potential Conflict in Practice. *Accounting, Auditing & Accountability Journal*, *36*(5), 1417–1440. https://doi.org/10.1108/aaaj-02-2020-4443

Ton, K. (2023). Do Shared Auditors Improve Audit Quality? Evidence from Banking Relationships. *The Accounting Review*, *98*(1), 423–451. https://doi.org/10.2308/tar-2017-0179

Tumwebaze, Z., Bananuka, J., Kaawaase, T. K., Bonareri, C. T., & Mutesasira, F. (2022). Audit Committee Effectiveness, Internal Audit Function and Sustainability Reporting Practices. *Asian Journal of Accounting Research*, *7*(2), 163–181. https://doi.org/10.1108/ajar-03-2021-0036