

Article

Assessing Information Security Risk Exposure During the Transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 in a Banking Institution

Noviati Nurani * and Nilo Legowo

Information Systems Management Department, BINUS Graduate Program, Bina Nusantara University, Jakarta 11480, Indonesia; nlegowo@binus.edu

* Correspondence: noviati.nurani@binus.ac.id

Abstract

The transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 is often approached as a certification and documentation update. However, for banking institutions with critical digital operations, the transition may create a distinct form of information security exposure when existing controls, evidence, ownership, and risk treatment decisions are not fully aligned with the revised control structure. This study examines transitional risk exposure in Bank XYZ, a banking institution with an established ISO/IEC 27001:2013-based Information Security Management System (ISMS). Using a qualitative single-case study design, the research analyzes ISMS documents, 96 information security risk records, Statement of Applicability records, control implementation evidence, ISO/IEC 27001:2013-to-ISO/IEC 27001:2022 control mapping materials, and stakeholder validation within the scope of core banking development and operations in data center and disaster recovery center environments. Risk exposure was assessed by comparing inherent and residual risks using a likelihood-impact matrix, while transition readiness was evaluated through control applicability, evidence adequacy, ownership clarity, supplier dependency, human factor readiness, and transition governance. The findings show that Bank XYZ implemented or provided evidence for 109 of 114 ISO/IEC 27001:2013 controls and reduced 96 inherent risks, consisting of 38 Moderate and 58 Moderate-to-High risks, into 13 Low and 83 Low-to-Moderate residual risks. Nevertheless, the transition review revealed that a mature residual risk position under ISO/IEC 27001:2013 does not automatically indicate readiness for ISO/IEC 27001:2022. Of 11 newly introduced controls, 2 were implemented, 4 were partially implemented, 4 were not implemented, and 1 was not applicable. The most significant transition gaps were found in threat intelligence, information deletion, data masking, and data leakage prevention. The study contributes by distinguishing transitional risk exposure from residual risk and by offering a control-level basis for prioritizing ISO/IEC 27001:2022 transition activities in banking institutions.

Keywords: ISO/IEC 27001:2022; ISO/IEC 27001:2013; information security management system; transitional risk exposure; residual risk; banking cybersecurity; control readiness



Academic Editors: Shao-Fang Wen and Basel Katt

Received: 4 June 2026

Revised: 30 June 2026

Accepted: 9 July 2026

Published: 16 July 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

In the banking sector, digital infrastructure is no longer a supporting layer of organizational activity. It is embedded in transaction processing, customer interaction, regulatory reporting, data management, operational continuity, and digital service delivery. As banking

services become increasingly dependent on interconnected systems, information security becomes a governance and risk management issue rather than a purely technical concern. A failure in confidentiality, integrity, or availability may affect not only internal operations, but also customer trust, regulatory compliance, institutional reputation, and business continuity. Global risk reports continue to identify cyberattacks and digital security threats as major risks for organizations and society [1].

This condition is particularly important because banks operate critical information systems, process sensitive customer information, rely on third-party technology providers, and face strict regulatory expectations. Cybersecurity risks in banking may arise from both internal and external sources, including unauthorized access, credential misuse, phishing, malware, data leakage, service disruption, supplier weakness, and operational control failure. These risks can lead to financial loss, data loss, data corruption, operational disruption, reputational damage, and legal exposure. For this reason, information security management in banking must be linked to risk ownership, control selection, evidence, accountability, monitoring, and continual improvement.

An Information Security Management System (ISMS) provides a structured mechanism for managing such risks. ISO/IEC 27001 is one of the most widely adopted standards for establishing, implementing, maintaining, and continually improving an ISMS [2]. It requires organizations to understand their context, assess information security risks, determine risk treatment options, and select appropriate controls. ISO/IEC 27002 supports this standard by providing guidance for information security controls across organizational, people, physical, and technological dimensions [3]. ISO/IEC 27000 defines information security through the preservation of confidentiality, integrity, and availability, supported by related properties such as authenticity, accountability, non-repudiation, and reliability [4].

The relevance of ISO/IEC 27001 is especially clear in the banking sector. Previous studies have examined the use of ISO/IEC 27001 as a basis for information security governance, risk assessment, and control implementation. Culot et al. [5] reviewed the ISO/IEC 27001 literature and called for broader organizational and theoretical perspectives beyond technical implementation. Podrecca et al. [6] found that ISO/IEC 27001 certification may be associated with organizational performance benefits, while Mirtsch et al. [7] discussed ISO/IEC 27001 diffusion and certification as a signal of information security capability. Kitsios et al. [8] further emphasized the relevance of ISO/IEC 27001 for extracting value from information security and data-related practices. In the banking context, Legowo and Juhartoyo [9] showed that ISO 27001-based risk assessment can be used to evaluate information technology security systems in banks, assess maturity, prioritize assets, and recommend risk controls. These studies indicate that ISO/IEC 27001 can support risk-based information security management beyond formal compliance.

However, the publication of ISO/IEC 27001:2022 changes the discussion. For organizations that have implemented ISO/IEC 27001:2013 [10], the transition is often treated as a routine update of certification documents. Such an approach is too narrow, particularly for banking institutions with critical digital operations and complex governance structures. The issue is not only whether existing documents can be revised to follow the new version, but whether existing controls remain applicable, sufficiently evidenced, properly owned, monitored, and aligned with the revised control structure. Maturity under ISO/IEC 27001:2013 does not automatically transfer into readiness under ISO/IEC 27001:2022.

ISO/IEC 27001:2022 retains the management system foundation of ISO/IEC 27001:2013, but it updates the control structure and strengthens alignment with contemporary information security, cybersecurity, and privacy protection needs [2,3]. The revised control guidance in ISO/IEC 27002:2022 introduces and reorganizes controls related to areas such as threat intelligence, information deletion, data masking, data leakage prevention, monitor-

ing activities, configuration management, web filtering, cloud services, and ICT readiness for business continuity [3]. Existing controls may therefore require remapping, reinterpretation, revised evidence, clearer ownership, or stronger monitoring. A bank may appear mature under ISO/IEC 27001:2013 and still become exposed when the basis for evaluating control readiness changes under ISO/IEC 27001:2022.

This paper refers to that condition as transitional risk exposure. Transitional risk exposure occurs when existing controls, documentation, evidence, accountability, or monitoring arrangements are not fully aligned with the revised standard. It differs from residual risk. Residual risk reflects the remaining risk after existing controls are applied within the current control environment. Transitional risk exposure, by contrast, reflects the uncertainty that emerges during migration from one version of a standard to another. This distinction is important because a low or moderate residual risk position under ISO/IEC 27001:2013 does not necessarily mean that the organization is ready for ISO/IEC 27001:2022.

Recent cybersecurity governance literature supports this view. Information security governance requires alignment between security policies, organizational objectives, accountability, and management commitment [11]. The three lines model in cybersecurity emphasizes that cyber risk management depends on clear role allocation among operational management, risk and compliance functions, and independent assurance [12]. At the same time, risk-based approaches can become superficial when risk assessment results are weakly connected to control evidence, accountability, and decision-making [13]. Voluntary cybersecurity standards and frameworks can strengthen organizational security posture, but only when they are properly operationalized [14]. These perspectives suggest that ISO/IEC 27001:2022 adoption should be examined as a governance and risk transition, not merely as a certification update.

This study is timely because the ISO/IEC 27001:2022 transition requires organizations with existing ISO/IEC 27001:2013 certification or implementation to reassess their control environment against revised expectations. For banking institutions, this transition is especially important because their ISMS must support critical systems, regulatory obligations, third-party dependencies, operational resilience, and customer trust. Therefore, the transition creates a practical and research-relevant opportunity to examine whether an apparently mature ISO/IEC 27001:2013-based ISMS is sufficient for ISO/IEC 27001:2022 readiness.

Bank XYZ is used in this paper to examine how transitional risk exposure can appear in an organization that already had a mature ISO/IEC 27001:2013-based ISMS. The case is relevant because Bank XYZ implemented ISO/IEC 27001:2013 within the scope of core banking development and operations in data center and disaster recovery center environments. The case involves multiple internal stakeholders, including top management, information technology, risk management, procurement, human resources, compliance, and general affairs. This cross-functional scope reflects the fact that information security controls are not owned by one function alone; they are distributed across governance, technology, operations, people, suppliers, compliance, and physical security functions.

The case evidence shows that Bank XYZ had a mature ISO/IEC 27001:2013 control baseline. The organization implemented or provided evidence for 109 out of 114 ISO/IEC 27001:2013 controls and reduced 96 identified inherent risks, consisting of 38 Moderate and 58 Moderate-to-High risks, into residual risks consisting of 13 Low and 83 Low-to-Moderate risks. These results suggest that the existing control environment was largely effective within the assessed scope. At the same time, the transition to ISO/IEC 27001:2022 revealed areas requiring further attention, including the Statement of Applicability (SoA), control remapping, evidence adequacy, awareness and training, supplier governance, control ownership, and transition planning.

The paper addresses the following research question: how can transitional information security risk exposure be identified and prioritized in a banking institution with a mature ISO/IEC 27001:2013-based ISMS during the transition to ISO/IEC 27001:2022?

To answer this question, the paper focuses on three analytical objectives. First, it evaluates whether the existing ISO/IEC 27001:2013-based ISMS effectively reduced information security risk exposure within the assessed banking scope. Second, it identifies areas of control readiness that require further attention during the transition to ISO/IEC 27001:2022. Third, it develops a risk-based basis for prioritizing remediation actions so that transition activities are guided by residual risk, control criticality, evidence adequacy, supplier dependency, human factor readiness, and governance accountability rather than by documentation updates alone.

This paper contributes to the information security governance literature in three ways. First, it extends ISO/IEC 27001 research from implementation, certification, and compliance assessment toward transitional risk exposure. Second, it distinguishes transitional risk exposure from residual risk and explains why residual risk reduction under ISO/IEC 27001:2013 does not automatically indicate ISO/IEC 27001:2022 readiness. Third, it provides empirical evidence from a banking institution and offers a control-level perspective for prioritizing ISO/IEC 27001:2022 transition activities based on risk exposure, control readiness, evidence, supplier dependency, and governance accountability.

2. Related Work

2.1. Information Security Management Systems and ISO/IEC 27001

An Information Security Management System (ISMS) provides a governance structure through which information security risks can be identified, assessed, treated, monitored, and continually improved. ISO/IEC 27001 is widely adopted because it links information security objectives with organizational context, risk assessment, risk treatment, control selection, implementation evidence, and continual improvement [2]. ISO/IEC 27000 defines information security as the preservation of confidentiality, integrity, and availability, while also recognizing related properties such as authenticity, accountability, non-repudiation, and reliability [4].

The risk-based nature of ISO/IEC 27001 makes it particularly relevant for organizations operating in regulated and technology-dependent environments. Rather than prescribing the same set of controls for all organizations, the standard requires organizations to understand their context, assess their risks, determine risk treatment options, and justify the applicability of selected controls. ISO/IEC 27002 complements this approach by providing control guidance across organizational, people, physical, and technological dimensions [3]. Therefore, ISO/IEC 27001 should be understood not merely as a compliance checklist, but as a management system that links risk decisions, accountability, evidence, and review.

Prior research has shown that ISO/IEC 27001 may provide value beyond formal certification. Culot et al. [5] reviewed the ISO/IEC 27001 literature and argued that the field requires broader organizational and theoretical perspectives. Podrecca et al. [6] found that ISO/IEC 27001 certification may be associated with improvements in profitability, labor productivity, and partly sales performance. Mirtsch et al. [7] examined ISO/IEC 27001 diffusion and highlighted certification as a signal of information security capability. Kitsios et al. [8] further discussed how ISO/IEC 27001 can support value extraction from information security and data-related practices in IT-oriented organizations.

In the banking context, Legowo and Juhartoyo [9] showed that ISO 27001-based risk assessment can be used to evaluate information technology security systems in banks, assess maturity, prioritize information technology assets, and recommend risk controls. Their

study is important because it demonstrates the practical relevance of ISO 27001 for banking risk assessment. However, prior studies of this type mainly examine implementation, maturity, compliance, or risk treatment under an existing version of the standard. They do not fully address the transition condition in which an organization that appears mature under ISO/IEC 27001:2013 must reassess control readiness under ISO/IEC 27001:2022.

2.2. Information Security Governance and Cyber Risk Management

Information security governance concerns the way security responsibilities, decision rights, oversight mechanisms, and accountability structures are embedded within an organization. It links security objectives with business objectives, risk appetite, compliance obligations, and management oversight. AlGhamdi et al. [11] emphasized that information security governance depends on alignment between security policies, organizational goals, management commitment, and operational practices.

Cyber risk management translates governance expectations into risk decisions. ISO 31000:2018 frames risk management as an integrated and iterative process that includes risk identification, analysis, evaluation, treatment, monitoring, review, communication, and consultation [15]. NIST SP 800-30 similarly provides guidance for risk assessment by considering threat sources, vulnerabilities, likelihood, impact, and risk responses [16]. In an ISMS context, these references support the view that controls should be selected and evaluated according to risk exposure rather than applied mechanically.

A recurring issue in cybersecurity governance is role clarity. Valkenburg and Bongiovanni [12] examined the three lines model in cybersecurity and showed that cyber risk management requires coordination among operational management, risk and compliance functions, and independent assurance. This is particularly relevant for banking institutions, where information security responsibilities are distributed across information technology, risk management, compliance, procurement, human resources, internal audit, and business units. A control may be documented, but its effectiveness can be weakened if ownership, monitoring responsibility, and assurance mechanisms are unclear.

Risk-based approaches may also become superficial when they are used only as formal assessment routines. Slapnicar et al. [13] argued that cyber risk management may create an illusion of a risk-based approach when risk measurement appears structured but remains weakly connected to decision-making, control evidence, and accountability. This critique is relevant for ISO/IEC 27001 transition because transition readiness should not rely only on risk scores or control mapping. It also requires evidence that controls are operationally meaningful, owned by accountable functions, and continuously reviewed.

2.3. ISO/IEC 27001:2022 Transition and Control Readiness

ISO/IEC 27001:2022 updates the ISMS requirements and aligns the standard with the revised control guidance in ISO/IEC 27002:2022 [2,3]. The revised control structure reflects contemporary information security concerns, including cybersecurity, privacy protection, cloud services, threat intelligence, information deletion, data leakage prevention, monitoring activities, configuration management, web filtering, and ICT readiness for business continuity [3]. These changes are not only structural; they also affect how organizations interpret control applicability, evidence, ownership, and monitoring.

For organizations that implemented ISO/IEC 27001:2013, the transition to ISO/IEC 27001:2022 can easily be treated as a document-mapping activity. Such an approach is limited. Updating policies, procedures, and the Statement of Applicability (SoA) may create the appearance of readiness, but it does not necessarily show whether controls remain relevant and effective under the revised standard. Transition readiness depends on

whether existing controls can be remapped, reinterpreted, evidenced, owned, monitored, and governed in relation to the new control structure.

Control readiness, in this paper, refers to the condition in which a control is applicable, formally defined, implemented, evidenced, monitored, reviewed, and aligned with current organizational risks. This concept is useful because a control that was sufficient under ISO/IEC 27001:2013 may still require updated evidence, clearer ownership, or stronger monitoring under ISO/IEC 27001:2022. The transition therefore creates a risk exposure of its own: not necessarily because the old controls failed, but because the revised standard changes the expectations used to evaluate readiness.

Recent studies on cybersecurity standards and governance reinforce this view. Reuben-Owoh and Haig [14] showed that voluntary cybersecurity standards and frameworks can support organizational security posture, but their value depends on how they are adopted and operationalized. McIntosh et al. [17] also noted that governance, risk, and compliance frameworks need to be interpreted in relation to emerging technological risks and regulatory expectations. NIST Cybersecurity Framework 2.0 places governance, risk prioritization, communication, and continual improvement at the center of cybersecurity risk management [18]. These perspectives support the view that ISO/IEC 27001:2022 transition should be treated as a risk and governance problem rather than as a checklist exercise.

2.4. Transitional Risk Exposure

This study introduces transitional risk exposure as a concept for analyzing the migration from ISO/IEC 27001:2013 to ISO/IEC 27001:2022. Transitional risk exposure refers to the uncertainty or exposure that emerges when existing controls, documentation, evidence, accountability, or monitoring arrangements are not fully aligned with the revised standard.

This concept differs from residual risk. Residual risk describes the remaining risk after existing controls have been applied in the current control environment. Transitional risk exposure describes the uncertainty that appears when the standard used to evaluate the control environment changes. Therefore, an organization may have low or acceptable residual risk under ISO/IEC 27001:2013 but still face transitional exposure if its controls are not sufficiently aligned with ISO/IEC 27001:2022.

In this study, transitional risk exposure is examined through seven interrelated dimensions: control applicability, evidence adequacy, ownership clarity, monitoring and review, supplier dependency, human factor readiness, and transition governance. These dimensions are not independent. For example, a control may remain applicable under ISO/IEC 27001:2022 but still create transition exposure if the responsible owner is unclear or the available evidence is insufficient. Supplier dependency may also increase exposure when a control depends on third-party implementation or monitoring. Human factor readiness affects whether employees and control owners understand their revised responsibilities. Transition governance connects these dimensions by determining whether gaps are formally assigned, prioritized, monitored, and reported.

The interrelation among these dimensions means that ISO/IEC 27001:2022 readiness cannot be assessed only by counting mapped controls. A control-level transition assessment must examine how control applicability, evidence, ownership, monitoring, supplier dependency, human behavior, and governance accountability jointly shape readiness. This is the basis for treating ISO/IEC 27001:2022 migration as a transitional risk problem rather than a documentation update.

2.5. Information Security Risk Management, Assets, and Human Factors

Information security risk management depends on an organization's ability to understand its assets, threats, vulnerabilities, control environment, and business impacts.

Webb et al. [19] proposed a situation awareness model for information security risk management, emphasizing the need for contextual understanding in risk decision-making. Shedden et al. [20] also highlighted that asset identification in information security risk assessment should reflect business practice, not merely technical inventory. This is important because risks attached to core business processes may not be visible if assets are viewed only as hardware, software, or databases.

Human and behavioral factors also shape the effectiveness of information security controls. Herath and Rao [21] developed a framework for security policy compliance based on protection motivation and deterrence. Siponen and Willison [22] criticized the way information security management standards may become ineffective when they are applied as formal compliance mechanisms rather than as operational governance tools. Spears and Barki [23] emphasized user participation in information systems security risk management, while Ifinedo [24] showed that socialization, influence, and cognition affect information security policy compliance.

More recent studies also directly connect human behavior with ISO/IEC 27001 implementation and information security policy compliance. Kor and Metin [25] emphasized that effective ISO/IEC 27001 implementation depends not only on technical controls and documentation, but also on individual security behavior and human-related organizational practices. Arif et al. [26] similarly showed that employees' compliance with organizational information security policies is influenced by human factors that shape security behavior. These studies support the view that awareness and training should not be treated as peripheral activities in ISO/IEC 27001:2022 transition. They form part of the organizational conditions that determine whether controls remain effective after the standard changes.

In the context of transitional risk exposure, human factors are particularly important because the revised standard may change control interpretation, evidence expectations, monitoring responsibilities, and ownership arrangements. Employees involved in procurement, IT operations, risk management, compliance, and human resources may require different forms of role-based awareness to understand their responsibilities under ISO/IEC 27001:2022. Therefore, human factor readiness is treated in this paper as one of the dimensions of transitional risk exposure.

2.6. Cybersecurity Risk in Banking and Digital Financial Services

Banking institutions operate in a digital environment where information security incidents can affect customer trust, transaction reliability, regulatory compliance, and service continuity. Unlike many other sectors, banks manage sensitive customer information, critical transaction systems, digital channels, regulatory reporting processes, and third-party service providers. Cybersecurity risk in banking is therefore closely connected to operational resilience and institutional trust.

Recent studies on financial technology and digital banking emphasize the need for sector-specific cybersecurity risk management. AlBenJasim et al. [27] developed a cybersecurity framework for FinTech ecosystems and highlighted the need to align cybersecurity controls with regulatory expectations, operational risks, and ecosystem dependencies. Azura et al. [28] proposed an integrated cybersecurity risk management framework for online banking systems, arguing that online banking requires structured approaches that address the specific risks of digital financial services.

Open banking and digital payment ecosystems further increase the complexity of security governance. Gounari [29] discussed the security and regulatory implications of open banking, emphasizing secure transaction protocols, data protection, and regulatory alignment. Although open banking arrangements differ across jurisdictions, the underlying issue

is relevant across banking environments: information security controls must address interconnected systems, third-party access, customer protection, and compliance requirements.

Human factors remain equally important in digital banking. Shafie et al. [30] examined mobile banking security and highlighted the role of confidentiality, authentication, and device trust. This supports the need to include awareness and training in transition readiness. Even where technical controls are available, employees and users may still be vulnerable to phishing, social engineering, weak authentication behavior, or improper handling of sensitive information. For banking institutions, technical controls and human behavior therefore need to be treated as connected parts of the same security environment.

2.7. Residual Risk and Transitional Risk Exposure

Risk exposure refers to the level of risk faced by an organization before or after the implementation of controls. In information security, exposure is shaped by threats, vulnerabilities, likelihood, business impact, asset criticality, and control effectiveness. Inherent risk describes the level of risk before controls are applied, while residual risk describes the remaining risk after controls have been implemented.

Residual risk analysis is important in an ISMS because it shows whether the control environment has reduced risk to an acceptable level. However, residual risk should not be interpreted as a permanent condition. Risk can change as technologies, organizational structures, regulatory expectations, threat actors, supplier dependencies, and business processes change. ISO 31000:2018 reflects this view by treating risk management as a dynamic process that requires monitoring, review, and continual improvement [15].

The transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 introduces another form of exposure: transitional risk exposure. This exposure may appear even in organizations with mature ISO/IEC 27001:2013 implementation. In this sense, residual risk and transitional risk exposure are related but not identical. Residual risk shows what remains after current controls are applied; transitional risk exposure shows what becomes uncertain when the basis for evaluating those controls changes.

This distinction is central to this paper. If a bank has reduced inherent risks to acceptable residual levels under ISO/IEC 27001:2013, the result indicates that the existing control environment is effective within the previous standard's structure. It does not automatically show that the same controls are ready for ISO/IEC 27001:2022. Transition readiness requires additional analysis of control mapping, evidence adequacy, applicability, ownership, monitoring, supplier dependency, human factor readiness, and governance accountability.

2.8. Research Gap

The literature indicates that ISO/IEC 27001 is well established as a risk-based ISMS standard and that certification may provide organizational and signaling benefits [2,5–8]. Prior banking-related research also shows that ISO 27001-based risk assessment can support maturity evaluation, asset prioritization, and risk control recommendations [9]. Research on cybersecurity governance further emphasizes the importance of accountability, control evidence, risk management, compliance, and business alignment [11,12,14]. Studies on information security risk management and human factors highlight the importance of asset identification, user participation, awareness, and security behavior [19–21,23–26].

What remains less developed is the transition condition. Existing studies tend to examine ISO/IEC 27001 implementation, certification, compliance assessment, risk treatment, framework comparison, or general cybersecurity governance. Less attention has been given to organizations that already appear mature under ISO/IEC 27001:2013 but must reassess their readiness when moving to ISO/IEC 27001:2022.

This distinction matters because maturity under the previous version does not automatically resolve the control-readiness questions introduced by the revised standard. A banking institution may show effective residual risk reduction under ISO/IEC 27001:2013 but still face transitional risk exposure if its controls require remapping, reinterpretation, updated evidence, clearer ownership, stronger supplier monitoring, role-based awareness, or a structured transition roadmap.

The gap is particularly relevant in banking. Banks operate critical digital services, process sensitive customer information, rely on third parties, and face strict regulatory expectations [27–33]. For such institutions, ISO/IEC 27001:2022 transition cannot be evaluated only by whether documentation has been updated. It requires a control-level and risk-based assessment of whether existing controls remain relevant, accountable, evidenced, monitored, and aligned with the revised standard.

This paper addresses that gap by examining transitional information security risk exposure in a banking institution with a mature ISO/IEC 27001:2013-based ISMS. Rather than treating compliance as the final outcome, the analysis positions ISO/IEC 27001:2013 maturity as the baseline for evaluating ISO/IEC 27001:2022 transition readiness.

3. Materials and Methods

3.1. Research Design and Case Selection

This study uses a qualitative single-case study design to examine information security risk exposure during the transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022, following established case study research principles [34]. The case study design was selected because the transition condition cannot be separated from the institutional context in which controls are implemented, evidenced, owned, monitored, and reviewed. The purpose of the study is not statistical generalization, but analytical generalization: the case is used to explain how a mature ISO/IEC 27001:2013-based ISMS may still generate transition exposure when assessed against ISO/IEC 27001:2022.

Bank XYZ was selected because it had an established ISO/IEC 27001:2013-based ISMS and maintained formal risk assessment records, a Statement of Applicability (SoA), control implementation evidence, internal audit evidence, and stakeholder validation records. The assessed ISMS scope covered the development and operation of the Core Banking System within data center and disaster recovery center environments. This scope was selected because it represents a critical banking environment in which confidentiality, integrity, availability, continuity, access management, incident handling, and supplier-related controls are directly linked to operational resilience.

The unit of analysis is the control-level transition from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 within the defined ISMS scope. The baseline condition is the ISO/IEC 27001:2013 control and residual risk profile. The transition condition is the readiness of the applicable ISO/IEC 27001:2022 control structure, with particular attention to newly introduced controls and controls requiring reinterpretation, updated evidence, or clearer ownership.

3.2. Dataset Description

The dataset consisted of six categories of evidence: ISMS documents, risk assessment records, SoA records, control implementation evidence, stakeholder interviews, and control mapping materials. The evidence was analyzed as an integrated dataset rather than as isolated documents. This was necessary because implementation status could not be verified from policy documents alone; it also required risk records, operational evidence, audit evidence, and stakeholder validation.

Table 1 describes the dataset used in the study. To protect institutional confidentiality, internal document titles, document codes, system names, and participant identities are not

disclosed. However, the type, analytical function, and scope of each evidence category are described to support transparency and reproducibility.

Table 1. Dataset used in the study.

Evidence Category	Dataset Scope	Analytical Use	Verification Role
ISMS documents	Policies, procedures, standards, and operational guidance within the certified ISMS scope	To identify formal control design, scope boundaries, control objectives, and documented responsibilities	Checked whether formal procedures existed and whether they were aligned with the assessed controls
Risk assessment records	96 information security risk records within the assessed ISMS scope	To compare inherent risk and residual risk as the ISO/IEC 27001:2013 baseline	Used as the baseline for evaluating whether mature residual risk reduction translated into transition readiness
Statement of Applicability	SoA records for ISO/IEC 27001:2013 and transition mapping to ISO/IEC 27001:2022	To examine applicability, exclusion rationale, control ownership, and transition needs	Used to confirm which controls were applicable, not applicable, implemented, or requiring transition update
Control implementation evidence	Evidence for 114 ISO/IEC 27001:2013 controls and 78 applicable ISO/IEC 27001:2022 controls	To verify whether controls were implemented, evidenced, monitored, and operationally integrated	Used to classify implementation status and identify evidence gaps
Stakeholder interviews	10 structured interviews with ISMS-related functions	To validate whether documented controls reflected operational practice	Used to triangulate document evidence and clarify ownership, monitoring, and implementation gaps
Control mapping materials	Mapping between ISO/IEC 27001:2013 Annex A controls and ISO/IEC 27001:2022 control categories	To identify control continuity, newly introduced controls, and areas requiring reinterpretation	Used to identify transition exposure at the control level

3.3. Interview Participants and Validation Procedure

Structured interviews were conducted with ten stakeholders involved in ISMS governance, implementation, monitoring, and assurance. The participants were selected purposively because their functions were directly related to the assessed controls. The interviews were used to validate documentary evidence, clarify control ownership, and identify operational gaps that were not visible in formal documents.

Table 2 summarizes the interview participants by functional role. Participant names and organizational titles are anonymized for confidentiality.

The validation process followed three steps. First, each relevant control was reviewed against formal documentation and available evidence. Second, stakeholder responses were used to confirm whether the documented control was implemented in practice. Third, inconsistencies between documentation, evidence, and stakeholder validation were treated as transition-relevant gaps. A control was not classified as implemented solely because a policy existed; it also had to be supported by operational evidence and clear responsibility. The interviews were structured validation interviews rather than surveys, and the results were used to confirm the consistency between documented evidence, operational practice, and control ownership.

Table 2. Interview participants used for stakeholder validation.

Code	Functional Area	Main Validation Focus
P1	Information security governance	ISMS scope, policy framework, SoA interpretation, and transition planning
P2	Core banking application operations	Application-level control implementation and operational evidence
P3	IT infrastructure and data center operations	Infrastructure controls, monitoring, backup, recovery, and availability controls
P4	Information security risk management	Risk register, inherent risk, residual risk, and treatment decisions
P5	Compliance	Regulatory alignment and compliance-related evidence
P6	Internal audit	Audit findings, evidence adequacy, and assurance perspective
P7	Procurement and supplier management	Supplier governance, third-party control evidence, and vendor monitoring
P8	Human resources and awareness	Security awareness, role-based training, and people-related controls
P9	General affairs and physical security	Physical security controls and environmental monitoring
P10	Management representative or ISMS coordinator	Cross-functional ownership, management review, and transition roadmap

3.4. Data Collection Procedure

Data collection was conducted through document review, risk record extraction, SoA review, control evidence review, and stakeholder validation. The document review identified the formal ISMS structure, including scope, policies, procedures, control objectives, and control ownership. The risk record extraction identified the number and distribution of inherent and residual risks within the assessed scope. The SoA review determined which controls were applicable, excluded, implemented, or required transition update. The control evidence review examined whether each control was supported by operational evidence, monitoring records, audit trails, or other verifiable artifacts. Finally, stakeholder validation was used to clarify whether documented controls reflected actual practice.

Data collection for the ISO/IEC 27001:2013 baseline was conducted during the thesis research period from January to May 2025. This period covered document review, risk assessment analysis, SoA review, control evidence review, and stakeholder validation within the certified ISMS scope. The ISO/IEC 27001:2022 transition mapping was subsequently prepared during the 2026 manuscript revision process to evaluate whether the 2025 baseline remained aligned with the revised control structure. This separation is important because the 2013 baseline represents the bank's mature pre-transition condition, whereas the 2022 mapping represents the transition-readiness assessment used in this paper.

The procedure was designed to improve reproducibility by linking each conclusion to a traceable evidence path. For example, a control classified as implemented had to be supported by: (1) formal documentation; (2) evidence of operation or monitoring; and (3) stakeholder confirmation. A control classified as partially implemented had some supporting evidence but lacked completeness, consistency, formalization, or monitoring. A control classified as not implemented lacked formalized procedures or operational evidence within the assessed scope. A control classified as not applicable was outside the defined ISMS scope and had to be justified in the SoA.

3.5. Risk Assessment and Baseline Selection

The study used the ISO/IEC 27001:2013 residual risk profile as the baseline for transition assessment. This baseline was selected because it represented the last mature control environment before ISO/IEC 27001:2022 transition. The baseline consisted of 96 informa-

tion security risks within the certified ISMS scope. At the inherent level, 38 risks were classified as Moderate and 58 risks were classified as Moderate-to-High. After the application of ISO/IEC 27001:2013 controls, the residual risk profile consisted of 13 Low risks and 83 Low-to-Moderate risks.

The risk assessment followed the logic of ISO 31000:2018 by comparing exposure before and after control treatment [15]. It also followed the risk assessment logic of NIST SP 800-30 by considering threats, vulnerabilities, likelihood, impact, and treatment responses [16]. In this study, these standards were not used as abstract references only. They were operationalized by: (1) identifying risk records within the ISMS scope; (2) comparing inherent and residual risk categories; (3) linking residual risk reduction to ISO/IEC 27001:2013 control evidence; and (4) reassessing whether the same baseline was sufficient for ISO/IEC 27001:2022 transition readiness.

Risk exposure was calculated using an institutional likelihood–impact matrix. Likelihood and impact were each scored on a five-point ordinal scale. The likelihood scale is presented in Table 3, and the impact scale is presented in Table 4. The risk value was calculated as Likelihood $\times$ Impact and interpreted using the bank’s internal risk attribute matrix presented in Table 5. The matrix classified risk into five categories: Low, Low-to-Moderate, Moderate, Moderate-to-High, and High. The interpretation of each risk level and its corresponding treatment expectation are presented in Table 6. The bank’s risk appetite was set at the Low-to-Moderate level; therefore, Moderate, Moderate-to-High, and High risks required escalation, evaluation, or mitigation by the relevant risk owner or Risk Committee.

Table 3. Likelihood scale used in the risk assessment.

Score	Likelihood Level	Description
1	Rare	The event is unlikely to occur within three years and may occur only under exceptional circumstances.
2	Unlikely	The event is unlikely to occur more than once within two to three years.
3	Possible	The event may occur within one to two years.
4	Likely	The event may occur within the next twelve months due to operational or external conditions.
5	Almost certain	The event is expected to occur or recur within twelve months.

Table 4. Impact scale used in the risk assessment.

Score	Impact level	General Interpretation
1	Low	Limited impact on information assets, operations, compliance, or service continuity.
2	Low-to-Moderate	Manageable impact that remains within normal operational tolerance.
3	Moderate	Meaningful impact on confidentiality, integrity, availability, compliance, business process continuity, or service delivery that requires management attention.
4	Moderate-to-High	Significant impact that may violate risk appetite and requires escalation and mitigation.
5	High	Severe impact that exceeds risk appetite and requires immediate escalation and mandatory mitigation.

Table 5. Risk attribute matrix used to classify likelihood-impact combinations.

Likelihood	Impact				
	1 Low	2 Low-to-Mod.	3 Moderate	4 Mod.-to-High	5 High
5 Almost certain	Moderate	Moderate	Moderate-to-High	High	High
4 Likely	Low-to-Moderate	Moderate	Moderate	Moderate-to-High	High
3 Possible	Low-to-Moderate	Low-to-Moderate	Moderate	Moderate-to-High	High
2 Unlikely	Low	Low-to-Moderate	Low-to-Moderate	Moderate	Moderate-to-High
1 Rare	Low	Low	Low-to-Moderate	Moderate	Moderate-to-High

Table 6. Risk level interpretation and treatment expectation.

Risk Level	Risk Appetite Interpretation	Treatment Expectation
Low	Within tolerance	Accept or monitor through routine control activities.
Low-to-Moderate	Within the bank's risk appetite	Accept with monitoring or maintain routine controls.
Moderate	Risk appetite may be threatened	Review, escalate when needed, and determine mitigation by the relevant risk owner.
Moderate-to-High	Risk appetite is considered violated	Escalate and mitigate through accountable risk owners or Risk Committee members.
High	Clearly exceeds risk appetite	Immediate escalation and mandatory mitigation.

The transition baseline was defined by two additional measures: the applicability of 78 ISO/IEC 27001:2022 controls within the assessed scope and the implementation status of 11 newly introduced controls. This baseline selection allowed the study to distinguish between residual risk maturity under ISO/IEC 27001:2013 and transition readiness under ISO/IEC 27001:2022.

3.6. Control Assessment Criteria

The control assessment combined documentary evidence, implementation evidence, SoA justification, and stakeholder validation. Table 7 defines the classification criteria used to assess control readiness.

Table 7. Control assessment categories and verification criteria.

Category	Verification Criteria
Implemented	The control was formally defined, supported by documented procedures, implemented within the assessed scope, evidenced by operational or monitoring records, and confirmed by relevant stakeholders.
Partially implemented	The control existed or was partly practiced, but evidence was incomplete, implementation was inconsistent, monitoring was not systematic, ownership was unclear, or the control was not fully integrated into the ISMS.
Not implemented	The control had no formalized procedure, no operational evidence, or no confirmed implementation within the assessed ISMS scope.
Needs transition update	The control existed under ISO/IEC 27001:2013 but required remapping, reinterpretation, revised evidence, clearer ownership, or updated SoA justification to align with ISO/IEC 27001:2022.
Not applicable	The control was outside the certified ISMS scope and its exclusion was documented or justified in the SoA.

This classification avoided a binary view of compliance. A control could be mature under ISO/IEC 27001:2013 and still require transition update if the evidence, ownership, monitoring, or interpretation did not fully align with ISO/IEC 27001:2022.

3.7. Interrelationship Among Inspected Factors

To address the interdependence among the inspected factors, the study treated transitional risk exposure as the result of interactions among residual risk, control readiness, evidence adequacy, ownership clarity, operational integration, supplier dependency, and SoA alignment. Figure 1 illustrates these relationships.

The figure shows that transition exposure was not treated as an isolated control gap. Instead, each control was interpreted through the interaction between the existing risk baseline, the revised control structure, and the operational evidence supporting implementation.

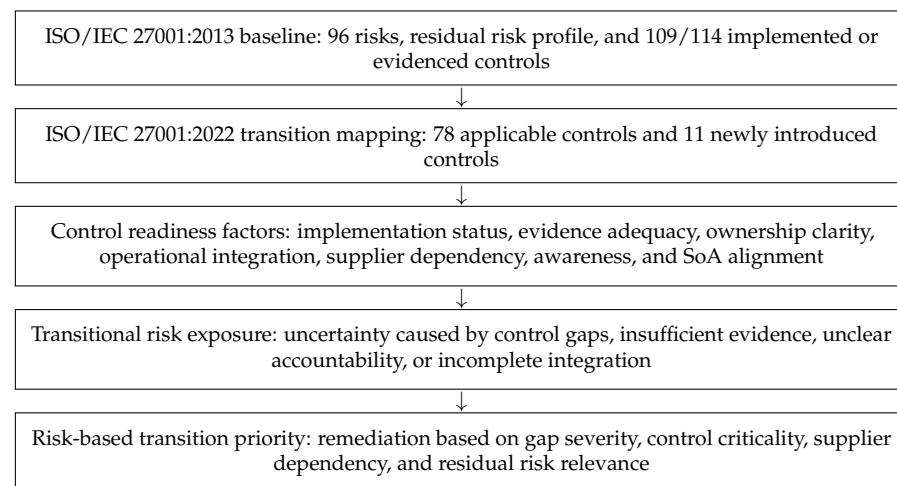


Figure 1. Interrelationship among inspected factors influencing transitional risk exposure.

3.8. Data Analysis Procedure

The analysis was conducted in seven stages. First, the certified ISMS scope was defined by reviewing the core banking development and operation environment, data center and disaster recovery center boundaries, and the organizational functions involved. Second, the ISO/IEC 27001:2013 risk baseline was established by extracting 96 risk records and comparing inherent and residual risk categories. Third, the ISO/IEC 27001:2013 control baseline was reviewed by examining 114 Annex A controls and identifying 109 controls that were implemented or supported by evidence.

Fourth, the ISO/IEC 27001:2022 control structure was mapped against the existing ISO/IEC 27001:2013 baseline. Fifth, 78 applicable ISO/IEC 27001:2022 controls were identified from the SoA and assessed against scope relevance, evidence, ownership, and monitoring. Sixth, the 11 newly introduced ISO/IEC 27001:2022 controls were analyzed in greater detail because they represented the most visible transition-specific control changes. Finally, findings were synthesized into a transition exposure profile by identifying which factors produced the strongest gaps and which areas should be prioritized for remediation.

4. Results

4.1. Existing ISMS Scope and ISO/IEC 27001:2013 Baseline

The ISMS scope at Bank XYZ covered the development and operation of the Core Banking System within data center and disaster recovery center environments. This scope represented a critical part of the bank's digital operations because core banking supported transaction processing, customer account management, service availability, and operational continuity. The assessment also showed that information security management within this scope was distributed across several organizational functions, including top management, information technology, risk management, procurement, human resources, compliance, internal audit, and general affairs.

The ISO/IEC 27001:2013 baseline showed a mature but not transition-complete control environment. Bank XYZ implemented or provided evidence for 109 out of 114 ISO/IEC 27001:2013 Annex A controls within the assessed scope. The remaining controls were excluded or considered not applicable based on scope boundaries, operational conditions, and SoA justification. This baseline indicates that the bank had a strong existing ISMS; however, it also provides a reference point for assessing whether maturity under the 2013 version was sufficient for transition to the 2022 version.

Table 8 provides the numeric baseline requested for verifying the research gap. The baseline shows that the case was not an immature ISMS. Instead, it was an organization with substantial ISO/IEC 27001:2013 coverage and a reduced residual risk profile. This makes the transition problem analytically important: the question is not whether the bank had basic controls, but whether an apparently mature control baseline remained sufficient when assessed against the revised ISO/IEC 27001:2022 control structure.

Table 8. ISO/IEC 27001:2013 baseline used for transition assessment.

Baseline Element	Numeric Evidence	Interpretation
ISO/IEC 27001:2013 controls reviewed	114 controls	Complete Annex A baseline for the assessed scope
Implemented or evidenced controls	109 controls	Mature implementation baseline under the 2013 standard
Information security risks assessed	96 risks	Risk baseline for inherent and residual exposure comparison
Moderate inherent risks	38 risks	Initial risk exposure before control treatment
Moderate-to-High inherent risks	58 risks	Higher initial exposure in critical operational areas
Low residual risks	13 risks	Risks reduced to the lowest assessed residual level
Low-to-Moderate residual risks	83 risks	Remaining residual risk requiring monitoring and continual improvement

The 109/114 figure reports the controls that were implemented or supported by evidence in the SoA baseline. To make the exclusion basis explicit, Table 9 lists the five ISO/IEC 27001:2013 controls that were treated as not applicable or outside the assessed ISMS scope in the control-count summary. The thesis scope review also flagged two broader development-related control areas, A.14.1.2 and A.14.2, for transition review; these are treated in this paper as transition-scope notes rather than as additional missing controls in the 109/114 baseline count.

Table 9. ISO/IEC 27001:2013 controls excluded from the assessed ISMS scope.

Control	Control Name	Justification
A.6.2.1	Mobile device policy	Mobile devices were not used as part of the assessed core banking, data center, and disaster recovery center ISMS scope.
A.10.1.1	Policy on the use of cryptographic controls	The assessed scope did not include active cryptographic control management requiring a separate cryptographic-control policy.
A.10.1.2	Key management	Key management was outside the assessed environment because active encryption-key administration was not performed within the defined scope.
A.11.2.6	Security of equipment and assets off-premises	Equipment and assets within the assessed scope were located in controlled office, data center, or disaster recovery center environments.
A.18.1.5	Regulation of cryptographic controls	The control was not applicable because cryptographic regulatory requirements were outside the assessed ISMS scope and were not part of the control baseline.

4.2. Inherent and Residual Risk Exposure

The risk assessment identified 96 inherent risks within the ISMS scope. Before considering the effect of implemented controls, 38 risks were categorized as Moderate and 58 risks were categorized as Moderate-to-High. After ISO/IEC 27001:2013 controls were applied, the residual risk profile shifted to 13 Low risks and 83 Low-to-Moderate risks, as summarized in Table 10.

Table 10. Change from inherent to residual risk exposure.

Risk Level	Inherent Risk	Residual Risk
Low	0	13
Low-to-Moderate	0	83
Moderate	38	0
Moderate-to-High	58	0
Total	96	96

The shift from Moderate and Moderate-to-High inherent risks toward Low and Low-to-Moderate residual risks indicates that the ISO/IEC 27001:2013 control environment was effective in reducing the assessed risk exposure. However, the residual risk profile did not, by itself, verify ISO/IEC 27001:2022 readiness. The transition assessment therefore used this risk profile as the baseline rather than as the final conclusion.

4.3. ISO/IEC 27001:2022 Applicability and Control Mapping

The transition mapping identified 78 ISO/IEC 27001:2022 controls as applicable within the assessed ISMS scope. The remaining controls were excluded based on SoA justification and scope boundaries. The transition baseline is summarized in Table 11. The mapping process showed that the transition was not merely a change in numbering. Several control expectations required reinterpretation of evidence, ownership, and operational integration.

Table 11. Transition baseline for ISO/IEC 27001:2022 assessment.

Transition Element	Numeric Evidence	Interpretation
Applicable ISO/IEC 27001:2022 controls	78 controls	Controls relevant to the certified ISMS scope
Newly introduced controls assessed	11 controls	Primary focus for transition-specific exposure analysis
Fully implemented new controls	2 controls	Existing practices already supported these controls
Partially implemented new controls	4 controls	Basic mechanisms existed but needed formalization, stronger evidence, or clearer integration into the development and operational governance process
Not implemented new controls	4 controls	Transition gaps requiring new capability or formal implementation
Not applicable new controls	1 control	Excluded based on scope and SoA justification

This transition baseline demonstrates why ISO/IEC 27001:2013 maturity did not automatically resolve ISO/IEC 27001:2022 readiness. Although the 2013 baseline showed strong residual risk reduction, the 2022 transition baseline revealed gaps in several new control areas.

4.4. Implementation Status of Newly Introduced Controls

The eleven newly introduced ISO/IEC 27001:2022 controls showed uneven implementation maturity, as detailed in Table 12. Two controls were fully implemented: physical

security monitoring and monitoring activities. These controls were supported by existing surveillance, monitoring, and operational security practices. Four controls were partially implemented: ICT readiness for business continuity, configuration management, web filtering, and secure coding. These areas had some existing mechanisms but lacked consistent formalization, complete evidence, or full integration into governance processes. Four controls were not implemented: threat intelligence, information deletion, data masking, and data leakage prevention. These controls represented the most significant transition exposure because they required new or substantially strengthened capabilities. One control was not applicable within the current ISMS scope.

Table 12. Implementation status and gap severity of newly introduced ISO/IEC 27001:2022 controls.

Control	Control Name	Status	Gap Severity	Evidence-Based Interpretation
5.7	Threat intelligence	Not implemented	High	No formal threat intelligence process was identified within the assessed ISMS scope.
5.23	Information security for use of cloud services	Not applicable	–	Excluded because cloud service use was outside the assessed certified scope.
5.30	ICT readiness for business continuity	Partially implemented	Medium	ICT recovery arrangements existed, but formal testing and transition evidence required strengthening.
7.4	Physical security monitoring	Implemented	None	Existing surveillance and physical monitoring evidence supported the control.
8.9	Configuration management	Partially implemented	Medium	Configuration control existed but was not consistently standardized across all relevant environments.
8.10	Information deletion	Not implemented	High	Formal data deletion procedures were not consistently defined across relevant environments.
8.11	Data masking	Not implemented	High	Data masking was not formally implemented for relevant non-production or testing contexts.
8.12	Data leakage prevention	Not implemented	High	DLP capability was not formally implemented as a measurable control.
8.16	Monitoring activities	Implemented	None	Monitoring mechanisms and operational security evidence were already available.
8.23	Web filtering	Partially implemented	Medium	Web filtering mechanisms existed, but policy and enforcement consistency required improvement.
8.28	Secure coding	Partially implemented	Medium	Development governance existed within the assessed scope, but secure coding evidence and role-specific verification required stronger formalization.

The numeric distribution of new-control readiness is summarized in Table 13. The largest share of transition exposure was located in controls that were not implemented or partially implemented.

Table 13. Distribution of implementation status for newly introduced controls.

Implementation Status	Number of Controls	Percentage
Implemented	2	18.2%
Partially implemented	4	36.4%
Not implemented	4	36.4%
Not applicable	1	9.1%
Total	11	100.0%

The results indicate that transition exposure was concentrated in proactive and data-centric controls. Threat intelligence, information deletion, data masking, and data leakage prevention had high gap severity because they were not merely documentation up-

dates; they required new processes, technical mechanisms, governance ownership, or evidence models.

4.5. Interrelationship of Transition Risk Factors

The analysis showed that transition exposure was shaped by the interaction among several factors rather than by a single missing control. Table 14 summarizes the observed relationship among inspected factors based on the case evidence.

Table 14. Interrelationship among inspected transition risk factors.

Factor	Strongest Relation	Observed Evidence	Implication for Transition Exposure
Residual risk baseline	Control readiness	96 risks were reduced to Low or Low-to-Moderate residual levels, but new controls still showed gaps	Mature residual risk reduction did not automatically ensure 2022 readiness
Evidence adequacy	Implementation status	Partially implemented controls had some evidence but lacked completeness, consistency, or testing	Evidence gaps created uncertainty even where some control activity existed
Ownership clarity	Operational integration	Controls distributed across IT, risk, procurement, HR, compliance, internal audit, and general affairs	Controls required cross-functional accountability rather than single-unit ownership
Supplier dependency	SoA and remediation priority	Supplier governance was identified as a transition improvement area	Third-party dependency increased the need for stronger monitoring and accountability
Awareness and training	People-related control readiness	Awareness existed but needed stronger role-based alignment	Human-factor exposure remained dynamic during transition
SoA alignment	Applicability and exclusion decisions	78 controls were applicable and exclusions required justification	Weak SoA justification could produce apparent compliance without verified readiness

This finding supports the argument that transitional risk exposure is not equivalent to residual risk. Residual risk describes the risk remaining after existing controls. Transitional risk exposure describes the uncertainty created when a revised control structure changes the evidence, ownership, applicability, and implementation expectations.

4.6. Risk-Based Transition Priority

Based on the assessment, ISO/IEC 27001:2022 transition should begin with activities that directly reduce the highest transition exposure. Table 15 ranks transition actions using the case evidence.

Table 15. Risk-based transition priorities derived from the case evidence.

Priority	Transition Activity	Primary Evidence	Expected Outcome
1	Formalize threat intelligence	Control 5.7 not implemented; high gap severity	Establish a repeatable process for collecting, analyzing, and using threat information
2	Define information deletion procedures	Control 8.10 not implemented; high gap severity	Create evidence-based deletion requirements across relevant environments
3	Implement data masking	Control 8.11 not implemented; high gap severity	Reduce exposure of sensitive data in non-production or testing contexts

Table 15. Cont.

Priority	Transition Activity	Primary Evidence	Expected Outcome
4	Establish DLP capability	Control 8.12 not implemented; high gap severity	Strengthen data leakage detection, prevention, and monitoring
5	Strengthen ICT readiness testing	Control 5.30 partially implemented; medium gap severity	Improve continuity evidence and recovery validation
6	Standardize configuration management	Control 8.9 partially implemented; medium gap severity	Improve consistency of configuration baselines and change evidence
7	Improve web filtering enforcement	Control 8.23 partially implemented; medium gap severity	Align policy, technical enforcement, and monitoring evidence
8	Update the SoA and ownership matrix	78 applicable controls and cross-functional ownership	Improve traceability among risks, controls, evidence, and accountable owners

This prioritization differs from a checklist approach because it uses the observed distribution of implementation status and gap severity. The most urgent transition actions are those linked to not implemented and high-severity controls, especially data-centric and proactive security controls.

5. Discussion

5.1. Original Findings from the Case

The first original finding is that ISO/IEC 27001:2013 maturity did not automatically translate into ISO/IEC 27001:2022 readiness. The evidence shows a mature baseline: 109 of 114 ISO/IEC 27001:2013 controls were implemented or supported by evidence, and 96 inherent risks were reduced to Low or Low-to-Moderate residual levels. However, the transition assessment still identified important gaps in the 2022 control structure. This demonstrates that residual risk maturity and transition readiness are related but not identical.

The second original finding is that transitional risk exposure was concentrated in newly introduced proactive and data-centric controls. Four of the eleven newly introduced controls were not implemented: threat intelligence, information deletion, data masking, and data leakage prevention. These controls had high gap severity because they required new capabilities, not merely revised wording in policies or the SoA. This finding supports the argument that ISO/IEC 27001:2022 transition should be treated as a control-level risk problem rather than as a documentation exercise.

The third original finding is that controls supported by existing operational routines were more transition-ready. Physical security monitoring and monitoring activities were fully implemented because they were already supported by established surveillance, monitoring, or operational evidence. By contrast, controls requiring new data governance or intelligence-driven processes showed weaker readiness. This contrast indicates that transition readiness depends on whether the revised controls can be absorbed into existing operational routines or require new organizational capability.

The fourth original finding is that transition exposure emerged from the interaction among evidence adequacy, ownership clarity, operational integration, supplier dependency, awareness, and SoA alignment. This finding extends the analysis beyond a list of control gaps. For example, a partially implemented control did not necessarily lack all activity; rather, it lacked consistency, formal evidence, testing, or clear integration into governance

processes. Therefore, remediation should focus not only on creating documents, but also on building evidence, ownership, and monitoring mechanisms.

5.2. Findings That Confirm Existing Literature

Several findings confirm existing literature on ISMS and cybersecurity governance. The importance of control ownership and accountability is consistent with prior work on information security governance and the three lines model [11,12]. The need to connect risk assessment with evidence and decision-making is also consistent with critiques of superficial risk-based approaches [13]. In addition, the relevance of supplier governance and awareness aligns with studies on digital banking, FinTech ecosystems, and human factors in security [21,24,27,29,30].

However, the contribution of this paper is not simply to restate that governance, suppliers, or awareness matter. The empirical contribution is to show where these issues appear during ISO/IEC 27001:2022 transition and how they interact with the control-level baseline. In the case of Bank XYZ, governance and evidence problems became visible because newly introduced controls required clearer implementation proof, more specific ownership, and stronger integration with operational processes.

5.3. Bottom-Up Interpretation of the Results

The results suggest three practical lessons. First, organizations should begin ISO/IEC 27001:2022 transition by establishing a verified baseline. In this study, the baseline consisted of 96 risk records, 114 ISO/IEC 27001:2013 controls, 109 implemented or evidenced controls, and a residual risk distribution of 13 Low and 83 Low-to-Moderate risks. Without this baseline, the organization could not distinguish between existing maturity and transition-specific gaps.

Second, organizations should prioritize new controls according to gap severity and operational relevance. In Bank XYZ, the highest-priority controls were threat intelligence, information deletion, data masking, and data leakage prevention because they were not implemented and had high transition relevance. These controls represent a shift toward proactive and data-centric security, which requires technical mechanisms, governance ownership, and repeatable evidence.

Third, the SoA should be treated as a risk governance artifact rather than a static compliance document. The identification of 78 applicable ISO/IEC 27001:2022 controls shows that applicability decisions must be traceable to risk, scope, evidence, and ownership. Weak SoA justification could create apparent compliance while leaving transition exposure unresolved.

5.4. Implications for Banking Institutions

For banking institutions, the findings indicate that ISO/IEC 27001:2022 transition should be managed as a structured risk phase. Banks should not rely only on previous certification, previous residual risk reduction, or high control coverage. Instead, they should create a transition register that links each applicable ISO/IEC 27001:2022 control to evidence, owner, risk relevance, implementation status, and remediation priority.

The case also shows that data-centric controls deserve particular attention. Information deletion, data masking, and data leakage prevention directly affect the protection of sensitive banking information. Their absence may increase exposure in development, testing, operational, and monitoring environments. Similarly, threat intelligence strengthens the organization's ability to anticipate relevant threats rather than only respond to incidents after they occur.

Supplier governance and awareness should also be integrated into the transition roadmap. Because banking controls are distributed across IT, risk management, procurement, compliance, human resources, internal audit, and general affairs, transition readiness requires cross-functional accountability. A control cannot be considered ready unless its owner, evidence, monitoring mechanism, and risk relevance are clear.

5.5. Summary of Discussion

The main implication of the case is that ISO/IEC 27001:2022 migration should not be reduced to control mapping or document revision. The transition creates a distinct exposure condition when the existing ISMS baseline does not fully meet the evidence, ownership, applicability, and operational integration expectations of the revised standard. The findings are most original in showing this distinction empirically through a mature banking ISMS baseline and a control-level assessment of the 2022 transition.

6. Conclusions

This paper examined transitional information security risk exposure during the migration from ISO/IEC 27001:2013 to ISO/IEC 27001:2022 in a banking institution. The case of Bank XYZ shows that a mature ISO/IEC 27001:2013-based ISMS can provide a strong foundation for risk reduction. Within the assessed ISMS scope, the bank implemented or provided evidence for 109 out of 114 controls, while the remaining controls were excluded or considered not applicable to the assessed environment. The bank also reduced 96 inherent risks into lower residual risk levels, indicating that the existing control environment was largely effective within the assessed scope.

The main conclusion is that ISO/IEC 27001:2013 maturity does not automatically eliminate transitional risk exposure. The transition to ISO/IEC 27001:2022 requires re-assessment of control applicability, evidence adequacy, ownership, supplier governance, awareness and training, and the SoA. For banking institutions, the transition should be approached as a risk-driven governance process rather than a documentation update or routine certification exercise.

The paper contributes to the information security governance literature by reframing ISO/IEC 27001:2022 adoption as a transition-risk problem. It also provides a control-level perspective for evaluating readiness in an organization that already appears mature under the previous standard. Practically, the findings suggest that banks should prioritize transition activities based on residual risk, control criticality, supplier dependency, regulatory relevance, and operational impact. Key actions include updating the SoA, mapping ISO/IEC 27001:2013 controls to ISO/IEC 27001:2022, integrating transition gaps into the risk register, clarifying control ownership, strengthening supplier governance, improving role-based awareness and training, conducting readiness audits, and monitoring continual improvement.

7. Limitations and Future Research

The study has several limitations. First, it is based on a single banking institution, so the findings may not represent all banks or financial institutions. Second, the assessment scope is limited to core banking development and operations within data center and disaster recovery center environments. Other banking processes, digital channels, business units, and external service ecosystems may produce different risk patterns.

Third, the analysis relies on qualitative evidence from document review, risk assessment records, control mapping, and stakeholder validation. This approach provides contextual insight, but future studies could strengthen the findings through quantitative maturity measurement, multi-case comparison, or longitudinal evaluation after ISO/IEC 27001:2022 implementation.

Future research may compare transition readiness across multiple banks or financial institutions, develop a quantitative maturity model for ISO/IEC 27001:2022 readiness, or evaluate whether remediation actions after transition reduce exposure over time. Another promising direction is to examine how ISO/IEC 27001:2022 can be integrated with other cybersecurity frameworks, such as the NIST Cybersecurity Framework 2.0, to build a more coherent cybersecurity governance model [18].

Author Contributions: Conceptualization, N.N. and N.L.; methodology, N.N.; validation, N.N. and N.L.; formal analysis, N.N.; investigation, N.N.; resources, N.N.; data curation, N.N.; writing—original draft preparation, N.N.; writing—review and editing, N.N. and N.L.; supervision, N.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Ethical review and approval were waived for this study because the research was a non-interventional organizational information security case study based on institutional documents, information security risk assessment records, control evidence, and limited stakeholder validation for organizational process assessment. The study did not involve clinical procedures, biomedical experimentation, vulnerable participants, customer-level banking data, medical data, or any physical or psychological intervention involving human participants. Stakeholder inputs were used only to validate organizational practices, control interpretation, and risk assessment results. No individual-level responses or personally identifiable participant data are reported in the manuscript. All institutional and stakeholder information was anonymized and presented in aggregated form. The waiver is justified with reference to the relevant Indonesian national legislation, namely Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection, which regulates the protection and processing of personal data and defines personal data as data relating to an identified or identifiable individual. Since the study reports only anonymized and aggregated organizational findings and does not disclose identifiable personal data, the study was considered minimal risk and exempt from formal ethical review.

Informed Consent Statement: Informed consent was obtained from all stakeholders who provided validation input for this study. Participants were informed about the purpose of the study, the voluntary nature of their participation, the confidentiality of the information provided, and the anonymized and aggregated reporting of the results. Stakeholder inputs were used only to validate organizational practices, control interpretation, and risk assessment results. No personally identifiable participant data are reported in this study.

Data Availability Statement: The data supporting the findings of this study are not publicly available due to confidentiality restrictions related to the participating banking institution. Aggregated results are presented in the manuscript. Further information may be available from the corresponding author upon reasonable request and subject to institutional approval.

Acknowledgments: The authors acknowledge the participating institution and stakeholders who supported the validation of the case study evidence.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. World Economic Forum. *The Global Risks Report 2024*; World Economic Forum: Geneva, Switzerland, 2024.
2. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2022.

3. ISO/IEC 27002:2022; Information Security, Cybersecurity and Privacy Protection—Information Security Controls. International Organization for Standardization: Geneva, Switzerland, 2022.
4. ISO/IEC 27000:2018; Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary. International Organization for Standardization: Geneva, Switzerland, 2018.
5. Culot, G.; Nassimbeni, G.; Podrecca, M.; Sartor, M. The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *TQM J.* **2021**, *33*, 76–105. [\[CrossRef\]](#)
6. Podrecca, M.; Culot, G.; Nassimbeni, G.; Sartor, M. Information security and value creation: The performance implications of ISO/IEC 27001. *Comput. Ind.* **2022**, *142*, 103744. [\[CrossRef\]](#)
7. Podrecca, M.; Sartor, M. Forecasting the diffusion of ISO/IEC 27001: A Grey model approach. *TQM J.* **2023**, *35*, 123–151. [\[CrossRef\]](#)
8. Kitsios, F.; Chatzidimitriou, E.; Kamariotou, M. The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. *Sustainability* **2023**, *15*, 5828. [\[CrossRef\]](#)
9. Legowo, N.; Juhartoyo, Y. Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. *J. Syst. Manag. Sci.* **2022**, *12*, 181–199. [\[CrossRef\]](#)
10. ISO/IEC 27001:2013; Information Technology—Security Techniques—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2013.
11. AlGhamdi, S.; Win, K.T.; Vlahu-Gjorgievska, E. Information security governance challenges and critical success factors: Systematic review. *Comput. Secur.* **2020**, *99*, 102030. [\[CrossRef\]](#)
12. Valkenburg, B.; Bongiovanni, I. Unravelling the three lines model in cybersecurity: A systematic literature review. *Comput. Secur.* **2024**, *139*, 103708. [\[CrossRef\]](#)
13. Slapnicar, S.; Axelsen, M.; Eulerich, M. Cyber risk management: An illusion of a risk-based approach. *J. Manag. Control* **2025**. [\[CrossRef\]](#)
14. Reuben-Owoh, B.; Haig, E. A systematic review of voluntary cybersecurity standards and frameworks. *Int. J. Inf. Secur.* **2025**, *24*, 206. [\[CrossRef\]](#)
15. ISO 31000:2018; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018.
16. National Institute of Standards and Technology. *Guide for Conducting Risk Assessments*; NIST Special Publication 800-30 Revision 1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2012. [\[CrossRef\]](#)
17. McIntosh, T.R.; Susnjak, T.; Liu, T.; Watters, P.; Xu, D. From COBIT to ISO 42001: Evaluating cybersecurity governance, risk and compliance frameworks for opportunities, risks and regulatory compliance in large language models. *Comput. Secur.* **2024**, *144*, 103958. [\[CrossRef\]](#)
18. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*; NIST Cybersecurity White Paper 29; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2024. [\[CrossRef\]](#)
19. Webb, J.; Ahmad, A.; Maynard, S.B.; Shanks, G. A situation awareness model for information security risk management. *Comput. Secur.* **2014**, *44*, 1–15. [\[CrossRef\]](#)
20. Shedden, P.; Ahmad, A.; Smith, W.; Scheepers, R. Asset identification in information security risk assessment: A business practice approach. *Commun. Assoc. Inf. Syst.* **2016**, *39*, 297–314. [\[CrossRef\]](#)
21. Herath, T.; Rao, H.R. Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* **2009**, *18*, 106–125. [\[CrossRef\]](#)
22. Siponen, M.; Willison, R. Information security management standards: Problems and solutions. *Inf. Manag.* **2009**, *46*, 267–270. [\[CrossRef\]](#)
23. Spears, J.L.; Barki, H. User participation in information systems security risk management. *MIS Q.* **2010**, *34*, 503–522. [\[CrossRef\]](#)
24. Ifinedo, P. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Inf. Manag.* **2014**, *51*, 69–79. [\[CrossRef\]](#)
25. Kor, B.; Metin, B. Understanding human aspects for an effective information security management implementation. *Int. J. Appl. Decis. Sci.* **2021**, *14*, 105–122. [\[CrossRef\]](#)
26. Arif, M.; Badila, M.; Warden, J.M.; Ur Rehman, A. A study of human factors toward compliance with organization's information security policy. *Inf. Secur. J. Glob. Perspect.* **2025**, *34*, 235–250. [\[CrossRef\]](#)
27. AlBenJasim, S.; Takruri, H.; Al-Zaidi, R.; Dargahi, T. Development of cybersecurity framework for FinTech innovations: Bahrain as a case study. *Int. Cybersec. Law Rev.* **2024**, *5*, 501–532. [\[CrossRef\]](#)
28. Azura, Y.T.Y.; Azad, M.A.; Ahmed, Y. An integrated cyber security risk management framework for online banking systems. *J. Bank. Financ. Technol.* **2025**, *9*, 85–104. [\[CrossRef\]](#)
29. Gounari, M.; Stergiopoulos, G.; Pipyros, K.; Gritzalis, D. Harmonizing open banking in the European Union: An analysis of PSD2 compliance and interrelation with cybersecurity frameworks and standards. *Int. Cybersec. Law Rev.* **2024**, *5*, 79–120. [\[CrossRef\]](#)
30. Shafie, E.; Alharthi, A.; Alsaedi, A.; Alharthi, M. Securing mobile banking in Saudi Arabia: Key insights on confidentiality, authentication and device trust. *Discov. Internet Things* **2025**, *5*, 75. [\[CrossRef\]](#)
31. Otoritas Jasa Keuangan. *Peraturan Otoritas Jasa Keuangan Nomor 18/POJK.03/2016 Tentang Penerapan Manajemen Risiko bagi Bank Umum*; Otoritas Jasa Keuangan: Jakarta, Indonesia, 2016.

32. Pemerintah Republik Indonesia. *Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik*; Pemerintah Republik Indonesia: Jakarta, Indonesia, 2019.
33. Badan Siber dan Sandi Negara. *Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik*; Badan Siber dan Sandi Negara: Jakarta, Indonesia, 2020.
34. Yin, R.K. *Case Study Research and Applications: Design and Methods*, 6th ed.; SAGE Publications: Thousand Oaks, CA, USA, 2018.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.