JPPIPA 12(4) (2026)

Jurnal Penelitian Pendidikan IPA

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

Information Security Architecture for Pesantren: The Synergy of ISO/IEC 27001 and TOGAF ADM in Supporting Sustainable Quality Education

Yussrizal Asygaf[1*], Dinar Mutiara Kusumo Nugraheni[1], Oky Dwi Nurhayati[1]

[1] Postgraduate Diponegoro University, Semarang City, Indonesia.

Received: February 02, 2026
Revised: March 05, 2026
Accepted: April 25, 2026
Published: April 30, 2026

Corresponding Author:
Yussrizal Asygaf
yussrizalasygaf@students.undip.ac.id

DOI: 10.29303/jppipa.v12i4.14712

Abstract: Digital transformation in Islamic boarding schools (pesantren) presents new challenges in protecting information assets and student data privacy. This study aims to perform an information security analysis in a pesantren currently undergoing a crucial digital transition, aligned with the institutional vision to implement digital administrative services and science-and-technology-based learning. The research methodology integrates the ISO/IEC 27001:2022 information security standard as an audit instrument into the TOGAF ADM framework, limited to Phase D (Technology Architecture). This approach aims to establish a foundational infrastructure and critical technical governance that complies with security standards prior to the architecture implementation phase. A selection of 41 security controls was made through asset identification and risk assessment to represent the specific operational needs of the pesantren for effective mitigation. Research findings reveal significant gaps in identity management, backup protocols, and cryptography, stemming from a governance approach that remains reactive. This study concludes that strengthening information security through policy standardization, the implementation of Role-Based Access Control (RBAC), and data recovery procedures is urgent to ensure the integrity and sustainability of digital services. The synergy between regulatory compliance and resilient technology architecture serves as the primary determinant in protecting data sovereignty within traditional educational institutions.

Keywords: Information security; ISO/IEC 27001:2022; Pesantren; Risk analysis; Togaf ADM

Introduction

The evolution of Islamic boarding schools (pesantren) in Indonesia has shifted from a traditional model toward modern pesantren, which historically emphasizes the integration of general curricula, classical systems, and the mastery of information technology. However, in this decade, a significant distinction has emerged between institutions that are merely modern in curriculum and those that actively implement information technology by digitalizing the education service cycle (Hadita et al., 2023). Pesantren adopting information technology go further by integrating complex student data management—ranging from admissions to academic and health records—to enhance institutional quality. This development shows that institutions like the XYZ Foundation in East Java, one of the largest pesantren in Indonesia, no longer focus solely on academic updates but are beginning to face information system integration challenges across various branches, demanding reliable enterprise architecture (Mof et al., 2026). Nevertheless, the higher the dependence on internet-connected services, the greater the security risks overshadowing information data and student privacy (Kusuma et al., 2021).

How to Cite:
Asygaf, yussrizal, Nugraheni, D. M. K., & Nurhayati, O. D. (2026). Information Security Architecture for Pesantren: The Synergy of ISO/IEC 27001 and TOGAF ADM in Supporting Sustainable Quality Education. *Jurnal Penelitian Pendidikan IPA*, *12*(4), 333–344. https://doi.org/10.29303/jppipa.v12i4.14712

The implementation of technologies such as Massive Open Online Courses (MOOCs) platforms and Artificial Intelligence (AI)-based evaluation systems demonstrates that digitalization can significantly increase engagement and academic performance (Warsihna et al., 2026). However, the integration of such advanced technology also opens new risk gaps. The large-scale use of digital tools without strict security oversight can threaten institutional data integrity; thus, awareness of information asset protection and resource capability is required from the digitalization planning stage.

Information system development in pesantren aims not only to support daily operations but also to strengthen competitiveness in facing globalization. With a robust information system, pesantren can focus more on their primary mission: educating the younger generation in both religious and general sciences in a balanced manner (Petrov et al., 2022). Furthermore, a sound system will enhance transparency and accountability in resource management, ultimately increasing public trust.

In implementing information systems, selecting the right method is vital (Mubarak et al., 2023). One relevant framework is TOGAF (The Open Group Architecture Framework) Version 10. TOGAF provides structured guidance from the planning to the evaluation stage, enabling pesantren to build information systems that are reliable and adaptive to change (Petrov et al., 2022).

Beyond architectural aspects, information security based on the ISO/IEC 27001:2022 standard is a crucial consideration. This standard focuses on an information security management system that covers protection against both internal and external threats. Given the sensitivity of student, teacher, and institutional data, this standard ensures the integrity, confidentiality, and availability of data. This is essential for pesantren to maintain credibility in the eyes of stakeholders, such as parents, donors, and partners (Mirtsch et al., 2026).

ISO/IEC 27001:2022 serves as a comprehensive information security management solution to address these challenges. The standard does not focus solely on technology but also touches on organizational and personnel aspects, which are highly relevant to the unique structure of pesantren. By adopting security controls aligned with the latest technological developments—such as web-based learning record platforms—pesantren can ensure that every implemented digital innovation remains within strict data protection corridors (Anjarwati et al., 2025; Khairani et al., 2025). Compliance with this standard provides assurance that digital transformation is conducted responsibly and sustainably.

The urgency of information security becomes more apparent with the use of data-based learning media such as Augmented Reality (AR) and QR Codes, which are now penetrating primary and secondary schools (Billa & Restian, 2026; Ibrahim et al., 2025). Students' personal data and academic track records stored in application-based systems, such as "smart point" apps or school management systems, are highly valuable assets (Khairunnisa et al., 2025). Without standard security protocols, this sensitive data is vulnerable to cyberattacks that could damage the institution's credibility as a trusted Islamic educational institution.

This massive digital transformation essentially creates an urgent need for strict information security standards like ISO/IEC 27001:2022 to protect sensitive student data and maintain institutional credibility (Istutik et al., 2023). Therefore, pesantren require a measurable methodology to secure their digital ecosystem through the following steps:

First Stage: Internal Audit and Observation Procedures. Before formulating rules, administrators must capture the actual field conditions (Astutik et al., 2025). This analysis includes the Organizational Structure by understanding the bureaucratic chain from the Leader (Kyai) and the Council of Elders (Dewan Masyayikh) to the daily staff operating computers. Computing Usage involves documenting system utilization, storage media like local servers, internet connectivity within the campus, and smartphone usage by teachers or staff. Process Dependency includes assessing how fatal a system shutdown would be—for instance, if the financial database is hacked, whether teaching and learning activities can still proceed.

Second Stage: Analysis of Actual Conditions. Using the ISO/IEC 27001 standard allows for the identification of information security risks in the applied technology, while the TOGAF ADM framework enables more efficient IT implementation that complies with security standards (Alier et al., 2021). It is noted that the broader the scope forced without infrastructure and human resource readiness, the greater the security risks. ISO/IEC 27001 is positioned in the literature as a certifiable standard to establish, implement, and maintain an Information Security Management System (ISMS) through systematic risk assessment and control application (Wijaya et al., 2024). ISO 27001:2022 implementation studies emphasize structured risk management through identification, analysis, evaluation, and mitigation.

Third Stage: Formulation of Recommendations and Security Policies (Wijaya et al., 2024). Formulated policies must be able to protect assets from external threats (hackers) and internal negligence (accidental staff errors). Mandatory points include: Confidentiality & Integrity: Ensuring data does not leak to unauthorized parties and avoiding information errors that could compromise institutional integrity. HR Education:

Providing training to administrators and teachers on aligning IT with teaching activities and ensuring they do not carelessly click phishing links or share admin passwords. Incident Response: Having clear procedures if the system is hit by ransomware or if social media accounts are hijacked. Legal Compliance: Following government regulations, such as the Personal Data Protection Act (UU PDP).

Challenges in implementation often appearing in pesantren involve policies that exist only "on paper." Frequently, new applications or technologies are inserted into activities without security evaluation. Furthermore, many policies are not socialized to students and staff, leading to the rules being perceived as non-existent (Mubarak et al., 2023). Given the limited expert personnel, a deep understanding of core principles must be instilled. Security as Continuous Riadhah (Exercise) means that information security is not a one-time setup but a continuous process that requires discipline, similar to maintaining istiqomah (consistency) in worship (Ma'arif et al., 2026). Large pesantren may afford to build internal IT teams, but for small-to-medium institutions, it is highly recommended to adopt existing security standards (such as using legal software and standard encryption) rather than building custom systems prone to vulnerabilities (Hadi et al., 2025).

Moreover, pesantren in this transformation process are faced with a lack of formal frameworks for technology risk management. As seen in various digital media developments, the main focus is often only on the validity and practicality of materials (Sari et al., 2025). In fact, technical aspects such as the use of Machine Learning and Hybrid Models for performance prediction or data management require a strong security foundation to prevent information leakage (Subangkit et al., 2026). Thus, the application of international standards becomes absolutely necessary as a strategic guide in mitigating information security risks.

Finally, this research offers novelty through the systematic integration of ISO/IEC 27001:2022 security standards and the TOGAF ADM enterprise architecture framework up to Phase D, specifically applied to the pesantren ecosystem (Ma'arif et al., 2026). Unlike previous studies that tend to separate risk analysis from architectural design, this study synergizes ISO management clauses and technical controls directly into the business, data, and application architecture domains to produce more applicable recommendations. The synergy between TOGAF ADM and ISO 27001:2022 controls also serves as an instrument for compliance with Indonesia's Personal Data Protection Act (UU PDP). This ensures that personal data governance is conducted through a systematic approach (Rambau et al., 2026). This is crucial as PDP regulations require a clear governance structure, allowing risk mitigation against internal negligence and external threats to be handled through standardized operational procedures and adaptive organizational adjustments.

Additionally, the originality of this research lies in the adaptation of international standards to the unique characteristics of pesantren as traditional educational institutions undergoing digital transformation, using a worst-case scenario score recapitulation approach to identify the highest vulnerability points in sensitive student data and institutional operations.

Method

This study adopts the Plan-Do-Check-Act (PDCA) methodology (Wijaya et al., 2024) as its theoretical foundation. This approach is crucial to ensure that the development of the Information Security Management System (ISMS) is not only structured but also systematically improved over time to address dynamic threats. In its implementation, this research simultaneously synergizes two primary frameworks: the ISO/IEC 27001:2022 standard and the TOGAF ADM framework. This integration process is carried out through data confirmation stages that align technical security controls with the organization's business architecture strategy (Geasela & Legowo, 2022).

An in-depth analysis of secure system requirements will help pesantren not only succeed in technological innovation but also maintain the sovereignty of Islamic educational information. By referencing best practices in educational technology development and the ISO/IEC 27001:2022 standard, pesantren are expected to become modern, competitive, and secure institutions amidst the massive wave of digital transformation (Akobiarek et al., 2026; Lusiani et al., 2026).

Implementation of ISO/IEC 27001:2022 Standard

The application of the ISO/IEC 27001:2022 standard is carried out rigidly in accordance with international requirements, which consist of two major parts: the initial section or clauses comprising 10 clauses, and the second section, Annex A, which consists of 93 controls (Rambau et al., 2026).

In this study, ISO/IEC 27001:2022 serves as the primary instrument to measure the extent of information security readiness and compliance within the pesantren environment. This standard consists of 10 main clauses implemented gradually. Clauses 1 to 3 are used as the baseline to describe the organizational scope, normative references, and terms and definitions relevant to the pesantren context. The primary focus is then placed on Clauses 4 to 10, which function to assess the current direction of information security governance. This section covers strategic aspects ranging from

organizational context, leadership, planning, support, and operation to performance evaluation and continuous improvement (Alfitrah & Leegowo, 2026). Once the governance direction is analyzed through these clauses, the next stage is to conduct a deeper assessment of technical aspects using Annex A of ISO/IEC 27001:2022. At this stage, questionnaire instruments are utilized to evaluate the organization's technical maturity. These questionnaires are designed to capture the actual implementation of existing security controls, ensuring that the results do not merely describe administrative policy conditions but also reflect the technical effectiveness of data and information asset protection in the field (Min & Kwak, 2025).

Implementation of the TOGAF ADM Framework

In parallel, this study utilizes the Architecture Development Method (ADM) from TOGAF Version 10 to design a reliable information system architecture (Alier et al., 2021). The architectural development is conducted through the following phases: Phase A (Architecture Vision): Defining the research scope, identifying key stakeholders, and aligning the architectural vision with the strategic goals of the pesantren. Phase B (Business Architecture): Defining business strategies, governance, and existing business processes to understand how information flows within the institution. Phase C (Information System Architecture): Conducting an in-depth analysis of the data architecture and application architecture domains used to support educational operations. Phase D (Technology Architecture): Determining the physical infrastructure, hardware, and software required to support a secure information management system (Al Omari et al., 2024; Rahmadani et al., 2024).

Limiting the use of TOGAF ADM to Phase D (Technology Architecture) is a logical strategic step, as these early phases provide the crucial foundation for defining the gap analysis between current governance and the target secure architecture before moving toward implementation stages that require significant resource investment. This aligns with the principles of efficiency in enterprise architecture development, where focusing on the baseline through to the technology architecture is sufficient to generate comprehensive and actionable security blueprints for educational institutions undergoing digital transition (Hardi & Legowo, 2023).

Through the synergy between these two methods, the research is divided into three main stages (as depicted in the research procedure diagram):

Framework Identification and Mapping Stage: The research begins with the "Start" process, immediately followed by the Planning Identification phase. In this phase, researchers conduct initial data collection using Observation and Interview methods to understand existing field conditions (Fray & Wiliński, 2024). The results of this identification serve as the basis for fulfilling procedures from the Preliminary Phase to Phase A of the TOGAF framework, alongside Framework Mapping by selecting relevant Annex A controls from the ISO/IEC 27001 standard.

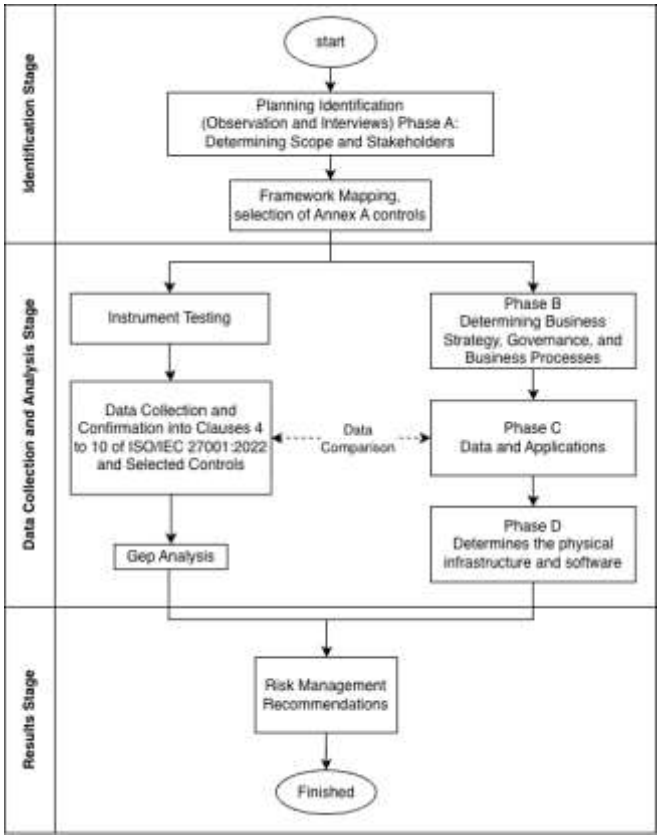

Figure 1. Research flow

Data Collection and Development Stage: Once the framework is mapped, the research splits into two concurrent mechanisms: Instrument Testing Path: Ensuring that the research measurement tools or questionnaires are understandable to the pesantren staff, who serve as the respondents (Djebbar & Nordstrom, 2023). After the instrument is validated, Data Collection and Confirmation are conducted for ISO/IEC 27001:2022 Clauses 4 to 10 and the selected controls. Framework Path (Phase B–D): In parallel, an in-depth analysis is performed using the Architecture Development Method (ADM) (Lattu et al., 2022). There is technical information exchange between the ISO standard data collection and Phase C (Data/Application Architecture) to determine the physical infrastructure and software required to support the system in Phase D.

Final Formulation Stage: After all data is analyzed, gaps identified, and the architectural design established, the research enters the final stage to formulate Risk Management Recommendations. These

recommendations serve as a strategic guide for the organization in managing information security risks based on the findings from the previous stages. The research concludes (Finished) once these recommendations have been compiled.

Table 1. Research format

Stage	ISO/IEC	Togaf
Stage 1	Initiation & Planning; Review of ISMS policies, procedures, and legality documents.	Preliminary; Phase A: Architecture Vision
Stage 2	Document Review; Fieldwork/Execution	Phase B: Business Architecture; Phase C: Information Systems Architecture; Phase D: Technology Architecture
Stage 3	Findings Analysis; Reporting	

Result and Discussion

Results

Based on the data collection results from observations and in-depth interviews, the analysis of the 10 mandatory ISO/IEC 27001:2022 clauses indicates that the pesantren is currently in a digital transition phase that requires governance reinforcement. Identification within the organizational context and leadership clauses reveals that although a technology-based management vision has been launched, the formal scope of the Information Security Management System (ISMS) has not yet been fully defined to protect critical information assets (Nelson et al., 2025). This aligns with the findings in the Preliminary Phase and Phase A (Architecture Vision) of the TOGAF ADM, where synergy between stakeholder needs and documented information security policies still requires strategic alignment to ensure operational continuity (Maulana et al., 2023).

In gathering information regarding the Initiation & Planning and the review of ISMS policies, procedures, and legal documents—integrated with the procedural checklists found in the Preliminary and Architecture Vision phases—41 ISO/IEC 27001:2022 Annex A controls were identified (Table 2). These controls are distributed across various categories (Organizational, People, Physical, and Technological Controls) and will undergo technical implementation confirmation through questionnaires distributed to relevant stakeholders, namely: the Director (R1), the New Student Admissions Division Staff or PSB Admin (R2), the Ubudiyah/Academic Division Staff or Diniah Admin (R3), the Developer or Programmer responsible for building the information systems (R4), and the General Admin covering various divisional administration fields (R5). The results of this classification serve as the foundation for conducting a Gap Analysis to assess the extent to which daily technical operations meet the desired security standards.

Table 2. Selected control

Control Classification	Selected Control
5 Organizational controls	5.1 5.2 5.3 5.4 5.5 5.6 5.9 5.12 5.15 5.16 5.18 5.23 5.24 5.26 5.27 5.32
6 People controls	6.2 6.3 6.4 6.8
7 Physical controls	7.1 7.3 7.4 7.6 7.9 7.10 7.11 7.13
8 Technological controls	8.2 8.3 8.5 8.12 8.13 8.15 8.16 8.19 8.20 8.21 8.26 8.28 8.32

Control Selection

Control classification consists of the selected points from Annex A that will be translated into audit and interview questionnaire instruments to measure the organization's existing conditions (Table 2: Selected Controls).

Organizational Controls: (5.01) Policies for information security, (5.02) Information security roles and responsibilities, (5.03) Segregation of duties, (5.04) Management responsibilities, (5.05) Contact with authorities, (5.06) Contact with special interest groups, (5.09) Inventory of information and other associated assets, (5.12) Classification of information, (5.15) Access control, (5.16) Identity management, (5.18) Access rights, (5.23) Information security for use of cloud services, (5.24) Information security incident management planning and preparation, (5.26) Response to information security incidents, (5.27) Learning from information security incidents, (5.32) Intellectual property rights. People & Physical Controls: (6.02) Terms and conditions of employment, (6.03) Information security awareness, education and training, (6.04) Disciplinary process, (6.08) Reporting information security events, (7.01) Physical security perimeters, (7.03) Securing offices, rooms and facilities, (7.04) Physical security monitoring, (7.06) Working in secure areas, (7.09) Security of assets off-premises, (7.10) Storage media, (7.11) Supporting utilities, (7.13) Equipment maintenance. (8.02) Privileged access rights, (8.03) Information access restriction, (8.05) Secure authentication, (8.12) Data leakage prevention, (8.13) Information backup, (8.15) Logging, (8.16) Monitoring activities, (8.19) Installation of software on operational systems, (8.20) Network security, (8.21) Security of network services, (8.26) Application security requirements, (8.28) Secure coding, (8.32) Change management.

Following the determination of relevant control points through the synchronization of ISO/IEC 27001:2022 and TOGAF ADM, the next step is to develop a structured research instrument in the form of a

questionnaire. Each selected security control is broken down into specific question items, which then undergo expert judgment review to ensure the instrument is understandable to respondents while accurately capturing field conditions. In this structure, each control is represented by two specific questions distributed to different respondents, tailored to the sub-sections and functional roles of each stakeholder. This approach aims to obtain double verification and a more objective perspective from various operational lines of the pesantren regarding the same security parameters.

Questionnaire Results

The following results were obtained from the questionnaire distribution. The distribution was conducted in a targeted manner, providing specific questions to respondents while taking into account the selected sub-controls.

Table 3. Questionnaire results for each question

Q	A1	V1	T1	A2	V2	T2
5.1	R1	5	5	R5	3	5
5.2	R2	4	5	R1	3	5
5.3	R1	5	5	R4	3	5
5.4	R1	3	5	R5	5	5
5.5	R5	5	5	R1	5	5
5.6	R4	2	5	R5	2	5
5.9	R5	4	5	R4	4	5
5.12	R2	5	5	R3	5	5
5.15	R2	5	5	R4	3	5
5.16	R5	1	5	R4	3	5
5.18	R1	3	5	R3	5	5
5.23	R4	1	5	R5	5	5
5.24	R4	2	5	R5	1	5
5.26	R2	5	5	R4	2	5
5.27	R1	4	5	R4	2	5
5.32	R5	3	5	R3	5	5
6.2	R1	5	5	R5	3	5
6.3	R3	2	5	R2	5	5
6.4	R1	3	5	R5	5	5
6.8	R3	5	5	R2	4	5
7.1	R5	5	5	R5	5	5
7.3	R5	1	5	R2	5	5
7.4	R5	4	5	R1	3	5
7.6	R3	5	5	R2	3	5
7.9	R5	5	5	R4	3	5
7.10	R5	1	5	R4	3	5
7.11	R5	5	5	R4	3	5
7.13	R4	4	5	R5	3	5
8.2	R4	5	5	R4	1	5
8.3	R4	5	5	R2	4	5
8.5	R4	1	5	R3	2	5
8.12	R4	1	5	R2	5	5
8.13	R4	1	5	R5	1	5
8.15	R4	1	5	R4	2	5
8.16	R4	1	5	R4	5	5
8.19	R5	2	5	R4	5	5
8.20	R4	2	5	R4	5	5
8.21	R1	5	5	R4	2	5
8.26	R4	1	5	R4	5	5
8.28	R4	3	5	R4	2	5
8.32	R4	3	5	R5	5	5

Legend:
Q = Question based on Control
R = Respondent
A = Answer
V = Answer Score
T = Target Score

The measurement of compliance levels in the questionnaire (Table 3: Questionnaire Results) utilizes a Likert scale ranging from 1 to 5, where a score of 1 represents a "very poor" condition and a score of 5 indicates a "very good" condition. During the distribution process, it was observed that several respondents selected a score of 1 due to a lack of knowledge regarding the context or technical substance of the questions. The researchers assume this lack of awareness as an indication of low security policy penetration within that specific unit.

GAP Analysis

Once the data was collected, a score recapitulation was performed using the worst-case scenario principle. In this method, the lowest value from the total questionnaire scores is taken as the final representation of each control. This is based on the understanding that the minimum score reflects the vulnerability point or the highest risk value requiring mitigation priority, as presented in Table 4.

The analysis of the information security level at the Pesantren was conducted by measuring the gap between the actual condition and the target condition. In this measurement, each security control is represented by two question items. Therefore, the total actual score for a single control is obtained by summing the scores of both questions. Correspondingly, the target value is also multiplied by two to align with the number of questions per control. The gap value is then calculated using the formula for the difference between the target value and the total actual score (Gap Value = Target Value – Total Score). To provide an overview of the vulnerability level, the gap results are grouped into three risk classification categories that determine the priority for information security handling.

The classification in Table 4 serves as an evaluation instrument for information technology managers within the Pondok Pesantren environment. A higher gap value indicates that the implementation of information security controls is still far from the established standards, thereby increasing potential threats to data integrity, confidentiality, and availability (Maradova et

al., 2026). With this categorization, the pesantren administration can map out mitigation priorities, starting with controls in the "High Risk" category to minimize the impact of future losses.

Table 4. GAP category

GAP Score Range	Category	Interpretative Description
0–2	Safe	Security controls have been well-implemented and are close to the expected targets.
3–4	Medium Risk	There are security gaps that need attention and require periodic improvement.
5–10	High Risk	There are significant gaps that require immediate corrective action to protect pesantren data.

Table 5. High risk classification

Control	Total Target Score	Total Score Actual	GAP Score
8.13 Information Backup	10	2	8
5.24 Information Security Incident Management Planning and Preparation	10	3	7
8.5 Secure Authentication	10	3	7
8.15 Recorded Login Activity	10	3	7
5.6 Contact with Special Interest Groups	10	4	6
5.16 Identity Management	10	4	6
7.10 Storage Media	10	4	6
8.28 Secure Encryption	10	5	5

Analysis of High-Risk Category Findings (Gap 5–10)

The results of the gap analysis conducted through the questionnaire indicate that several information security controls fall into the High Risk category. These findings are a direct reflection of the governance conditions identified during the identification and preliminary stages, where the organization currently lacks a dedicated Enterprise Architecture unit and formally documented information security policies as required by Clause 5 of ISO/IEC 27001:2022. The absence of this structure results in high risks for controls 5.6 (Contact with Special Interest Groups), 5.16 (Identity Management), and 5.24 (Information Security Incident Management). Strategically, this proves that IT management within the pesantren remains reactive and heavily dependent on internal habits (trust-based); consequently, coordination with external parties and response planning for security incidents lack systematic, standard procedures within the Preliminary Phase of the TOGAF ADM framework.

At a more detailed operational level, these high-risk findings align with the Baseline Business Architecture conditions. The significant gaps in controls 7.10 (Storage Media) and 8.13 (Information Backup) are a tangible impact of using storage media, such as spreadsheets, which lack consistent security measures and centralized backup procedures within an Architecture Repository. These risks are particularly critical for sensitive work units, such as the PSB (Admissions) Division and the Finance Division, which manage students' personal data. Furthermore, risk findings in technical controls such as 8.5 (Secure Authentication), 8.15 (Logging Activity), and 8.28 (Secure Coding/Encryption) confirm that the institutional vision to protect student data confidentiality has not yet been transformed into operational technical architecture principles.

Table 6. Moderate risk classification

Control	Total Target Score	Total Score Actual	GAP Score
5.23 Information security for use of cloud services	10	6	4
5.27 Learning from information security incidents	10	6	4
7.3 Securing offices, rooms and facilities	10	6	4
8.2 Privileged access rights	10	6	4
8.12 Data leakage prevention	10	6	4
8.16 Monitoring activities	10	6	4
8.26 Application security requirements	10	6	4
5.2 Information security roles and responsibilities	10	7	3
5.26 Response to information security incidents	10	7	3
6.3 Information security awareness, education and training	10	7	3
7.4 Physical security monitoring	10	7	3
7.13 Equipment maintenance	10	7	3
8.19 Installation of software on operational systems	10	7	3
8.20 Networks security	10	7	3
8.21 Security of network services	10	7	3

As a solution to mitigate these risks, the results of this analysis serve as the basis for designing the Target Business Architecture. Improvement efforts are focused on the implementation of Role-Based Access Control (RBAC), robust password policies, and database

encryption for high-risk services, such as the new student registration system. These steps are organized into a Business Architecture Roadmap within Phase B of the TOGAF ADM to ensure that every control selected in the Statement of Applicability (SoA) can be integrated into the pesantren's business services. Thus, the synchronization between governance and operational procedures becomes the primary key to closing the security gaps that currently threaten the sustainability of educational services within the pesantren environment.

Findings in the Medium Risk category indicate that security implementation efforts are already underway but remain undocumented and lack comprehensive integration within the organizational structure. Organizational and people-oriented controls—such as security roles and responsibilities, awareness through training, and the use of cloud services—reflect an IT management condition that is currently purely operational and centralized within the IT staff, without formal separation of oversight functions. This gap aligns with the early-stage analysis, which found that the pesantren's business principles of maintaining traditional values alongside science and technology have not yet been fully translated into standardized technical policies. Consequently, security incident responses and the learning processes derived from such events remain ad-hoc, even though a basic organizational structure and several IT management mandates are already in place.

Regarding physical and technological controls, the medium risks detected in facility protection, network security, and data leakage prevention are closely linked to the business process mapping of the administrative, academic, and financial units. The use of integrated platforms for various student operational modules demands security mechanisms such as privileged access rights and stricter activity monitoring; however, current human resource capability constraints result in these controls being suboptimal. The results of this analysis validate the need to strengthen the business architecture by drafting documented data backup and recovery procedures, as well as utilizing non-disclosure agreements (NDAs) for relevant personnel. Integrating these audit results with the architectural development plan ensures that every business service—from registration to financial systems—has a systematic risk mitigation foundation aligned with global information security standards.

Findings in the low-risk or "safe" category indicate that the organization has established a solid foundation in terms of basic policy, legality, and initial division of duties. Controls such as information security policies, relations with authorities, and intellectual property rights management reflect the pesantren's strategic vision, which recognizes the importance of defining the boundaries for implementing an information security management system. The success in maintaining low risk regarding asset inventory and basic information classification proves that stakeholder identification—ranging from the leadership (pengasuh) to administrative staff—has effectively defined the scope of data protection. This provides a stable footing for further architectural development, as work boundaries and architectural deliverables already possess a sufficient legal basis and leadership commitment.

Table 7. Low risk classification

Control	Total Target Score	Total Score Actual	GAP Score
5.1 Policies for information security	10	8	2
5.3 Segregation of duties	10	8	2
5.3 Management responsibilities	10	8	2
5.9 Inventory of information and other associated assets	10	8	2
5.15 Access control	10	8	2
5.18 Access rights	10	8	2
5.32 Intellectual property rights	10	8	2
6.2 Terms and conditions of employment	10	8	2
6.4 Disciplinary process	10	8	2
7.6 Working in secure areas	10	8	2
7.9 Security of assets off-premises	10	8	2
7.11 Supporting utilities	10	8	2
8.32 Change management	10	8	2
6.8 Information security event reporting	10	9	1
8.3 Information access restriction	10	9	1
5.5 Contact with authorities	10	10	0
5.12 Classification of information	10	10	0

On the operational dimension, the safe category achieved in physical controls and change management shows that the internal culture for maintaining work areas and employee discipline is well-established. Capability assessments at the foundational level have proven effective in supporting physical access control and off-site asset security, aligning with organizational efforts to maintain the sustainability of educational services. In the context of business architecture, stability in aspects such as security event reporting and employment contract requirements indicates that core business processes within administrative units have consistent daily procedures in place. This safe condition

allows the organization to focus its resources and architectural development roadmap on more complex technical transformations without having to rebuild the administrative foundations that are already functioning well.

Discussion

The analysis results indicate that the Pondok Pesantren is currently in a digital transition phase characterized by a strong administrative foundation but remaining vulnerable at the technical layers and formal governance. The organization's success in achieving the "Safe" category in basic policy controls, physical perimeters, and legal aspects demonstrates that a trust-based culture and leadership commitment have become the primary capital in maintaining educational service continuity. This aligns with the Preliminary and Phase A stages of TOGAF ADM, where the organizational vision of preserving traditional values runs parallel with compliance with operational boundaries. However, safety at the administrative level is insufficient to face modern cyber threats if it is not promptly transformed into more standardized technical policies.

Significant gaps found in the "High Risk" category, particularly regarding Identity Management, Backup, and Encryption, underscore a disconnect between macro business principles and micro-technological implementation. These findings indicate that while the vision for student data protection has been established, the absence of a dedicated Enterprise Architecture unit and an Architecture Board results in IT security controls that remain reactive and operational. From the perspective of ISO/IEC 27001:2022, these risks are a consequence of not yet implementing systematic risk management (Clause 6.1). Therefore, integrating security audit results into the Business Architecture becomes a crucial step to ensure that critical services, such as New Student Admissions (PSB) and financial management, possess data resilience tested through Role-Based Access Control (RBAC) mechanisms and formal disaster recovery procedures.

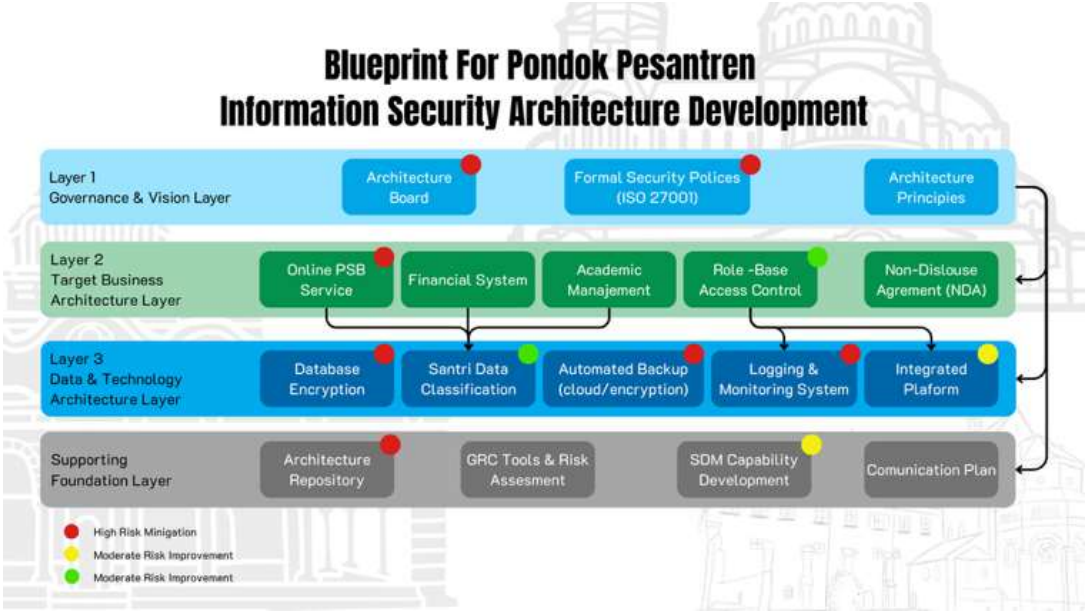

Figure 2. Blueprint information security architecture

Overall, this study recommends an architectural transformation focusing on strengthening the centralized architecture repository to resolve issues related to scattered documentation. The development roadmap, structured up to TOGAF ADM Phase D, must prioritize the mitigation of high-risk controls through security automation and human resource capability enhancement. By aligning every pesantren business service with the Statement of Applicability (SoA), the organization not only meets ISO compliance standards but also builds an information system architecture that is resilient, efficient, and remains in harmony with the noble values of pesantren education. This synergy between governance, people, and technology will serve as a future blueprint for traditional educational institutions facing the challenges of massive digital transformation.

Conclusion

This study concludes that pondok pesantren are currently in a crucial digital transition phase, where a strong administrative foundation must be promptly accompanied by the reinforcement of formal

information security governance. The synergy between the ISO/IEC 27001:2022 standard and the TOGAF ADM 10 framework has proven effective in identifying vulnerability points in critical information assets, while simultaneously serving as an instrument for compliance with national regulations such as the Personal Data Protection Act (UU PDP). Evaluation results indicate that the absence of organizational structures, such as an Architecture Board, causes technology management to remain reactive; therefore, transforming from a trust-based security model to a standardized technical policy-based model is an urgent necessity to maintain institutional credibility. The implementation of information security within the pesantren environment must be viewed as a continuous process—or Riadhah—that harmoniously integrates technology, organization, and personnel. The strategic recommendations generated through this research up to TOGAF ADM Phase D provide concrete guidance for the institution to mitigate high risks, such as student data leaks, through the strengthening of architecture repositories and the automation of technical controls. By adopting a resilient and adaptive architectural blueprint, pondok pesantren will not only be able to protect the sovereignty of Islamic educational information from modern cyber threats but also enhance the transparency and accountability of digital services in the eyes of all stakeholders.

Acknowledgments

The author would like to express his deepest gratitude to all parties who have provided support and contributions to this research. Special thanks are extended to Dinar Mutiara Kusumo Nugraheni, S.T., M.InfoTech.(Comp)., PhD. and Dr. Oky Dwi Nurhayati, S.T., M.T. Furthermore, the author thanks Diponegoro University for their encouragement and support throughout the research process.

Author Contributions

Conceptualization, writing—original draft preparation, Y.A.; methodology, writing—review and editing, supervision, D.M.K.N. and O.D.N. All authors have read and agreed to the published version of the manuscript.

Funding

This research received no external funding.

Conflicts of Interest

he authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Akobiarek, M. N. R., Hariyadi, S., Indrawati, I., & Tanta, C. (2026). Profile of Basic Teaching Skills of Prospective Biology Teachers: A Video-Based Longitudinal Study in a Microteaching Course (2020–2023). *Jurnal Penelitian Pendidikan IPA*, *12*(1), 879–886. https://doi.org/10.29303/jppipa.v12i1.14197

Al Omari, H., Alkhateeb, A., & Hammo, B. (2024). Applying Togaf-Based Enterprise Architecture in The Healthcare Sector: A Case Study of The National Center for Diabetes in Jordan. *Jordanian Journal of Computers and Information Technology (JJCIT)*, *10*(02). https://doi.org/10.5455/jjcit.71-1705704023

Alfitrah, D. A., & Leegowo, N. (2026). Risk Assessment of Healthcare Information Systems in Indonesian Regional Government Hospitals Using ISO 27001:2022. *Journal of Computer Science*, *22*(3), 778–786. https://doi.org/10.3844/jcssp.2026.778.786

Alier, M., Guerrero, M. J. C., Amo, D., Severance, C., & Fonseca, D. (2021). Privacy and E-Learning: A Pending Task. *Sustainability (Switzerland)*, *13*(16). https://doi.org/10.3390/su13169206

Anjarwati, A., Qomariyah, R. S., Prameswari, D. A., Laili, S. N., & Wahyuningrum, P. D. R. (2025). Transforming Science Learning in the Era of Education 5.0 Through Virtual Reality (VR) Millea Lab: Improving Understanding of Science Concepts and Technological Literacy for Digital Native Students. *Jurnal Penelitian Pendidikan IPA*, *11*(11), 256–264. https://doi.org/10.29303/jppipa.v11i11.12850

Astutik, S., Andayani, S., & Hertika, A. M. S. (2025). Comparison of Water Conditions and Growth Performance of Vannamei Shrimp (Litopenaeus vannamei) under Different Pond Management Systems (Superintensive, Intensive, and Traditional Culture Systems). *Jurnal Penelitian Pendidikan IPA*, *11*(6), 390–403. https://doi.org/10.29303/jppipa.v11i6.10130

Billa, Y. S., & Restian, A. (2026). Development of Augmented Reality-Based Scansmart Card Media to Improve Elementary Students' Understanding of Photosynthesis in Support of SDG 4 (Quality Education). *Jurnal Penelitian Pendidikan IPA*, *12*(1), 797–805. https://doi.org/10.29303/jppipa.v12i1.14281

Djebbar, F., & Nordstrom, K. (2023). A Comparative Analysis of Industrial Cybersecurity Standards. *IEEE Access*, *11*, 85315–85332. https://doi.org/10.1109/ACCESS.2023.3303205

Fray, I. El, & Wiliński, A. (2024). Modifications of the Formal Risk Analysis and Assessment for the Information System Security. *Advances in Science and Technology Research Journal*, *18*(2), 317–332. https://doi.org/10.12913/22998624/185162

Geasela, Y. M., & Legowo, N. (2022). Designing Information System Architecture Based on Education 4.0 Case Study: Senior High School

Institutions of Indonesia. *Journal of Computer Science*, *18*(7), 622–637. https://doi.org/10.3844/JCSSP.2022.622.637

Hadi, M. D. S., Gultom, R. A. G., Ansori, A., & Kustiawan, B. (2025). Defense Information Systems Architecture for Cyber Threats: A Systematic Review of the Research Literature. *Jurnal Penelitian Pendidikan IPA*, *11*(10), 10–22. https://doi.org/10.29303/jppipa.v11i10.12905

Hadita, A., Wufron, W., & Septiana, Y. (2023). Analisis Penerimaan Sistem Informasi Akademik Santri Berbasis Web di Pondok Pesantren Al Halim Garut Menggunakan Metode Technology Acceptance Model. *Jurnal Algoritma*, *20*(1), 190–198. https://doi.org/10.33364/algoritma/v.20-1.1160

Hardi, K. V., & Legowo, N. (2023). Enterprise Architecture: Enabling Digital Transformation for Operational Business Process during COVID-19. *HighTech and Innovation Journal*, *4*(1), 1–18. https://doi.org/10.28991/HIJ-2023-04-01-01

Ibrahim, I., Nurwahidah, N., Suranti, N. M. Y., & Alimuddin, N. (2025). Integrating QR Code Technology in Elementary Science Content: A Developmental Study on Critical Thinking Skills. *Jurnal Penelitian Pendidikan IPA*, *11*(11), 215–228. https://doi.org/10.29303/jppipa.v11i11.12629

Istutik, I., Rahmawati, I. P., & Tuakia, H. (2023). Konstruksi Laporan Keuangan Pondok Pesantren (Studi pada Pondok Pesantren Al-Washoya Jombang). *Jurnal Manajemen Dirgantara*, *16*(1), 141–147. https://doi.org/10.56521/manajemen-dirgantara.v16i1.920

Khairani, L., Rifai, H., & Husna, H. (2025). Integration of Edupark and Digital Technology: Analysis of the Need for a Physics Learning Website to Address Misconceptions. *Jurnal Penelitian Pendidikan IPA*, *11*(11), 35–44. https://doi.org/10.29303/jppipa.v11i11.12610

Khairunnisa, F., Ilham, I., Widowati, A., Nugraha, U., & Sukendro, S. (2025). Pengembangan Aplikasi Penilaian Senam Aerobik pada Pusat Pendidikan dan Latihan Olahraga Pelajar (PPLP) Provinsi Jambi. *Jurnal Penelitian Pendidikan IPA*, *11*(11), 138–143. https://doi.org/10.29303/jppipa.v11i11.13354

Kusuma, F. A., Nurhayati, N., & Susilo, S. (2021). Penguatan Pendidikan Karakter Peserta Didik Melalui Peraturan Pondok Pesantren di Era 4.0. *Jurnal Ilmiah Mimbar Demokrasi*, *21*(1), 48–52. https://doi.org/10.21009/jimd.v21i1.23046

Lattu, A., Saepudin, S., Destria, N., Irawan, C., Sembiring, F., & Jatmiko, W. (2022). Perancangan Enterprise Menggunakan Framework Togaf pada Yayasan Baitul Huda. *Jurnal Sistem Informasi dan Teknologi Informasi)*, *4*(2), 83–89. https://doi.org/10.52005/jursistekni.v4i2.133

Lusiani, L., Vidhiasi, D. M., & Supriyanto, S. (2026). The Implementation of a Deep Learning Approach Using QR Code–Based Learning Media to Enhance High School Students' Academic Performance in Kinematics. *Jurnal Penelitian Pendidikan IPA*, *12*(1), 521–536. https://doi.org/10.29303/jppipa.v12i1.13484

Ma'arif, M. A., Arif, M., Rokhman, M., Hali, A. U., Kartiko, A., & Sirojuddin, A. (2026). Model of Kiai Leadership Based on Local Wisdom: Preventing Radicalism and Building Education in the Global South. *Kharisma*, *5*(1), 17–31. https://doi.org/10.59373/kharisma.v5i1.149

Maradova, K., Blecha, P., Samelova, V., Marada, T., & Zuth, D. (2026). Bayesian Networks for Cybersecurity Decision Support: Enhancing Human-Machine Interaction in Technical Systems. *Applied Sciences (Switzerland)*, *16*(6). https://doi.org/10.3390/app16063053

Maulana, Y. M., Rizal, Z., Azmi, M., & Arshah, R. A. (2023). Modeling of Strategic Alignment to Modify TOGAF Architecture Development Method Based on Business Strategy Model. *IJASEIT*, *13*(1). https://doi.org/10.18517/ijaseit.13.1.16565

Min, C. H., & Kwak, J. (2025). RMF-A: An Availability Assurance Framework for Quantitative Evaluation of Operational Resilience. *Electronics (Switzerland)*, *14*(23). https://doi.org/10.3390/electronics14234644

Mirtsch, M., Pohlisch, J., & Blind, K. (2026). Certification as a Compensation Mechanism for Weak Regulation? Exploring the Diffusion of the International Standard ISO/IEC 27001 for Information Security Management. *Computers and Security*, *162*. https://doi.org/10.1016/j.cose.2025.104774

Mof, Y., Ramadan, W., & Mizani, H. (2026). Evaluating the Effectiveness of the Santripreneur Program in Islamic Boarding School: A CIPP-Based Qualitative Assessment of Screenprinting Training. *Munaddhomah*, *7*(1), 141–156. https://doi.org/10.31538/munaddhomah.v6i4.2435

Mubarak, M. Z., Fuad, S., & Kholid, N. (2023). Implementasi Total Quality Management Perspektif Hensler dan Brunell di Pondok Pesantren Salafiyah. *Jurnal Manajemen dan Pendidikan Islam*, *9*(2), 104–113. https://doi.org/https://doi.org/10.26594/dirasat

Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: *(IJACSA) International Journal of*

Advanced Computer Science and Applications. https://doi.org/10.6028/NIST.SP.800-61r3

Petrov, P., Kuyumdzhiev, I., Malkawi, R., Dimitrov, G., & Jordanov, J. (2022). Digitalization of Educational Services with Regard to Policy for Information Security. *TEM Journal*, *11*(3), 1093–1102. https://doi.org/10.18421/TEM113-14

Rahmadani, R. G., Nurhayati, O. D., & Nugraheni, D. M. K. (2024). Governance in Samarinda City Using TOGAF (The Open Group Architecture Framework): Literature Review. *Edelweiss Applied Science and Technology*, *8*(6), 5161–5168. https://doi.org/10.55214/25768484.v8i6.3139

Rambau, T. M., Munyoka, W., Phahlamohlaka, L. J., & Kadyamatimba, A. (2026). Evaluating Cyber Resilience Frameworks for E-Government: Applicability of NIST CSF, ISO/IEC 27001 and COBIT 2019 in Developing Country Contexts. *Information and Computer Security*, 1–22. https://doi.org/10.1108/ICS-09-2025-0376

Sari, V. K., Jalmo, T., & Suyatna, A. (2025). Development of Differentiated Student Worksheets (LKPD) Oriented Towards Inquiry-Based Learning to Improve Critical Thinking Skills of High School Students on The Subject of The Human Digestive System. *Jurnal Penelitian Pendidikan IPA*, *11*(11), 286–298. https://doi.org/10.29303/jppipa.v11i11.12433

Subangkit, H. S., Taqqa, T. H., & Saputra, D. I. S. (2026). Lecturer Performance Prediction Based on Student Evaluation Data Using a Hybrid K-Means and Random Forest Model. *Jurnal Penelitian Pendidikan IPA*, *12*(1), 352–358. https://doi.org/10.29303/jppipa.v12i1.14163

Warsihna, J., Ramdani, Z., Kurniawan, H., Zulfikri, Z., Kosasih, F. R., Mudayat, M., & Syaikhu, A. (2026). Students' Perceptions of the Use of Artificial Intelligence in Discussion Forum Evaluation on Massive Open Online Courses Platform. *Jurnal Penelitian Pendidikan IPA*, *12*(1), 893–900. https://doi.org/10.29303/jppipa.v12i1.13975

Wijaya, I. S., Ridho, M., Hidayati, D. L., & Mahdi, M. (2024). Utilization of Digital Technology in Islamic Boarding Schools: A Case Study in Samarinda. *Lentera: Jurnal Ilmu Dakwah dan Komunikasi*, *7*(2), 140–153. https://doi.org/10.21093/lentera.v7i2.7390