Designing Attack Surface in Early Childhood Education System Environment using Risk Assessment and Enterprise Architecture Approach

[1]Dadang Setiawan*, [2]Dita Oktaria, [3]Sidik Prabowo, [4]Elizabeth Sastrina Indrasari
[1]Informatika, Fakultas Informatika, Universitas Telkom
[2,3]Teknologi Informasi, Fakultas Informatika , Universitas Telkom
[4]Manajemen, Fakultas Ekonomi dan Bisnis, Universitas Telkom
[1,2,3,4]Jl.Telekomunikasi No 1, Terusan Buah Batu, Bandung Jawa Barat 40257
*e-mail: dadangset@telkomuniversity.ac.id

(***received*:** 18 September 2024, ***revised*:** 28 October 2024 ***accepted*:** 4 November 2024)

Abstract

As digital technologies increasingly permeate the education sector, the need to safeguard sensitive personal data within early childhood education systems becomes paramount. In Indonesia, where the adoption of digital tools in education is rapidly expanding, these systems are particularly vulnerable due to the hybrid nature of their processes, varying levels of digital literacy among stakeholders, and a complex regulatory environment. This research addresses the challenge of securing Indonesia's early childhood education systems by designing a minimized attack surface through the integration of ISO 27005-based risk assessment and the TOGAF enterprise architecture framework. ISO 27005 provides a systematic methodology for identifying, assessing, and mitigating information security risks, ensuring compliance with the Indonesian Personal Data Protection Law (UUPDP). TOGAF is utilized to structure the enterprise architecture, aligning IT strategies with institutional goals while embedding robust security measures across the digital infrastructure. The research methodology involves identifying critical assets and potential threats, evaluating these threats using ISO 27005, and developing a secure architecture tailored to the unique needs of Indonesian early childhood education systems. The proposed framework is validated through application in a case study involving several Indonesian early childhood education institutions. This approach not only enhances the security posture of these institutions but also aligns with cultural and regulatory considerations, offering a comprehensive solution for protecting vulnerable educational environments in Indonesia.

Keywords: *Cybersecurity, Attack Surface, ISO 27005, TOGAF, Early Childhood Education*

1 Introduction

In today's increasingly digital world, the education sector, including early childhood education, has become deeply integrated with information technology systems. These systems not only enhance educational delivery but also manage vast amounts of sensitive personal data, including information about young children. The safeguarding of this data, as well as the overall security of the digital infrastructure, is paramount, particularly in the context of Indonesia, where the adoption of technology in education is growing rapidly. As these systems expand, so too does their attack surface—the total sum of vulnerabilities that can be exploited by malicious actors. Therefore, a strategic approach to minimizing this attack surface is essential to protect these critical educational environments.

This research focuses on designing the attack surface in Indonesia's early childhood education system environment by integrating ISO 27005-based risk assessment with TOGAF (The Open Group Architecture Framework) for enterprise architecture. ISO 27005 provides a systematic approach to identifying, analyzing, and managing information security risks, making it a valuable tool for understanding and mitigating potential threats to educational systems [1][2]. On the other hand, TOGAF offers a structured framework for designing and managing enterprise architecture, ensuring that IT initiatives align with the strategic objectives of the institution [3][4]. By combining these two methodologies, the research aims to create a robust, secure architecture tailored to the specific needs and challenges of early childhood education systems in Indonesia.

 ISSN:2302-8149
e-ISSN:2540-9719

The need for enhanced cybersecurity in educational systems has been increasingly recognized. According to Cerqueira Junior and Arima [1], educational institutions have become prime targets for cyber-attacks due to their vast repositories of personal data and generally weaker security postures compared to other sectors. In Indonesia, the integration of digital tools in education has accelerated, but this growth has also exposed significant vulnerabilities [5]. Hommel, Metzger, and Steinke [2] have argued that risk management frameworks like ISO 27005 are essential for systematically identifying and addressing these vulnerabilities, particularly in sectors like education where data sensitivity is high.

TOGAF has been widely adopted in various sectors for enterprise architecture, including education, to align IT systems with organizational goals while ensuring compliance with security standards[6]. Supriyadi and Amalia [3] demonstrated the effectiveness of TOGAF in designing secure and compliant educational IT architectures that can adapt to evolving threats and regulatory requirements. Similarly, Burmeister, Drews, and Schirmer [4] highlighted the role of TOGAF in creating privacy-driven architectures that support compliance with data protection regulations, a critical need in educational environments.

Despite these advancements, there remains a gap in the literature regarding the application of ISO 27005 and TOGAF specifically within the context of early childhood education systems in Indonesia. These systems are unique not only because of the age and vulnerability of their users but also because of the specific cultural and regulatory environment in Indonesia [7][8]. This research seeks to fill this gap by proposing a tailored approach to designing the attack surface of early childhood education systems in Indonesia, using ISO 27005 for risk assessment and TOGAF for enterprise architecture. The methodology developed in this research will be validated through expert judgment and applied to a case study within an Indonesian early childhood education environment [9][10].

The objectives of this research are threefold: first, to identify the critical assets and potential threats within Indonesia's early childhood education systems; second, to evaluate these threats using ISO 27005's risk assessment framework [11][12]; and third, to develop an enterprise architecture using TOGAF that effectively minimizes the attack surface while aligning with the institution's overall goals and regulatory requirements [13][14].

2 Literature Review

The design of secure and resilient information systems, particularly in educational environments, has become a critical area of focus in the field of cybersecurity. As the adoption of digital technologies in early childhood education grows, so does the need to protect sensitive data and minimize the attack surface—the total number of points where an unauthorized user can try to enter or extract data. This literature review explores existing research on the application of risk assessment frameworks, particularly ISO 27005, and the use of enterprise architecture frameworks like TOGAF in designing and securing educational systems.

2.1 Importance of Cybersecurity in Educational Systems

Educational institutions, including those focused on early childhood education, have increasingly become targets for cyber-attacks due to the sensitive nature of the data they hold and often inadequate security measures. In developing a secure architecture for early childhood education systems, prior research demonstrates the effectiveness of structured risk management frameworks like ISO 31000:2018 in identifying and mitigating threats within educational information systems[15] Smith and Jones highlight the growing risk faced by these institutions, emphasizing the need for robust security frameworks that can adapt to the unique challenges of the educational environment [1]. Similarly, White discusses the challenges faced by educational institutions in protecting student data, particularly in environments with limited resources for implementing advanced security measures [8]. This underscores the importance of a systematic approach to managing cybersecurity risks in educational settings.

2.2 Risk Management in Educational Environments Using ISO 27005

ISO 27005 provides a structured approach to risk management, particularly in identifying, assessing, and mitigating risks associated with information security. Anderson et al. (2020) argue that ISO 27005 is especially useful in educational contexts, where risk management practices are often underdeveloped [5]. The standard offers a comprehensive methodology that can be tailored to the specific needs of educational institutions, including those focused on early childhood education.

 ISSN:2302-8149
e-ISSN:2540-9719

Patel and Verma further illustrate the application of ISO 27005 in educational environments, highlighting its role in systematically identifying vulnerabilities and threats [2]. They suggest that the standard's flexibility makes it suitable for a wide range of educational settings, from large universities to smaller, more specialized institutions like early childhood education centers. This is supported by Chang and Taylor, who demonstrated the effectiveness of ISO 27005 in a case study of a mid-sized educational institution, where the standard was used to identify critical security gaps and implement targeted risk mitigation strategies [13].

2.3 Enterprise Architecture in Educational Systems: The Role of TOGAF

The integration of enterprise architecture frameworks, such as TOGAF, into educational systems is crucial for aligning IT strategies with institutional goals while ensuring robust security measures. TOGAF provides a comprehensive framework that includes guidelines for developing secure and efficient IT infrastructures that support the overall objectives of educational institutions. The importance of TOGAF is highlighted in creating secure architectures that are flexible enough to adapt to the changing needs of educational environments [3]. They note that TOGAF's modular approach allows for the integration of security considerations at every stage of the architecture development process.

The role of TOGAF is further discussed in ensuring compliance with data protection regulations, particularly in educational institutions that handle large amounts of personal data [4]. Their research highlights the framework's ability to support privacy-driven architectures that are essential for protecting sensitive information in early childhood education systems. This is particularly relevant in the context of Indonesia, where regulatory requirements for data protection are becoming increasingly stringent.

2.4 Combining ISO 27005 and TOGAF for Secure Educational Systems

The combination of ISO 27005 and TOGAF provides a powerful approach to designing secure educational systems. Researchers explore the integration of these two frameworks in the context of educational IT systems, demonstrating how their combined use can enhance both the security and efficiency of these systems. Their study shows that while ISO 27005 provides the tools for identifying and managing risks, TOGAF offers the architectural framework necessary to implement these measures in a cohesive and strategic manner [11][12].

The integration of ISO 27005 with TOGAF in educational institutions, particularly in terms of creating a unified approach to risk management and IT governance can lead to more resilient systems that are better equipped to handle the complexities of modern educational environments. The importance of using both ISO 27005 and TOGAF in educational settings is also highlighted, particularly in the context of protecting student data. The combination of these frameworks allows for a more comprehensive approach to data protection, one that addresses both the technical and organizational aspects of security.

2.5 Challenges and Considerations in the Indonesian Context

The application of these frameworks in Indonesia presents unique challenges, particularly in early childhood education systems. It is further emphasized that the importance of understanding the local educational landscape when applying these frameworks is needed, particularly in terms of aligning them with national policies on education and data protection [13]. The successful implementation of these frameworks in Indonesia requires a deep understanding of the local regulatory environment, as well as the specific needs of early childhood education institutions [3].

2.6 Case Studies and Practical Implementations

Several studies have documented the practical implementation of ISO 27005 and TOGAF in educational settings, providing valuable insights for their application in Indonesia's education system [14][16]. However, there has not been much research that covers the implementation in early education settings. Those gaps underscore the importance of a systematic approach to cybersecurity in educational environments, particularly in early childhood education systems in Indonesia. The combination of ISO 27005 and TOGAF provides a robust framework for identifying, managing, and mitigating risks while ensuring that IT systems are aligned with the strategic goals of the institution. However, the successful application of these frameworks in Indonesia requires careful consideration of local regulatory, cultural, and institutional factors. Future research should focus on the practical implementation of these frameworks in Indonesian early childhood education systems, providing further insights into how they can be adapted to meet the unique challenges of this context.

 ISSN:2302-8149
e-ISSN:2540-9719

3 Research Method

The research methodology is conducted to examine the attack surface in educational system especially focusing on early childhood through a risk assessment approach. This chapter outlines the structured approach taken to identify, analyze, and assess the vulnerabilities within these systems using a multi-phase research design, ensuring a systematic exploration of potential attack vectors and their impacts on educational infrastructure.

3.1 Research Phases

The research phases outlined in the diagram Figure 1 showing a structured approach that ensures the attack surface design is comprehensive and well-suited to the specific needs of the early childhood education system environment. Each phase builds on the previous one, creating a systematic pathway from theoretical analysis to practical implementation and validation.

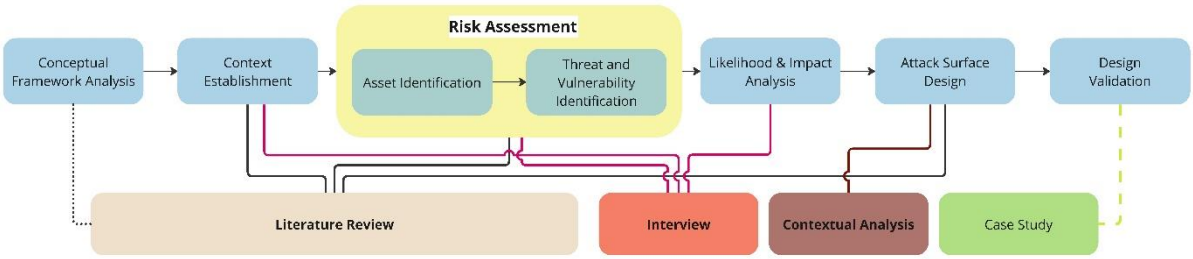

Figure 1. Research phases

The use of various research techniques, including literature reviews, interviews, and expert judgments, ensures that the design is grounded in both theory and practical insights, making it robust and applicable in the real world. Below is an explanation of each phase in the context of this research:

3.1.1 Conceptual Framework Analysis

In this initial phase, the research aims to establish a clear conceptual framework. This involves understanding the theoretical foundation and context within which the research will be conducted. The literature review is conducted to explore existing theories, models, and studies relevant to attack surface design, risk assessment, and enterprise architecture in the context of early childhood education systems.

3.1.2 Context Establishment

This phase involves defining the specific context of the research. It includes understanding the unique characteristics of the early childhood education system environment and how it influences the attack surface. The literature review helps in identifying general contextual factors, while interviews with stakeholders (such as IT administrators, educators, and security experts) provide insights into the specific environment of the early childhood education system.

3.1.3 Identify Asset

The goal of this phase is to identify the key assets within the early childhood education system that need protection. These assets could include sensitive data, IT infrastructure, and educational resources. A combination of literature review and interviews is used to comprehensively identify and categorize these assets, ensuring that all critical components are considered.

3.1.4 Identify Threat & Vulnerability

This phase focuses on identifying potential threats and vulnerabilities that could affect the identified assets. It involves understanding the types of threats (e.g., cyber-attacks, insider threats) and the vulnerabilities within the system. The literature review provides information on common threats and vulnerabilities in educational systems, while interviews help to uncover specific vulnerabilities relevant to the system in question.

3.1.5 Analyze Likelihood & Impact

In this phase, the research assesses the likelihood of identified threats exploiting vulnerabilities and the potential impact of such events on the system. Interviews with experts and stakeholders help to evaluate the probability of threats and their potential consequences, forming the basis for risk assessment.

 ISSN:2302-8149
e-ISSN:2540-9719

3.1.6 Designing Attack Surface

Based on the findings from the previous phases, this phase involves designing the attack surface for the early childhood education system. This design aims to minimize vulnerabilities and protect the identified assets. The design process is informed by best practices and frameworks identified through literature, combined with analytical insights gained from previous phases.

3.1.7 Design Validation

The final phase involves validating the designed attack surface to ensure it is effective and aligns with the identified risks and context. Validation ensures that the proposed design meets security requirements and is feasible within the system environment. Case studies in early childhood education, and enterprise architecture conducted to review the proposed design to validate its effectiveness and appropriateness.

3.2 Conceptual Framework

The conceptual framework illustrated in the diagram Figure 2 presents a structured approach to designing an attack surface for an education system environment by integrating risk assessment (as per ISO 27005) with enterprise architecture methodologies such as TOGAF and OWASP Threat Modelling. The diagram illustrates how risk assessment feeds into the design of the attack surface. By systematically identifying, analyzing, and evaluating risks (as guided by ISO 27005), the framework ensures that the resulting attack surface design is both comprehensive and aligned with the organization's overall enterprise architecture.

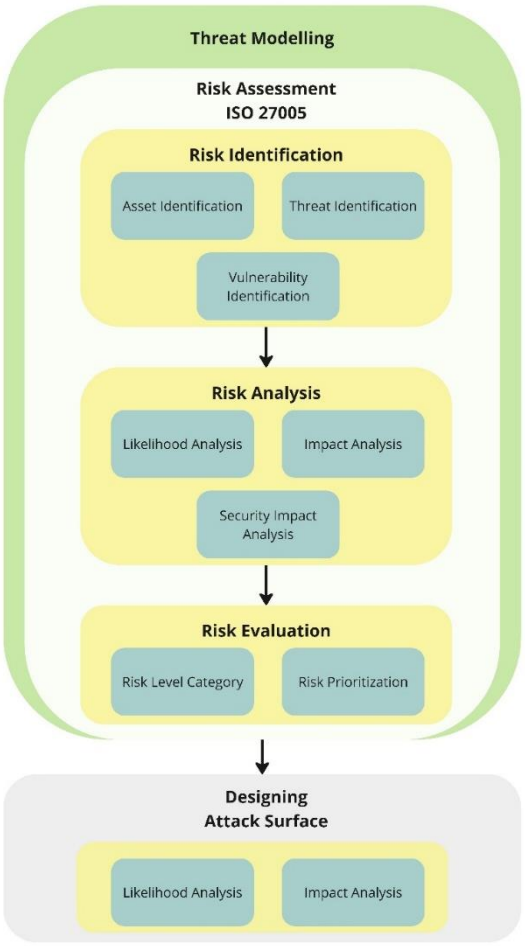

Figure 2. Conceptual framework

 ISSN:2302-8149
e-ISSN:2540-9719

3.2.1 Conceptual Framework

The overarching goal of the framework is to design a secure attack surface through comprehensive threat modeling. This process encompasses identifying, analyzing, and evaluating potential threats within the education system environment. The following threat modelling is composed with the guidance of ISO 27005 as follows.

3.2.2 Risk Assessment (ISO 27005)

a. Risk Identification

In the initial part of risk assessment, a thorough identification is conducted that contains asset identification, threat and vulnerability identification. Asset identification involves identifying critical assets within the educational environment, such as student records, financial data, and IT infrastructure. The next step is to identify potential threats to the previously listed assets by considering factors such as cyber-attacks, data breaches, and system failures. The last step in the risk assessment is to identify existing vulnerabilities within the system which could be exploited by the identified threats.

b. Risk Analysis

The risk assessment is then continued with risk analysis to further deepen the likelihood, impact, and security impact of the risk that follows each of the asset. The first step in the risk analysis process is to analyze the likelihood of the risk by estimating the probability that identified threats will exploit vulnerabilities. The impact analysis is then followed by assessing the potential impact on the education system if the threats were to materialize. The last part in this process is to analyze the security impacts of the threats by considering the sensitive nature of the educational data and operations.

c. Risk Evaluation

The following process is to conduct a risk evaluation which consists of risk level and risk prioritization, detailed in Table 1. The first step is to categorize risk based on the analysis into levels of very low, low, medium, high and very high. The next step is to prioritize the risks based on their severity and potential impact on the education system which will guide the focus of the subsequent attack surface design.

Table 1. Risk level matrix

Risk Level					
Likelihood/ Impact	5	4	3	2	1
5	Critical	Critical	High	High	Medium
4	Critical	High	High	Medium	Medium
3	High	High	Medium	Medium	Low
2	High	Medium	Medium	Low	Very Low
1	Medium	Medium	Low	Very Low	Very Low

The following table contains the risk severity matrix based on its impact and likelihood of score 1-5. There are five risk levels which are ‘Very Low’, ‘Low’, ‘Medium’, ‘High’ and ‘Critical’. The assets are categorized as ‘Critical’ risk level have the highest priority and therefore further assessed to see their attack survey. This risk assessment will be further discussed in Chapter 4 and is visualized as Figure 3.

 ISSN:2302-8149
e-ISSN:2540-9719

3.2.3 Designing Attack Surface

After all processes in the risk assessment have been fully conducted, all risks that have been mapped are then visualized into an attack surface. There are two architecture methodologies which are the TOGAF Standard and the OWASP Threat Modelling. The Open Group Architecture Framework (TOGAF) Standard ensures that the attack surface design is aligned with the broader enterprise architecture as well as the security measures to integrate seamlessly with the existing IT infrastructure and educational goals. On the other hand, the OWASP Threat Modelling is also incorporated to specifically address web and application-level threats that are prevalent in educational systems. This ensures that the attack surface design is robust against modern cyber threats.

For an educational system environment, the joined framework between the TOGAF Standard and the OWASP Threat Modelling ensures that all potential threats are systematically addressed, and the attack surface is designed with a deep understanding of the specific needs and risks of educational institutions. The integration of TOGAF ensures alignment with the institution's strategic goals, while OWASP Threat Modelling provides practical defenses against common web-based threats, making the attack surface both robust and practical.

This conceptual framework, therefore, provides a comprehensive approach to designing an attack surface that is tailored to the unique risks and requirements of educational systems, ensuring both security and operational integrity.

4 Results and Analysis

The findings and analysis is then presented in this following chapter which derived from the structured investigation outlined previously. This chapter delves into the data collected and the examination of it by looking at the risk perspectives to highlight the vulnerabilities and potential points.

4.1 Context Establishment

In the context of Indonesia's early childhood education institutions, the increasing integration of digital technologies poses significant challenges to data protection and cybersecurity. Despite the gradual adoption of digital processes, many institutions still rely heavily on paper-based systems for critical activities such as student admission. This hybrid environment, coupled with varying levels of digital literacy and security awareness among teachers, academic staff, students, and parents, creates a complex attack surface that is vulnerable to various risks. The enactment of the Indonesian Personal Data Protection Law (UU PDP) further underscores the need for robust security measures that comply with national regulations while being culturally sensitive.

4.2 Risk Assessment

The risk assessment based on the types of assets is then detailed in the following Table 2.

Table 2. Risk assessment

No	Type of Asset	Name of Asset	Vulnerability	Threats	CIA Map	Likelihood Level	Impact Level	Impact Category
1	Software	Admission Application	Wrong allocation of access rights	Illegal processing of data	Integrity	4	5	Operational, Financial, Reputation
2		Financial Information System	No or insufficient security software testing	Corruption of data	Integrity	4	5	Operational, Financial
3		Human Resource Information System	No or insufficient security software testing	Violation of Information System Maintainability	Integrity	4	5	Operational
4		Government Application	Widely distributed software	Failure of service providers	Availability	4	5	Operational

 ISSN:2302-8149
e-ISSN:2540-9719

No	Type of Asset	Name of Asset	Vulnerability	Threats	CIA Map	Likelihood Level	Impact Level	Impact Category
5		Third Party Productivity Tools	Widely distributed software	Failure of service providers	Availability	4	5	Operational
6	Server	Server	Lack of or incomplete back-up copies	Terror, attack, sabotage	Confidentiality	4	5	Operational
7	Endpoint	Endpoint Device	Ineffective or lack of mechanisms for identification and authentication of sender and receiver	Abuse of rights or permissions	Confidentiality	4	5	Operational
8	Network	Wireless Access	Ineffective or lack of mechanisms for identification and authentication of sender and receiver	Abuse of rights or permissions	Confidentiality	4	5	Operational
9	Personnel	Student	Poor security awareness	Carelessness of students	Confidentiality	5	4	Operational
10		Student's Parents	Poor security awareness	Phishing	Confidentiality	5	4	Operational
11		Employee (Teacher & Academic Support Staff)	Insufficient security training	Lack of employees' security skills and awareness	Confidentiality	5	5	Operational
12	Partner/ Vendor	Partner/ Vendor	Insufficient provisions (concerning security) in contracts with customers and/or third parties	Failure of service providers	Confidentiality	4	5	Operational
13	Site	Teacher's Office	Insufficient physical protection of the building, doors, and windows	Unauthorized entry to facilities	Confidentiality	4	5	Operational

4.4 Risk Evaluation

The risk evaluation based on the risk assessment based on the previous subchapter is then detailed in the following Table 3.

 ISSN:2302-8149
e-ISSN:2540-9719

Table 3. Risk evaluation

No	Name of Asset	Risk Events	CIA Map	Risk Level
1	Admission Application	The potential for illegal data processing due to vulnerabilities in access rights allocation and the lack of policies regulating personal data, which impacts the student admission process and violates personal data protection regulations.	Integrity	**Critical**
2	Financial Information System	The potential for illegal data alteration and system failure due to insufficient application security testing and vendor non-compliance with regulations, leading to data breaches.	Integrity	**Critical**
3	Human Resource Information System	The potential for illegal data processing due to vulnerabilities in access rights allocation and the lack of policies regulating personal data, which impacts employee data management and violates personal data protection regulations.	Integrity	**Critical**
4	Government Application	The potential for a data breach due to attacks on the Government's application.	Availability	**Critical**
5	Third Party Productivity Tools	The potential for operational disruption of the foundation due to issues with third-party productivity applications.	Availability	**Critical**
6	Server	The potential for system failure containing critical data due to insufficient security testing, impacting the institution's operations.	Confidentiality	**Critical**
7	Endpoint Device	The potential for misuse of rights or permissions due to inadequate identification and authentication mechanisms, leading to institutional data leaks.	Confidentiality	**Critical**
8	Wireless Access	The potential for misuse of rights or permissions due to inadequate identification and authentication mechanisms, leading to institutional data leaks.	Confidentiality	**Critical**
9	Student	The potential for student negligence due to vulnerabilities caused by low security awareness.	Confidentiality	**Critical**
10	Student's Parents	The potential for students' parents to fall victim to fraud and phishing due to vulnerabilities caused by low security awareness.	Confidentiality	**Critical**
11	Employee (Teacher & Academic Support Staff)	The potential for illegal data processing due to vulnerabilities in access rights allocation and the lack of policies regulating personal data, impacting the institution's operations and violating personal data protection regulations.	Confidentiality	**Critical**
12	Partner/Vendor	The potential for data damage and loss due to a data breach caused by the lack of clauses regulating information security in vendor contracts.	Confidentiality	**Critical**
13	Teacher's Office	The potential for illegal access to the school building due to insufficient protection of room access, leading to potential illegal access to personal data and data leakage.	Confidentiality	**Critical**

 ISSN:2302-8149
e-ISSN:2540-9719

4.5 Attack Surface Design

After mapping out the risk assessment in each types of assets, the attack surface is then designed along with its risk events that linked to the assets as follows.

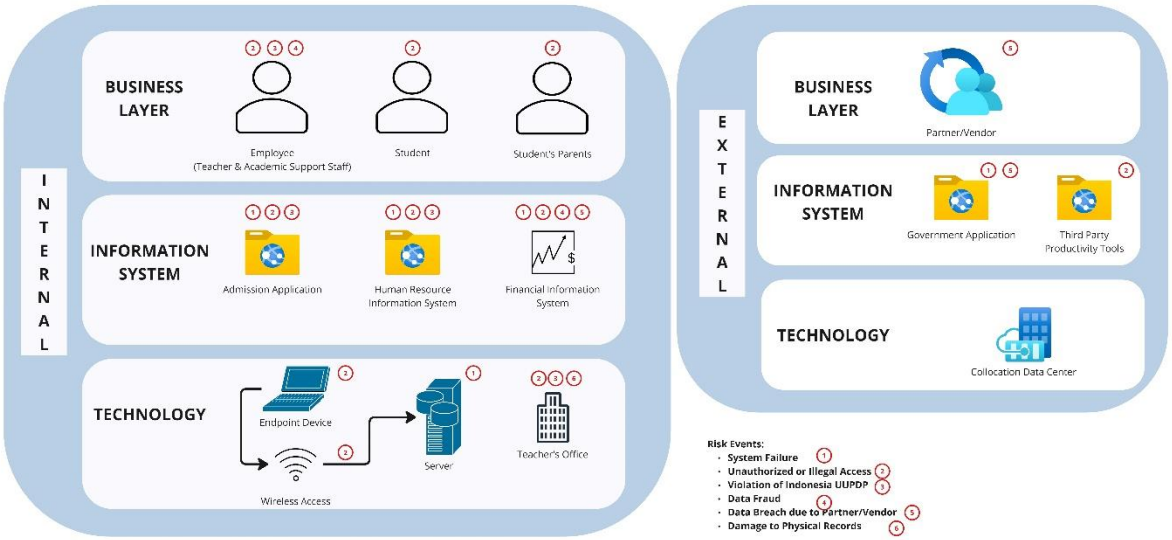

Figure 3. Attack surface design

4.5.1 Architecture Component:

The diagram shown in Figure 3 breaks down the system environment into three main layers, which align with TOGAF's concept of the four architectural domains: Business, Data, Application, and Technology Architectures. Although the diagram doesn't explicitly label the Data layer, it implicitly includes data management within the Information System layer.

In the Business Layer, the components are Teachers, Academic Support Staff, Students, Students' Parents, and External Partners/Vendors. The Business Architecture in TOGAF defines the structure and interactions between the business processes, people, and organizational units. In this context, it focuses on how these entities interact with the educational system and highlights potential risk areas, such as unauthorized access or data fraud.

In the Information System Layer, the components are Admission Application, Human Resource Information System, Financial Information System, Government Application, Third-Party Productivity Tools. The Application Architecture in TOGAF describes how applications are structured to support business processes. This layer in the diagram represents critical applications that need to be protected against various threats, such as system failure or data breaches. It emphasizes the importance of secure design and implementation, aligning with TOGAF's principles for creating robust, reliable application architectures.

In the Technology Layer, the components are Endpoint Devices, Wireless Access, Servers, Physical Locations like the Teacher's Office. The Technology Architecture in TOGAF outlines the hardware, software, and network infrastructure needed to support the deployment of core applications. This layer of the diagram focuses on the underlying technology that could be vulnerable to risks like system failure, unauthorized access, or damage to physical records. TOGAF's guidance on creating a resilient and secure technology infrastructure is crucial here.

4.5.2 Risk Events Analysis:

The right side of Figure 3 lists key risk events and their correlation with the different layers of the system, which can be analyzed and mitigated using TOGAF's Architecture Development Method (ADM). The risk events mapped in the surface attack are further elaborated below.

1) **Risk Event 1: System Failure**

Outdated technology or lack of regular maintenance or inadequate testing can lead to severe system failures or loss of critical data. This condition arises because the system is unable to keep up with modern technology and business developments, increasing the risk of significant operational disruptions. In TOGAF, the Technology Architecture phase includes considerations for maintaining system stability and reliability. The architecture should incorporate redundancy,

 ISSN:2302-8149
e-ISSN:2540-9719

regular maintenance schedules, and up-to-date technology to avoid outdated components causing failures.

2) Risk Event 2: Unauthorized or Illegal Access

Weak access controls or ineffective identification mechanisms allow unauthorized access by individuals. This increases the risk of data theft or information leakage that can jeopardize the institution's security. The TOGAF's Security Architecture, which spans across all domains, emphasizes the need for strong authentication mechanisms and access controls. This risk highlights the importance of implementing security measures in both the Business and Technology Architectures to prevent unauthorized access.

3) Risk Event 3: Violation of Indonesian Personal Data Protection Law

The cause of this risk is due to formal policy have yet to be established and may result in unauthorized data processing, leading to data breach and violation of the Indonesian Personal Data Protection Law. The TOGAF's Compliance and Regulatory Considerations are vital in the Business and Information System layers. The architecture should ensure that all processes and systems comply with relevant laws and regulations, in this case, the Indonesian Personal Data Protection Law.

4) Risk Event 4: Data Fraud

Data fraud involves the intentional manipulation, falsification, or tampering of data for malicious purposes, typically for personal gain or to deceive others. In the Business Architecture phase, TOGAF encourages the development of processes and controls that detect and prevent fraud. This involves not only technological measures but also process-oriented controls and audits.

5) Risk Event 5: Data Breach due to Partner/Vendor

This risk is probable when the vendor may not be fully compliant with applicable regulations or industry standards and may mishandle sensitive data during development or testing, leading to a data breach. TOGAF's approach to managing external relationships (including partners and vendors) involves establishing clear security requirements and compliance checks. This aligns with the need to manage risks from external vendors who interact with sensitive data.

6) Risk Event 6: Damage to Physical Records

Physical records are damaged or destroyed due to environmental factors such as fire or flooding or improper handling, resulting in the loss of critical student information. This relates to the Physical Security aspects within TOGAF's Technology Architecture. The framework advocates for physical security controls to protect data centers, office spaces, and other physical locations where critical data may be stored.

5 Conclusion

This research highlights the critical need to safeguard early childhood education systems in Indonesia by minimizing the attack surface through the integration of ISO 27005-based risk assessment and the TOGAF enterprise architecture framework. By identifying potential risks and aligning them with organizational goals, the proposed framework offers a comprehensive strategy for enhancing cybersecurity in educational environments. The study's practical approach, validated through expert judgment and case studies, ensures that the unique regulatory and cultural challenges of Indonesia are addressed, providing a robust solution to protect sensitive data and ensure compliance with national laws. Future research should continue to explore the implementation of this framework to further enhance its adaptability and effectiveness in the evolving digital landscape of early childhood education.

Reference

[1] A. S. . Cerqueira Junior and C. H. . Arima, "Cyber Risk Management and ISO 27005 Applied in Organizations: A Systematic Literature Review", Rev. Foco, vol. 16, no. 02, p. e1188, Feb. 2023.

[2] W. Hommel, S. Metzger, and M. Steinke, "Information Security Risk Management in Higher Education Institutions: From Processes to Operationalization," Handle.net, 2015, doi: https://doi.org/2409-1340.

 ISSN:2302-8149
e-ISSN:2540-9719

[3] H. Supriyadi and E. Amalia, "Development of Enterprise Architecture in Senior High School Using TOGAF as Framework," Universal Journal of Educational Research, vol. 7, no. 4A, pp. 8–14, Apr. 2019, doi: https://doi.org/10.13189/ujer.2019.071402.

[4] F. Burmeister, P. Drews, and I. Schirmer, "A Privacy-driven Enterprise Architecture Meta-Model for Supporting Compliance with the General Data Protection Regulation," Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019, pp. 60040.

[5] F. Al-Mudaires, A. Al-Samawi, A. Aljughaiman, and L. Nissirat, "Information security risk management framework for a governmental educational institute / Fajer Al-Mudaires ... [et al.] - UiTM Institutional Repository," Uitm.edu.my, Apr. 2023, doi: https://ir.uitm.edu.my/id/eprint/77315/1/77315.pdf.

[6] G. Fuentes-Quijada, F. Ruiz-González, and A. Caro, "Enterprise Architecture and IT Governance to Support the BizDevOps Approach: a Systematic Mapping Study," Information Systems Frontiers, Feb. 2024, doi: https://doi.org/10.1007/s10796-024-10473-2.

[7] Siegfried Rouvrais and Sobah Abbas Petersen, "An Architecture Framework for Higher Education," Jan. 2024, doi: https://doi.org/10.5220/0012738900003690.

[8] S. Faris and S. El. Hasnaoui, "Toward an Effective Information Security Risk Management of Universities' Information Systems Using Multi Agent Systems, Itil, ISO 27002, ISO 27005," International Journal of Advanced Computer Science and Applications, vol. 5, no. 6, 2014, doi: https://doi.org/10.14569/ijacsa.2014.050617.

[9] J. De, D. Imbaquingo, and J. Llumiquinga, "Hybrid Information Security Framework Based on ISO/IEC 27005:2022 and the NIST Framework for the Ministry of Education of Ecuador (TIC)," Lecture notes in computer science, pp. 71–85, Jan. 2024, doi: https://doi.org/10.1007/978-3-031-65285-1_6.

[10] A. F. Guzmán-Castillo, G. Suntaxi, B. N. Flores-Sarango, and D. A. Flores, "Towards Designing a Privacy-Oriented Architecture for Managing Personal Identifiable Information," Journal of internet services and information security, vol. 14, no. 1, pp. 64–84, Mar. 2024, doi: https://doi.org/10.58346/jisis.2024.i1.005.

[11] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, "The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda," *The TQM Journal*, vol. 33, no. 7, pp. 76–105, Mar. 2021, doi: https://doi.org/10.1108/tqm-09-2020-0202.

[12] B. M. Dioubate, W. Daud, and W. Norhayate, "Cyber Security Risk Management Frameworks Implementation in Malaysian Higher Education Institutions," *International Journal of Academic Research in Business and Social Sciences*, vol. 12, no. 4, Apr. 2022, doi: https://doi.org/10.6007/ijarbss/v12-i4/12300.

[13] Dražen Oreščanin, Tomislav Hlupić, and B. Vrdoljak, "Managing Personal Identifiable Information in Data Lakes," IEEE access, pp. 1–1, Jan. 2024, doi: https://doi.org/10.1109/access.2024.3365042.

[14] G. F. Nama, Tristiyanto, and D. Kurniawan, "An enterprise architecture planning for higher education using the open group architecture framework (togaf): Case study University of Lampung," *IEEE Xplore*, Nov. 01, 2017. https://ieeexplore.ieee.org/abstract/document/8280610/

[15] A. Sulistiawati and K. D. Hartomo, "Risk Management Analysis of School Management Information Systems Using ISO 31000:2018," *Sistemasi: Jurnal Sistem Informasi*, vol. 13, no. 5, pp. 2020–2032, 2024.

 ISSN:2302-8149
e-ISSN:2540-9719

[16] Hery Dian Septama, Muhamad Komarudin, Puput Budi Wintoro, Mahendra Pratama, Titin Yulianti, and Bambang Sundari, "Enterprise Architecture Planning based on One Data in Indonesian Higher Education," *2022 Seventh International Conference on Informatics and Computing (ICIC)*, Dec. 2022, doi: https://doi.org/10.1109/icic56845.2022.10006947.