Journal of Information Systems and Informatics
Vol. 7, No. 3, September 2025 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v7i3.1265 Published By DRPM-UBD

ISO/IEC 27005-Based E-Learning Risk Management with Blockchain Architecture: A Case Study of Semarang University

Muhammad Nur Irfan[1], Salwa Ramadhania[2], Soiful Hadi[3], Prind Triajeng Pungkasanti[4]

[1,2,3,4]Information System Department, Faculty of Information and Communication Technology, Semarang University, Indonesia
Email: [1]mnirfan33@gmail.com, [2]salwaramadhania123@gmail.com, [3]saiful@usm.ac.id, [4]prind@usm.ac.id

Abstract

This study aims to analyze information security risk management in the Semarang University E-Learning System using the ISO/IEC 27005 standard and to design a blockchain-based architecture as a conceptual strategy for improving data security. The implementation of blockchain in this study is limited only to the conceptual design stage, which serves as a risk mitigation framework without direct application to the system. The research method uses a Waterfall approach that includes the stages of risk identification, needs analysis, risk evaluation, adjustment through expert judgment, risk prioritization, and design of a blockchain-based mitigation architecture. Data were collected through quantitative surveys of students, lecturers, and system users, and qualitative assessments from information technology administrators. The analysis results show that the risks with very high priority are R005 with a score of 22.03 related to personal data security, and R007 with a score of 21.03 related to system access failure at critical times. The integration of blockchain in this design serves to improve data integrity, transaction process transparency, and service availability through distributed recording and smart contract-based automatic verification. This study provides novelty by simultaneously combining the ISO/IEC 27005 approach and blockchain architecture concepts in the context of a university e-learning system, resulting in a comprehensive strategic framework for information security risk management. The blockchain implementation in this study is limited to the conceptual design stage.

Keywords: ISO/IEC-27005, information security, e-learning, risk management, blockchain

1. INTRODUCTION

One of the most important tactics to support the learning process in higher education is the shift to digital learning through e-learning platforms. These systems offer high flexibility, efficiency, and accessibility for students and lecturers. However, with increasing reliance on digital platforms, the challenges of maintaining information security, data integrity, and service availability during

critical moments are increasingly complex. This requires a systematic risk management approach based on international standards.

Several previous studies have addressed security risk management in e-learning systems. Rifki Maulana and Fathoni Mahardika mapped security risks in e-learning systems using the ISO/IEC 27005 framework, which identifies technical and non-technical assets, as well as common threats such as phishing and malware [1]. Another study discussed the role of blockchain in strengthening security and privacy in e-learning systems, pointing to decentralization, transparency, and data reliability as the main benefits of the technology [2]. Furthermore, research in the manufacturing industry found that blockchain serves as a mediator between e-learning and information security, as well as enhancing the digital orientation of institutions [3]. However, there is still little research that simultaneously integrates the ISO/IEC 27005 framework with technological solutions such as blockchain in the context of university e-learning.

Furthermore, Meitarice et al., underlined that the use of ISO/IEC 27005:2018 in the information risk management process was able to identify more than 30 threats and 43 vulnerabilities, as well as produce more effective risk mitigation recommendations [4]. Wibowo et al., also stated that "blockchain technology is a mechanism that makes it possible to validate digital transactions securely and decentralized," thus providing extra protection for data integrity [5]. In addition, Adhicandra et al., stated that "blockchain offers an excellent solution to address security and data integrity issues," because this technology provides transparency, immutability, and a more secure data distribution mechanism [6]. Similar results were also found in MDPI research, where blockchain was shown to improve data privacy and security in digital education systems [7].

Therefore, there is a research gap in the absence of studies that comprehensively combine ISO/IEC 27005-based risk analysis with blockchain-based mitigation architecture design in the domain of e-learning systems, particularly in higher education environments. This study seeks to fill this gap by proposing a new framework that combines ISO/IEC 27005 risk management methodology with blockchain architecture design. This approach is not only relevant to Semarang University but can also be applied by other universities in Indonesia that rely on e-learning systems for academic activities, particularly in the face of similar data security and system reliability risks. This research addresses the need for risk mitigation solutions that are not only systematic but also utilize emerging technologies to maintain data integrity, transparency, and system reliability.

The main problem addressed in this research is: "How to comprehensively manage information security risks in Semarang University's e-learning system based on the ISO/IEC 27005 approach, and how can blockchain architecture design be used as

a conceptual mitigation strategy to strengthen data security and the reliability of e-learning systems?"

The main contribution of this research is the introduction of a new conceptual model that combines blockchain technology and the international risk management standard ISO/IEC 27005 as an information security mitigation strategy. This approach is expected to serve as a reference in the development of more secure, reliable, and trustworthy e-learning systems in various higher education institutions.

2. METHODS

2.1. Research Methods

This study uses the ISO/IEC 27005:2022 approach combined with a conceptual blockchain architecture design for information analysis and security risk mitigation in the Semarang University (USM) E-Learning System. The ISO/IEC 27005 approach was chosen because it provides a systematic framework for identifying, analyzing, disseminating, and controlling information security risks. The research stages follow the risk management cycle flow as recommended by ISO/IEC 27005. It is used as a specific guideline for risk management information, which includes contextualization, risk assessment, evaluation, and mitigation. [4].

The combination of ISO/IEC 27005 and conceptual blockchain architecture design provides a methodological advantage not available in previous research. ISO/IEC 27005 offers a systematic framework for managing information risks, while blockchain adds a layer of transparency, decentralization, and enhanced data security. This approach is not only relevant to Semarang University but can also be applied to other universities using similar e-learning platforms, such as Gadjah Mada University, BINUS University, or Telkom University, as an effort to improve overall information security governance. Blockchain architecture as a mitigation tool is relevant to recent studies demonstrating the technology's role in enhancing data security and integrity in digital applications [1], [2]. Figure 1 shows the risk assessment process flow integrated with the blockchain architecture design. The research stages are structured as follows.

1) Risk Identification

The initial step in this research was to identify potential risks in the University of Semarang (USM) e-learning system through a quantitative survey and qualitative interviews. Quantitative data was collected through a Likert-scale questionnaire (1–5) from 42 respondents, consisting of students and lecturers as active users of the e-learning system. Qualitative data was obtained through interviews with five information technology experts who acted as expert judges, including a system

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

administrator, a content management lecturer, and IT security staff. Risk identification was conducted to help the organization identify potential sources of threats. This step is crucial for understanding the risk drivers and their potential impact. impacts [8].

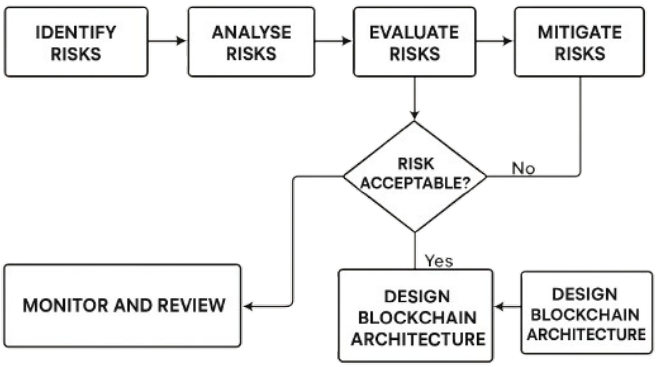

Figure 1. Risk Management Methodology ISO/IEC 27005

The sample size of 42 respondents was selected based on guidelines from Ali Memon et al. [9], which state that a sample size of over 30 respondents is considered adequate for descriptive analysis in research using a Likert scale approach. Although this sample size is relatively small compared to structural model-based research (e.g., PLS-SEM or AHP, which typically use 100–200 respondents), this limitation is due to the limited research period and the availability of active respondents during the data collection period.

To address these limitations and maintain the validity of the results, this study combined survey results with expert judgment. This approach aimed to strengthen the quantitative results with qualitative perspectives from experts familiar with operational and technical risks in e-learning systems. Furthermore, the five experts met the Delphi method's recommendations, where a panel of 3–10 experts is considered ideal for achieving a credible and representative consensus. Risk identification results are categorized into usability & accessibility, data security & privacy, and procedures & compliance. The risk identification stage includes identifying assets, threats, and controls with existing vulnerabilities [10]. All of which are relevant to the context of information security management in e-learning systems in higher education.

2) Risk Analysis (Likelihood dan Impact)

At this stage, the level of likelihood of occurrence and impact of the risks that have been identified is predicted [11]. Survey data was processed using a 1–5 Likert scale

to calculate the likelihood and impact of each risk. The survey data was then processed to obtain an average likelihood and impact score for each question. The basic formula used is as shown in Equation 1.

$$Risk\ Score = Likehood\ X\ Impact \quad (1)$$

The analysis results are arranged in a risk matrix according to ISO/IEC 27005:2022, and each risk is assigned a code R001–R010 to facilitate mitigation prioritization.

3) Risk Evaluation (Risk Score)

Risk scores are obtained by multiplying likelihood and impact. Each risk score is then categorized into three levels: Low (1–10), High (11–20), and Very High (>20). By comparing the risk levels against established criteria, we determine which risks are acceptable and which require management [12]. Risks with high and very high scores are the top priority in mitigation.

4) Adjustment with Expert Judgment

Qualitative data from IT experts was used to adjust the quantitative results by adding expert weights to risks assessed as critical. Expert weights are calculated as an adjustment factor to the final risk score using the formula as shown in Equation 2.

$$Final\ Priority = (Risk\ Score) + (Expert\ Weight) \quad (2)$$

For example, risk R005 (personal data security) received an Expert Weight of +1, increasing its score from 21.03 to 22.03, while R007 (access failure) received an Expert Weight of +10, bringing its total score to 21.03. These adjustments ensure that risks that are technically critical but perhaps less visible from the survey still receive high priority for mitigation. The researchers conducted a qualitative face validity test involving three expert judges to review the statements previously drafted by the researchers. The results of these three observations were then synthesized based on aspects and indicators to draw conclusions. Furthermore, the researchers revised the wording of several statements deemed in need of improvement based on expert feedback [13].

5) Determination of Final Priority Scale

After completing the risk analysis, the study maps risks into three categories: Very High, High, and Low, which form the basis for subsequent mitigation strategies. This stage produces a prioritized risk mitigation list that forms the basis for designing the blockchain architecture. ISO/IEC 27005 emphasizes the importance

of prioritizing risks and evaluating them in accordance with the organization's objectives [14]. A similar approach is also recommended by NIST SP 800-30 as an important part of the risk assessment process: "identifying, locating, and prioritizing security risks." [15].

6) Blockchain-Based Mitigation Architecture Design

The final step in the research was to design a conceptual blockchain architecture to mitigate information security risks. This design hasn't reached the implementation stage, but it serves as a conceptual model for improving data integrity, process transparency, and service availability through distributed transaction logging.

Junyi Zheng stated that: "This study provides new ideas and guidance for an e-learning blockchain framework... solving the problems of traceability and tamper-evident." This design provides a foundation for a secure and transparent e-learning system through blockchain [16]. Other research has shown that layered blockchain architectures are effective in simplifying implementation while improving scalability and security, particularly in edge or IoT networks—which potentially aligns with the need for layered architectures in online learning [17]. The architecture consists of four main layers:

a) User Layer – Students, lecturers, and administrators access the e-learning system.
b) Application Layer – The e-learning system interacts with the blockchain API.
c) Blockchain Layer – Smart contracts handle validation, access rights, and activity recording.
d) Storage & Security Layer – Data is stored in a distributed ledger with encryption.

3. RESULTS AND DISCUSSION

Data collection, context determination, risk assessment, and risk management are all part of the information security risk management (ISMS) design process at this point.. Based on a business risk perspective, the information security risk management system is a component of the organization's overall management system that aims to create, implement, run, monitor, review, maintain, and enhance information security [18].

3.1. Context Setting

Context setting is the establishment of essential criteria for information security management. The breadth and boundaries of hazards are described by context setting, which is modified according to the degree of information security [19].

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Context determination is the initial activity undertaken to implement the risk management process. At this stage, basic requirements and risk criteria are established.

1) Establishment of Basic Requirements

The techniques used in the Regulation of the Minister of State Apparatus Empowerment and Bureaucratic Reform Number 5 of 2020, which establishes risk management guidelines in electronic government systems, were applied in this study. This approach is based on the company's need to comply with government regulations, as the company wants to diversify its market by providing services to public schools, which are government agencies. This principle is suitable for use by both government agencies and private institutions providing services to government agencies to implement information security risk management. According to the ISACA Journal, the risk assessment process should begin with "a qualitative analysis to determine initial priorities before conducting an in-depth quantitative analysis of the key risks." [20]. Thus, this approach ensures consistency between the legal basis, internal university policies, and the operational needs of the e-learning system.

2) Determination of Risk Criteria

Following the procedures outlined in Regulation No. 5 of 2020 of the Minister of Administrative and Bureaucratic Reform, the research adopted a number of risk criteria based on the predetermined basic requirements. These criteria refer to ISO/IEC 27005:2018 and are adapted to the conditions of the USM e-learning system.

a) Impact Criteria

The impacts absorbed in this study include three impact areas based on the Service, Reputation, and Performance Regulation No. 5 of 2020 of the Minister of Administrative and Bureaucratic Reform. Information security risk management analysis of an academic information system at a public university in Indonesia shows that "setting risk impact and likelihood using ISO/IEC 27005:2018 allows for more precise classification of risks ... especially when combined with stakeholder evaluation and expert judgment." [4]. Table 1 presents the research impact criteria.

Table 1. Impact Criteria

Impact Level

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Impact Area		1 Not Significant	2 Less Significant	3 Moderately Significant	4 Significant	5 Highly Significant
Service	Positive	Increase <20%	Increase 20% to <40%	Increase 40% to <60%	Increase 60% to <80%	Increase ≥ 80%
	Negative	Decrease <20%	Decrease 20% to <40%	Decrease 40% to <60%	Decrease 60% to <80%	Decrease ≥ 80%
Reputation	Positive	Increase <20%	Increase 20% to <40%	Increase 40% to <60%	Increase 60% to <80%	Increase ≥ 80%
	Negative	Decrease <20%	Decrease 20% to <40%	Decrease 40% to <60%	Decrease 60% to <80%	Decrease ≥ 80%
Performan	Positive	Increase <20%	Increase 20% to <40%	Increase 40% to <60%	Increase 60% to <80%	Increase ≥ 80%
	Negative	Decrease <20%	Decrease 20% to <40%	Decrease 40% to <60%	Decrease 60% to <80%	Decrease ≥ 80%

b) Possibility Criteria

The Possibility Criteria adopted in this study are in accordance with the Regulation of the Minister of Administrative and Bureaucratic Reform No. 5 of 2020, namely probabilistic (the opportunity for an event to occur at a certain time) or frequentist (the average number of events in a certain time). This is in line with the findings in Information Technology Risk Management in Educational Institutions Using ISO 31000 Framework that "establishing risk evaluation criteria based on probability and impact is essential for educational institutions to proactively mitigate potential disruptions in service delivery" [21]. As shown in Table 2. the possibility criteria

Table 2. Possibility Criteria

Level of Possibility	Percentage Probability of Occurring in One Year	Number of Possible Frequency of Occurrence in One Year
1 Hardly Ever	X ≤ 5%	X < 2 times
2 Rarely Ever	5% < X ≤ 10%	2 times ≤ X ≤ 5 times
3 Sometimes Ever	10% < X ≤	6 times ≤ X ≤ 9 times
4 Frequently Ever	20% < X ≤ 50%	10 times ≤ X ≤ 12 times
5 Almost Certainly Ever	X > 50%	X > 12 times

c) Analysis Criteria

The combination of impact and likelihood levels in the risk analysis matrix, as an important step in establishing the risk level. The article Determining the context in the risk management process in industrial processes explains that "risk criteria establishment consists of probability and impact criteria used to measure the level of risk" [22]. Table 3 presents the research risk analysis matrix. (Risk Analysis Matrix Table).

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Tabel 3. Risk Analysis Matrix

Risk Analysis Matrics		Impact Level				
		1	2	3	4	5
		Not Significant	Less Significant	Quite Significant	Significant	Very Significant
Likelihood	5 Almost Certain	9	15	18	23	25
	4 Frequently Occurs	6	12	16	19	24
	3 Sometimes Occurs	4	10	14	17	22
	2 Rarely Occurs	2	7	11	13	21
	1 Almost Never Occurs	1	3	5	8	20

d) Risk Level Criteria

Once the risk analysis matrix is obtained, the risk level can be determined. Figure 5 presents the research risk level along with color information for each risk level based in accordance with Regulation No. 5 of 2020 of the Minister of Administrative and Bureaucratic Reform. This is shown in Table 4. Risk Analysis Matrix

Table 4. Risk Analysis Matrix

	Risk Level	Risk Magnitude Range	Information
1	Very Low	1-5	Blue
2	Low	6-10	Green
3	Currently	11-15	Yellow
4	Tall	16-20	Orange
5	Very high	21-25	Red

e) Risk Acceptance Criteria

Drawing from interviews with risk owners, this study establishes the following criteria for risk acceptance: low and very low risks are acceptable, medium risks can be managed, and high and very high risks need to be reduced.

3.2. Risk Assessment

The risk assessment process is carried out through three main stages: identification, analysis, and evaluation of risks in accordance with the SNI ISO/IEC 27005:2022 framework. The integration of quantitative and qualitative approaches is applied to increase the validity of the assessment results, with the support of expert judgment from IT administrators as parties who understand the operational context of the system. The integration of ISO/IEC 27005 with NIST SP 800-30 in the banking and insurance sector emphasizes the importance of dual risk evaluation criteria (quantitative and qualitative) for accurate risk assessment [23].

1) Risk Identification

Initial steps were taken to identify potential threats to USM's e-learning system. Quantitative data were obtained from 42 respondents (students and lecturers), while qualitative data were collected through interviews with five IT experts. The sample size of 42 respondents was deemed adequate for descriptive analysis using a 1–5 Likert scale, as per the guidelines of Kajiwara et al. [24], which state that a sample size of ≥30 is considered appropriate for exploratory studies. However, this study recognized the limited number of respondents compared to the ideal guideline (≥100), due to time constraints and user participation. Therefore, an expert judgment approach was employed to strengthen the validity of the findings and balance the quantitative results with professional perspectives. The risk identification results included 10 risk codes (R001–R010) grouped into four main domains:

a) System Usability & Accessibility (R001, R004, R007, R010)
b) Data Security & Privacy (R002, R005, R008)
c) Procedures & Compliance (R003, R006, R009)
d) System Policies & Guidelines (R009)

2) Risk Analysis

Based on the survey results and expert assessments, an average Likelihood and Impact score was obtained for each risk. The Risk Score = Likelihood × Impact calculation produces a risk classification.

Table 5. Risk Analysis Results of USM E-Learning System Based on ISO/IEC 27005

Risk	Code	Risk Probability	Risk Impact	Likelihood	Impact
System Usability & Accessibility	R001	The e-Learning system is easy to use	If it's difficult to use, it can impact learning.	4,43	4,02
Data Security & Privacy	R002	I feel safe using the system	If it's not secure, it can impact trust.	4,33	4,10
Procedures & Compliance	R003	I understand how to log in/log out	If you don't understand it, it can impact account security.	4,64	4,14
System Usability & Accessibility	R004	Have I ever experienced problems	If it's disrupted, it can impact assignments/exams.	2,57	3,33
Data Security & Privacy	R005	Personal data security is secure	If it's not secure, it can impact privacy/reputation.	4,31	4,88

Risk	Code	Risk Probability	Risk Impact	Likelihood	Impact
Procedures & Compliance	R006	Have I ever forgotten to log out	If you forget to log out, it can impact account misuse.	2,86	3,29
System Usability & Accessibility	R007	Failed to access at a crucial time	If you fail to access it, it can impact academic performance.	3,36	3,29
Data Security & Privacy	R008	Security features are adequate	If it's inadequate, it can impact account hacking.	3,81	4,24
Procedures & Compliance	R009	I understand the policies/guidelines	If you don't understand it, it can impact misuse.	4,17	3,95
System Usability & Accessibility	R010	Have I ever encountered an error message	If there's an error, it can impact work/exams.	2,45	2,93

Risk Score	Expert Weight	Final Priority	Risk Level
17,82	0	17,82	Tall
17,75	0	17,75	Tall
19,23	0	19,23	Tall
8,57	0	8,57	Low
21,03	+1	22,03	Very High
9,39	0	9,39	Low
11,03	+10	21,03	Very High
16,15	0	16,15	Tall
16,47	0	16,47	Tall
7,18	0	7,18	Low

3) Risk Evaluation

The evaluation phase was conducted to determine mitigation priorities based on the Risk Score and Expert Weight. The two main risks with the highest scores were R005 (22.03) and R007 (21.03). Both were categorized as very high risk and therefore became the main mitigation priorities.

Table 6. Risk Evaluation Results based on ISO/IEC 27005:2022

Risk	Risk Description	Priority	Level	Evaluation Decision
R001	The system is difficult to use	17,82	Tall	UX design improvements are needed
R002	Doesn't feel safe using the system	17,75	Tall	Second priority mitigation
R003	Login/logout errors	19,23	Tall	Second priority mitigation
R004	Disruptions while using the system	8,57	Low	Periodic monitoring is sufficient

Risk	Risk Description	Priority	Level	Evaluation Decision
R005	Personal data security is not maintained	22,03	Very High	Immediate mitigation is needed
R006	Forgot to log out of the account	9,39	Low	Auto-logout solution & education
R007	Failed to access important exams/assignments	21,03	Very High	Immediate mitigation is needed
R008	Inadequate security features	16,15	Tall	Strengthen security systems
R009	Doesn't understand system policies	16,47	Tall	Security policy socialization
R010	Error messages interfere with activities	7,18	Low	Periodic technical fixes

Based on the risk evaluation results table, it is divided into 3 priorities:

1. Very high risk R005 & R007 (immediate mitigation required)
2. High risk R003, R002, R001, R008, & R009 (medium priority mitigation required)
3. Low risk R004, R006, & R010 (Periodic monitoring required)

3.3. Integration with ISO/IEC 27005

The use of three main domains (CIA Triad), a combination of quantitative and qualitative data, and mitigation priorities according to operational realities are consistent practices found in previous research on ISMS risk management frameworks with ISO/IEC 27005 [23]. The results of the risk analysis associated with the CIA Triad concept show a mitigation focus on the Confidentiality (R005) and Availability (R007) aspects.

1. Smart Contract → Manages access authorization to protect personal data (mitigates R005).
2. Distributed Ledger → Ensures transaction and record-keeping reliability to prevent access loss (mitigates R007).
3. API Gateway Middleware → Securely connects traditional e-learning systems with blockchain.

3.4. Blockchain Architecture Design for Risk Mitigation

A blockchain architecture design is proposed to strengthen the security of USM's e-learning system. This design consists of four main layers, as shown in Figure 2 below.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

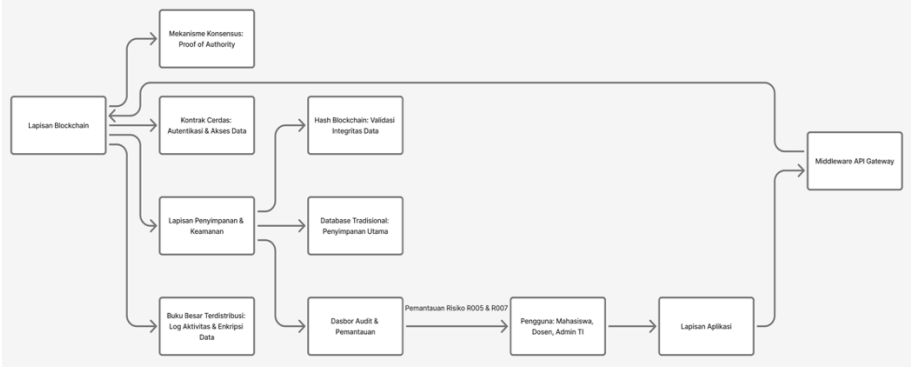

Figure 2. Blockchain Architecture Design of USM E-Learning System

Layer Explanation as follow.

a) User Layer: Students, lecturers, and IT administrators authenticate and access activities.
b) Application Layer: API Gateway verifies each transaction before it is forwarded to the blockchain network.
c) Blockchain Layer: Smart contracts govern access rights and automatic record-keeping. A distributed ledger stores data hashes to maintain integrity. A consensus mechanism (PoA) ensures efficient validation between university nodes.
d) Storage & Security Layer: Encrypted storage, audit logs, and distributed data backup.

Implementation Challenges as follow.

a) Integration with legacy systems requires high compatibility between APIs.
b) Computational resource requirements for blockchain processing remain a technical constraint in university environments.
c) Node management and IT operator training are required to avoid administrative errors.

While this design is conceptual, its effectiveness can be tested through simulation-based validation, for example, by comparing authentication times and access success rates between centralized and blockchain systems. The results of this study align with the findings of Su, Jiahong et al. [25] in the journal Computers & Education: Artificial Intelligence, which showed that implementing a multi-layer blockchain can increase transparency and user trust in digital learning systems without compromising system performance. This approach strengthens the validity of the conceptual design in this study, particularly the implementation of smart contracts and distributed ledgers to mitigate risks R005 (personal data security) and R007 (system access failure at critical times).

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 7. Risk Mapping Results and Mitigation Control Recommendations With Blockchain Architecture

Code	Level	Recommended Mitigation Controls	Blockchain's Role in Mitigation
R005	Very High	- Implement advanced encryption (AES-256). - Regular security audits. - Limit user access rights.	- The blockchain stores hashes of user data to ensure data integrity. - Every data change is permanently recorded in the ledger.
R007	Very High	- Prepare server backups and load balancers. - Implement a failover system. - Conduct regular server stress testing.	- The distributed ledger ensures academic data can be accessed from different nodes in the event of a primary server failure.
R003	Tall	- Implement Multi-Factor Authentication (MFA). - Educate users about login/logout procedures. - Provide login validation features.	- Smart contracts verify user identity before granting access to the e-learning system.
R002	Tall	- Implement TLS/SSL security protocols. - Conduct penetration testing. - Strengthen firewalls and IDS/IPS systems.	- The blockchain increases the transparency of user activity recording, providing greater user security.
R008	Tall	- Add OTP and captcha. - Integrate token-based authentication. - Update security systems regularly.	- Smart contracts validate user access to prevent data manipulation.
R009	Tall	- Provide interactive digital guides. - Disseminate security policies. - Create an automated reminder system.	- The blockchain stores proof of user acceptance of policies in the form of immutable hashes.
R001	Tall	- Make interface improvements (UI/UX). - Add interactive user guides.	- Smart contracts manage authentication processes and access flows to simplify and automate them.
R004	Tall	- Monitor server performance in real time. - Set up an automatic notification mechanism. - Conduct regular system updates.	- Blockchain hashes are used to verify transaction status, making tampering easier to detect.
R006	Low	- Add a time-based auto-logout feature. - Educate users about account security. - Display duplicate login warnings.	- Smart contracts can manage user sessions to automatically close access when idle time expires.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Code	Level	Recommended Mitigation Controls	Blockchain's Role in Mitigation
R010	Low	- Implement an automated bug detection system. - Integrate a ticketing-based error reporting feature. - Update application patches regularly.	- Blockchain logs record error details to facilitate more accurate and faster debugging.

3.5. Regular Monitoring

Periodic monitoring and reviews are conducted to ensure the effectiveness of the designed risk mitigation strategies and to assess whether the risk level is decreasing or increasing over time. This process follows the principles outlined in ISO/IEC 27005:2022, which emphasizes that information risk management is cyclical and must be periodically updated to reflect changes in the environment, technology, and organizational needs. The monitoring process takes into account very high risks (R005 and R007), which require more frequent monitoring than other risks. High-category risks (R001, R002, R003, R008, R009) are reviewed semi-annually, while low-category risks (R004, R006, R010) are evaluated at least annually.

Table 8. Risk Mapping Results and Mitigation Control Recommendations

Code	Level	Mitigation Actions	PIC (Person in Charge)	Review Frequency
R005	Very High	Blockchain implementation for encryption and audit trails	Admin IT & Unit E-Learning	Once / 3 months
R007	Very High	Server optimization, load balancing, and backup systems	Admin IT	Once / 3 months
R003	Tall	Account security education and socialization of login/logout Standard Operating Procedures	Admin IT & Unit E-Learning	Once / 6 months
R002	Tall	Authentication security enhancements and user education	Admin IT	Once / 6 months
R008	Tall	OTP implementation and additional firewalls	Admin IT	Once / 6 months
R009	Tall	Policy socialization, user training, and regular education	Admin IT & Unit E-Learning	Once / 6 months
R001	Tall	UX/UI improvements and user training	Dev E-Learning Team	Once / 6 months
R004	Low	Real-time system performance monitoring	Admin IT	Once / 12 months

Code	Level	Mitigation Actions	PIC (Person in Charge)	Review Frequency
R006	Low	Implementation of auto-logout session timeouts	Admin IT	Once / 12 months
R010	Low	Regular debugging and application code optimization	Dev E-Learning Team	Once / 12 months

This monitoring also takes into account feedback from users and IT administrators through follow-up interviews every six months. The evaluation is conducted to assess the effectiveness of blockchain-based mitigation in improving data integrity, activity transparency, and system audit logs. Monitoring findings will be used to reset risk priority weights if significant changes in risk frequency or impact are detected. Because this research is still in the conceptual design stage, monitoring is conducted using simulations using scenarios based on historical e-learning data. This simulation aims to measure the effectiveness of the blockchain architecture in the context of user activity logging (log integrity) and response to system access failures, which are the root causes of the primary risks (R005 and R007).

3.6. Discussion

The findings of this study highlight two critical vulnerabilities in Semarang University's e-learning system that demand immediate mitigation: R005 – personal data security and R007 – system access failure in critical situations. These risks were identified as having the highest severity, receiving "Very High" classification scores based on the ISO/IEC 27005 risk analysis methodology combined with expert judgment. The results emphasize the urgency of adopting a robust mitigation strategy that not only protects sensitive data but also ensures the continuous availability of services during academic operations. To address this, the research proposes a four-layer blockchain-based architecture that offers a comprehensive, risk-aligned solution to fortify data confidentiality and system reliability.

The proposed architecture includes four primary layers: the User Layer, where students, lecturers, and administrators interact with the system; the Application Layer, responsible for authenticating and verifying user requests via an API Gateway; the Blockchain Layer, where smart contracts govern access, validate transactions, and record them immutably; and the Storage & Security Layer, which provides encrypted, distributed data storage. Together, these layers form an integrated defense mechanism that leverages blockchain's core strengths—immutability, decentralization, and transparency—to address the specific risk domains identified in the system.

For Risk R005 (personal data security), smart contracts play a central role in managing user access rights, encrypting personal data, and ensuring that only verified users can perform actions within the system. By requiring two-layer authentication and logging every activity permanently in a distributed ledger, the architecture significantly reduces the risk of unauthorized access or data breaches. Even in the event of an attempted attack or system anomaly, the transparency and traceability of blockchain ensure that the source of the issue can be identified quickly and accurately. Furthermore, the use of strong cryptographic standards such as AES-256 for data encryption ensures that user data remains secure, even if accessed maliciously.

In the case of Risk R007 (system access failure in critical moments), the blockchain's distributed nature provides a powerful solution. Unlike traditional centralized systems where a single point of failure can cause a complete service outage, a blockchain-based system distributes data and logs across multiple nodes. If one node fails—whether due to technical issues, overload during exam periods, or cyberattacks—the system can still function by routing access through other available nodes. This improves overall system resilience, ensuring that students and faculty retain access to essential services when they need them the most. The implementation of a lightweight consensus mechanism such as Proof of Authority (PoA) allows for rapid validation and synchronization among nodes without compromising performance.

Additionally, a real-time Audit and Monitoring Dashboard further strengthens the system by enabling proactive detection of security anomalies. By analyzing user behavior patterns and transaction logs, IT administrators can identify potential threats—such as brute force attacks or unusual access attempts—before they cause significant harm. This shifts the institution's approach from reactive to preventative, allowing for faster response times and minimizing system disruption. It also aligns with ISO/IEC 27005's emphasis on continuous risk monitoring and response.

The design and findings of this research align closely with those of Kumar, Li, and Wang (2023) in the Computers & Education: Artificial Intelligence journal. Their work highlighted the effectiveness of multi-layer blockchain architectures in promoting trust and transparency within digital learning systems. However, this study differentiates itself by positioning ISO/IEC 27005 risk assessment as the initial design step, ensuring that blockchain implementation is tailored to the most urgent and relevant threats rather than being adopted generically. This approach creates a more purposeful technology application that prioritizes institutional risk realities over technological hype.

Despite its conceptual strengths, implementing this architecture is not without challenges. The first is the computational overhead required to maintain

blockchain operations, particularly during peak usage periods involving thousands of users. University systems, especially in developing regions, may lack the infrastructure to support high-frequency blockchain transactions. Secondly, integration with legacy systems—which still operate on centralized databases—presents technical hurdles in ensuring seamless API communication and data synchronization. Lastly, network readiness and IT training vary across institutions, making distributed node management and smart contract deployment complex and potentially error-prone.

To validate the effectiveness of this conceptual architecture, simulation-based testing using platforms like Hyperledger Fabric or a private Ethereum network is recommended. These environments can model real-world scenarios—such as concurrent logins during exam sessions or unauthorized access attempts—to evaluate the architecture's performance in terms of transaction speed, system availability, and data integrity. Such experimental validation would provide practical insights into whether this blockchain-based solution can scale and function effectively in a university environment.

Ultimately, the integration of ISO/IEC 27005 and blockchain offers more than a technical fix—it presents a systematic, forward-looking approach to information security in digital learning environments. This research contributes a conceptual foundation that aligns risk management with emerging technology, creating a model that is adaptable, secure, and rooted in operational needs. It encourages universities not only to adopt blockchain but to do so with a clear understanding of what risks it addresses and how it can be systematically implemented for long-term resilience.

4. CONCLUSION

This study concludes that the current information security risk management of the University of Semarang (USM) e-learning system, when assessed using the ISO/IEC 27005:2022 framework, reveals critical vulnerabilities—particularly in personal data protection (R005) and system availability during crucial academic moments (R007). These two risks were identified as "very high" and require urgent mitigation. The integrated analysis, which combined quantitative data from user surveys with qualitative expert evaluations, further identified several high and low-level risks that necessitate structured mitigation strategies and ongoing monitoring. These findings underscore the pressing need for universities to adopt not only technical security solutions but also a comprehensive, standards-based approach to risk governance.

In response, this study proposes a conceptual blockchain-based architecture that enhances identity management, data integrity, and service transparency without replacing existing e-learning infrastructure. By leveraging smart contracts and

distributed ledgers, this model offers a layered security framework that aligns directly with ISO/IEC 27005 risk priorities. Beyond its relevance to USM, this model provides a scalable and adaptable solution for other higher education institutions in Indonesia and similar contexts. The research offers a concrete, step-by-step mitigation roadmap that bridges traditional risk management with emerging technologies. For future development, it is recommended that pilot implementations be conducted and supported by AI-driven analytics to enable real-time threat detection and adaptive risk response, thus enhancing both the practical scalability and theoretical value of blockchain-integrated risk management in digital education systems.

REFERENCES

[1] R. Maulana and F. Mahardika, "Analisis risiko keamanan pada sistem e-learning berdasarkan ISO 27005," *Jurnal Informatika, Multimedia dan Teknik*, vol. 2, no. 1, pp. 11–20, Jul. 2025, doi: 10.71456/jimt.v2i1.1362.

[2] M. Bidry, A. Ouaguid, and M. Hanine, "Enhancing e-learning with blockchain: characteristics, projects, and emerging trends," *Future Internet*, vol. 15, no. 9, Sep. 2023, Art. no. 293, doi: 10.3390/fi15090293.

[3] A. A. Nassani, A. Grigorescu, Z. Yousaf, R. A. Trandafir, A. Javed, and M. Haffar, "Leading role of e-learning and blockchain towards privacy and security management: a study of electronics manufacturing firms," *Electronics*, vol. 12, no. 7, Apr. 2023, doi: 10.3390/electronics12071579.

[4] S. Meitarice, L. Febyana, A. Fitriansyah, R. Kurniawan, and R. A. Nugroho, "Risk management analysis of information security in an academic information system at a public university in Indonesia: Implementation of ISO/IEC 27005:2018 and ISO/IEC 27001:2013 security controls," *Journal of Information Technology and Cyber Security*, vol. 2, no. 2, pp. 58–75, Nov. 2024, doi: 10.30996/jitcs.12099.

[5] G. A. Wibowo and A. Y. Vandika, "Development and evaluation of blockchain-based e-learning platforms to improve data security," *Indonesian Journal of Education*, vol. 4, no. 1, pp. 39–53, Apr. 2024.

[6] I. Adhicandra, F. M. Kaaffah, C. H. Maharaja, and S. Sabri, "The impact of implementing blockchain technology in learning on data security and integrity," *Journal of Computer Science Advancements*, vol. 2, no. 1, pp. 1–18, Jul. 2024, doi: 10.70177/jsca.v2i1.927.

[7] J. Bai and Q. Yang, "Design of plasmon absorbing structure suitable for super high frequency," *Electronics*, vol. 12, no. 9, May 2023, doi: 10.3390/electronics12092121.

[8] A. N. Fanani, B. T. Hanggara, and A. R. Perdanakusuma, "Manajemen risiko keamanan informasi menggunakan ISO/IEC 27005 studi kasus pada Dinas Komunikasi dan Informatika Kabupaten Sidoarjo," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 9, no. 6, pp. 2548–2564, 2025.

[9] M. A. Memon, H. Ting, J.-H. Cheah, R. Thurasamy, F. Chuah, and T. H. Cham, "Sample size for survey research: review and recommendations," *Journal of Applied Structural Equation Modeling*, vol. 4, no. 2, pp. 25–45, 2020, doi: 10.47263/jasem.4(2)01.

[10] M. K. Putri and A. R. Hakim, "Perancangan manajemen risiko keamanan informasi layanan jaringan MKP berdasarkan kerangka kerja ISO/IEC 27005:2018 dan NIST SP 800-30 revisi 1," *Jurnal Info Kripto*, vol. 15, 2021.

[11] M. Amirinnisa and R. Bisma, "Analisis penilaian risiko keamanan informasi berdasarkan ISO 27005 untuk persiapan sertifikasi ISO 27001 pada Pemerintah Kota Madiun," 2023.

[12] N. A. Chandra and M. Yusuf, "Penilaian risiko keamanan aplikasi web menggunakan standar ISO/IEC 27005:20022 pada layanan organisasi," *Jurnal Computer Science and Information Technology (COSCITECH)*, vol. 6, Aug. 2025.

[13] V. Sinantia, A. T. Nariswari, I. D. Ramadhani, M. M. Alghifari, K. A. Tjarliman, and Y. K. Qisthi, "Konstruksi alat ukur homesickness pada mahasiswa rantau," *Jurnal Empati*, vol. 13, no. 4, p. 9, Apr. 2024.

[14] ISO, "Information technology — Security techniques — Information security risk management," ISO/IEC 27005:2018, Geneva, Switzerland, 2018.

[15] NIST, "Guide for conducting risk assessments," NIST SP 800-30 Revision 1, Gaithersburg, MD, USA, Sep. 2012, doi: 10.6028/NIST.SP.800-30r1.

[16] J. Zheng, "Blockchain framework for digital learning and information and communications technology," *International Journal of Communication Networks and Information Security*, vol. 16, no. 1, pp. 283–296, 2024.

[17] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Multi-layer blockchain-based security architecture for internet of things," *Sensors*, vol. 21, no. 3, pp. 1–26, Feb. 2021, doi: 10.3390/s21030772.

[18] R. Fauzi, "Implementasi awal sistem manajemen keamanan informasi pada UKM menggunakan kontrol ISO/IEC 27002," *JTERA (Jurnal Teknologi Rekayasa)*, vol. 3, no. 2, pp. 145–156, Dec. 2018, doi: 10.31544/jtera.v3.i2.2018.145-156.

[19] M. L. B. Hikam, F. Dewi, and D. Praditya, "Analisis manajemen risiko informasi menggunakan ISO/IEC 27005:2018 (studi kasus: PT XYZ)," *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, vol. 9, no. 2, pp. 728–734, May 2024, doi: 10.29100/jipi.v9i2.4709.

[20] ISACA, "Qualitative and quantitative risk analysis techniques," *ISACA*, vol. 2, pp. 1–6, 2021.

[21] N. L. Putri and A. F. Wijaya, "Information technology risk management in educational institutions using ISO 31000 framework," *Journal of Information Systems and Informatics*, vol. 5, no. 2, pp. 630–649, May 2023, doi: 10.51519/journalisi.v5i2.468.

[22] Y. J. Raihanah, E. L. E. Napitupulu, and N. D. Q. Aini, "Penentuan konteks dalam proses manajemen risiko pada proses industri," *Journal of Disaster Management and Community Resilience*, vol. 1, no. 1, pp. 28–35, Feb. 2024, doi: 10.61511/jdmcr.v1i1.604.

[23] A. P. Putra and B. Soewito, "Integrated methodology for information security risk management using ISO 27005:2018 and NIST SP 800-30 for insurance sector," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 14, no. 4, pp. 415–422, 2023.

[24] Y. Kajiwara, A. Matsuoka, and F. Shinbo, "Machine learning role playing game: Instructional design of AI education for age-appropriate in K-12 and beyond," *Computers and Education: Artificial Intelligence*, vol. 5, Jan. 2023, Art. no. 100162, doi: 10.1016/j.caeai.2023.100162.

[25] J. Su, D. T. K. Ng, and S. K. W. Chu, "Artificial intelligence (AI) literacy in early childhood education: The challenges and opportunities," *Computers and Education: Artificial Intelligence*, vol. 5, Jan. 2023, Art. no. 100124, doi: 10.1016/j.caeai.2023.100124.