Advance Sustainable Science, Engineering and Technology (ASSET)
Vol. 8, No.3, July 2026, pp. 02603017-01 ~ 02603017-015
ISSN: 2715-4211 DOI: https://doi.org/10.26877/asset.v8i3.2912

A CIA-based Sustainable Security Risk Mitigation Model for E-Certificate Systems

Teguh Nurhadi Suharsono[1*], John Choi[2], Raden Ricky Agusiady[3], Didin Saepudin[3], Sukadwilinda[4], Heri Purwanto[1], Peti Savitri[5], Ketut Abimanyu Munastha[1]

[1]Faculty of Engineering, Universitas Sangga Buana, Jl. PHH Mustofa No 68, Bandung 40124, Indonesia

[2]MarkAny Co., Ltd., Seoul, South Korea

[3]Postgraduate Directorate, Universitas Sangga Buana, Jl. PHH Mustofa No 68, Bandung 40124, Indonesia

[4]Faculty of Economics, Universitas Sangga Buana, Jl. PHH Mustofa No 68, Bandung 40124, Indonesia

[5]Vocational Directorate, Universitas Sangga Buana, Jl. PHH Mustofa No 68, Bandung 40124, Indonesia

*teguh.nurhadi@usbypkp.ac.id

Abstract. E-certificates are increasingly adopted across sectors, yet existing studies have not developed an integrated risk mitigation model that combines CIA-based sustainable security with operational and stakeholder perspectives. Current frameworks primarily address isolated technical risks or focus on general PKI security, leaving a gap in holistic modeling tailored to end-to-end e-certificate implementation. This study addresses this gap by proposing a Sustainable Security Risk Mitigation Model for e-certificate systems, guided by the CIA triad—Confidentiality, Integrity, and Availability. A mixed-methods approach was employed, including literature analysis, a Focus Group Discussion (FGD) with industry, government, and academic stakeholders, and expert evaluation using CIA-based scoring on a Likert scale. The empirical data include qualitative perspectives gathered from the FGD and quantitative assessments from expert validation. The proposed model operates in a continuous cycle consisting of risk assessment, mitigation planning, deployment and monitoring, and iterative improvement, ensuring that security controls adapt to emerging threats. Results show that the model achieves an average security validation score (asv) of 4.67, outperforming other existing risk mitigation models in CIA-based evaluation. The findings indicate that institutions can use the model as a practical framework to strengthen e-certificate governance, improve resilience against cyber threats, and support sustainable information security management.

Keywords: e-certificate systems, sustainable information security, CIA triad, cyber risk mitigation, information security modelling, public key infrastructure (PKI)

(Received 2025-10-27, Revised 2025-12-10, Accepted 2026-05-04, Available Online by 2026-06-03)

1. Introduction

The increasing adoption of e-certificates across education, government, and industrial sectors reflects a growing demand for secure, efficient, and scalable credential management systems. Compared with paper-based certificates, e-certificates offer faster processing, lower administrative costs, and improved verification procedures. However, these benefits are accompanied by significant risks related to data confidentiality, document integrity, and system availability—three domains traditionally defined by the CIA triad [1].

There have been several previous studies that have researched this e-certacte system. E-certificates have been researched in various contexts in recent years. The first study describes the impact and constraints of implementing government policies in e-certification led by the Electronic Certification Board (BSE) [2]. Other research proposes the use of RSA digital signatures to authenticate electronic certificates and prevent forgery [3]. The next research explains that the Digital Certificate Authority (OSD) is a certification body owned by the Electronic Certification Center (BSrE) of the State Cyber and Cryptography Agency (BSSN). Digital certificate management is the main business process of the Universal Service Digital Certificate Authority (OSD LU) which if there is a disruption, the OSD business process cannot run smoothly and has an impact on the digital certification process. With problems in maintaining the reliability and security of the system, an effort is needed to classify, analyze, and manage these risks appropriately in order to reduce the negative impact that may arise at an acceptable level. The main goal is to overcome problems regarding risk management planning, especially if there is no information security risk management plan in the BsrE environment [4]. Another study assessed the security risks in the Malaysian e-Passport PKI and recommended the implementation of PACE and following ICAO standards to improve security [5]. Another study conducted a probabilistic approach to quantitative risk assessment in X.509 PKI to address security risks in certificate-based security [6].

Despite various contributions, no existing work has developed a holistic risk mitigation model that integrates CIA-based sustainable security, stakeholder perspectives, and operational risks throughout the end-to-end e-certificate lifecycle [7]. This gap is especially critical as institutions increasingly rely on digital certification systems that require continuous, adaptive, and sustainability-oriented security controls.

This study addresses the identified gap by pursuing several research objectives. First, it aims to identify key risks in e-certificate implementation related to confidentiality, integrity, and availability (CIA). Second, it seeks to design an integrated and sustainable security risk mitigation model that incorporates technical, operational, and stakeholder perspectives. Finally, the study intends to validate the proposed model through expert CIA-based assessment and to compare its performance with existing risk mitigation frameworks.

This article is an original modeling study, not a review paper. Its contributions include: (i) proposing a CIA-integrated sustainable security model tailored to e-certificate systems; (ii) incorporating empirical insights from a multi-stakeholder Focus Group Discussion (FGD); and (iii) providing comparative validation against established risk mitigation models. The remainder of this paper is structured as follows: Section 2 describes the mixed-methods approach used in the study; Section 3 presents the proposed risk mitigation model; Section 4 reports the evaluation and comparison results; and Section 5 concludes with implications for practice.

2. Methods

This study employed a mixed-methods design that integrates qualitative data from a Focus Group Discussion (FGD) with quantitative expert assessment using CIA-based scoring [8-10]. The methodological approach follows a modeling-oriented epistemological stance, in which empirical inputs (literature review, stakeholder perspectives, and expert judgment) are used to construct and validate a conceptual mitigation model rather than to perform large-scale statistical testing. All methodological steps presented below describe the actual procedures applied during the research [11-13].

The methods applied in this study consist of several stages/procedures, namely literature study, focus group discussion, data analysis, development of risk mitigation modeling, and evaluation along with targeted achievement indicators at each stage of research as shown in Figure 1.

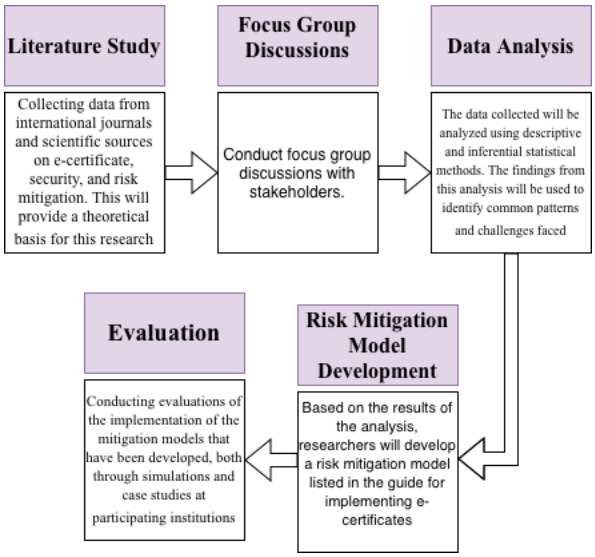

Figure 1. Research Stages

This research will use qualitative and quantitative approaches. The methods to be carried out include:

2.1. Literature Study

The literature review was conducted to identify security challenges, digital certificate frameworks, PKI mechanisms, and risk mitigation models relevant to e-certificate systems. Three major scientific databases were used: Scopus, IEEE Xplore, and Web of Science, covering publications from 2018 to 2025. Keywords included “e-certificate security”, “PKI”, “CIA triad”, “risk mitigation model”, “digital certificate”, “sustainable security”, and “cybersecurity risk management”. Studies were included if they: (i) addressed digital certificates or PKI security; (ii) proposed or evaluated risk mitigation frameworks; or (iii) discussed CIA-related security mechanisms. Publications focusing solely on social, pedagogical, or non-technical certificate contexts were excluded.

The review served two purposes: (1) to build contextual understanding of risks in e-certificate systems; and (2) to identify structural and conceptual components that inform the design of the proposed risk mitigation model.

2.2. Focus Group Discussion (FGD):

The FGD involved 12 participants representing key stakeholder groups in e-certificate ecosystems:

- Government agencies (State Cyber and Cryptography Agency; Ministry of Digital Communication) – 4 participants

- Industry (MarkAny Co., Ltd., specializing in certificate and content security) – 3 participants
- Higher education institutions (Universitas Sangga Buana and Universiti Utara Malaysia) – 5 participants.

Participants were purposively selected based on their involvement in digital certificate issuance, cybersecurity, or institutional policy-making. The FGD was conducted during the International Symposium on the Urgency of E-Certificate Interest in Digital Transformation and lasted two hours. A semi-structured protocol was employed, covering themes such as existing challenges in e-certificate systems, technical and operational risks, concerns related to validity and authenticity, and requirements for a sustainable CIA-oriented model. The sessions were audio-recorded with informed consent and supplemented by detailed moderator notes.

2.3. Data Analysis

The FGD data were analyzed using thematic content analysis. Transcripts were coded independently by two researchers, who identified categories related to confidentiality threats, integrity issues, availability concerns, and operational or policy-driven risks. Disagreements were resolved through discussion to ensure coding reliability. Ethical considerations included anonymization of institutions and participants, secure storage of transcripts, and confidentiality agreements for all researchers.

2.4. Development of Risk Mitigation Models

Risk scenarios were derived from the literature review and FGD results. Threats were categorized under the CIA triad and operationalized into measurable indicators, including confidentiality aspects such as unauthorized access attempts and encryption failure points, integrity aspects such as tampering risks, digital signature vulnerabilities, and data modification pathways, and availability aspects such as system downtime, recovery latency, and the threat of denial-of-service attacks. These indicators formed the basis for the architecture of the Sustainable Security Model, which integrates continuous assessment, mitigation planning, deployment, and improvement.

2.5. Evaluation

Evaluate the application of mitigation models that have been developed, both through simulations and case studies in participating institutions. To validate the model, six experts were recruited, two cybersecurity specialists from a national cyber agency, two PKI experts from industry (MarkAny), and two information-security academics with publications on CIA-based modeling.[RR2.1] Experts had 8–20 years of experience in cybersecurity or PKI infrastructure.

Each expert independently scored the proposed model using a 5-point Likert scale (1 = very weak to 5 = very strong) for the following criteria: protection of Confidentiality (C), protection of Integrity (I), and protection of Availability (A). [RR3.1] Scores were aggregated by computing the average for each criterion. Inter-rater variation was examined by calculating the standard deviation; all SD values were below 0.5, indicating acceptable consistency.

The average security validation (asv) score was calculated using: $asv = (C + I + A) / 3$, where C mean expert score for Confidentiality, I mean expert score for Integrity, and A mean expert score for Availability.

An asv score above 4.0 was interpreted as “high security performance” based on thresholds used in prior CIA-based evaluation studies. The qualitative results (FGD themes and literature insights) informed the construction of the model components, while the quantitative CIA scoring provided empirical validation of its performance. Integration occurred at the interpretation stage, where model efficacy was assessed through pattern convergence between stakeholder concerns, risk indicators, and expert-based evaluations.

3. Results and Discussion

3.1. Study Literature

The literature review produced three main insights that directly informed the model design. First, studies on PKI and digital signatures highlight the need for cryptographically verifiable integrity and non-repudiation, motivating the inclusion of strong integrity controls in the proposed model. Second, research on cybersecurity risk management (e.g., ISO 27005, NIST SP 800-30) emphasizes iterative and continuous cycles, but these frameworks do not explicitly integrate the CIA triad as a dynamic set of interlinked pillars. Third, morphological and probabilistic modeling approaches demonstrate the value of scenario-based evaluation, which guided the comparison phase of this study.

Accordingly, rather than restating the full content of earlier works, the present section highlights the conceptual foundations that shaped the model architecture: a CIA-oriented structure, iterative lifecycle logic, and integration of stakeholder-driven risks. [7]. The following research resulted in 16 risk sources and 17 risk mitigation measures grouped into five clusters, namely prework, execution, monitoring, regulation, and automation. The results of the ANP BOCR show that the execution cluster is the top priority in the implementation of mitigation measures with a score of 38.57 [14-17]. The next research is to elaborate and evaluate various RM scenarios from initial risk identification and priority solutions. The proposed scenario modeling technique is based on morphological analysis (MA) as an exploratory scenario tool for RM. The MA is used to develop a framework to proactively assess critical risk variables. First, the MA is used to create a comprehensively possible RM scenario and, second, to assess the likelihood of each scenario. The proposed approach addresses the need for a basic rubric to help identify and select an RM approach. A real-life case study from the food industry is provided to illustrate the application of the proposed approach. To handle all possible MA strategies, a special MORPHOL software package is used. In addition, Risk Management (RM) strategies are selected based on sustainability indicators. The results of the case study prove that MA has significant value for SCRM. This shows that companies can adopt some robust strategies in the form of scenarios that describe all stages of SCRM in an integrated representation [18-20]. Several studies have not discussed risk mitigation modelling for sustainable security in the implementation of e-certificates.

3.2. Focus Group Discussion (FGD)

3.2.1. Key Themes and Illustrative Quotes

Thematic analysis of the FGD produced four prominent risk themes:

1. Confidentiality threats (11 of 12 participants mentioned)
2. Integrity risks and document tampering (10 of 12 participants)
3. Availability and system continuity concerns (8 of 12 participants)
4. Operational and policy misalignment (9 of 12 participants)

Selected participant quotes include:

- "*Our biggest concern is unauthorized copying or forging of issued certificates." — Government agency participant*
- "*If the verification service goes down, universities cannot authenticate graduates during peak periods*." — Higher education participant
- "*Stakeholders need a structured model, not just security tools*." — Industry participant (MarkAny).

These empirical insights guided prioritization of controls within the model: confidentiality for access control, integrity for verification mechanisms, and availability for service continuity.

The FGD was carried out through the International Symposium "The Urgency of e-certificate Interest in Digital Transformation". The FGD activities were attended by several stakeholders, namely:

- MarkAny Co., Ltd., South Korea which is engaged in system security that already has a system in the management of e-certificate security.
- Universitas Sangga Buana from the education sector has prepared the implementation of e-certificates.

- Speakers from Universiti Utara Malaysia who gave their views on the implementation of e-certificates in Malaysia.
- Speakers from the State Cryptography and Cyber Agency of the Republic of Indonesia related to government policies on the use of e-certificates and their risks and security
- Speakers from the Ministry of Digital Communication who discussed the policy for the use of e-certificates in Indonesia.

3.2.2. Influence on Model Components

FGD results directly shaped the model in several ways. Confidentiality emphasis is reflected in stronger encryption layers and multi-factor access control. Integrity emphasis is reflected in the inclusion of digital signatures (RSA/ECDSA), hash-chain validation, and optional blockchain audit trails. Availability emphasis is reflected in multi-zone replication, auto-failover mechanisms, and disaster recovery integration. Operational risk findings are reflected in the integration of stakeholder-based feedback loops in the "Monitoring and Improvement" phase.

3.3. Data Analysis

Based on the data that has been collected related to primary data (FGD results) and secondary data (based on theories from journals and other scientific sources), it is successfully analyzed as follows.

3.3.1. Challenges of e-certificate implementation

The main challenges in the implementation of e-certificates revolve around security issues including data security, authenticity, and verification in the midst of rapid digitalization, namely:

3.3.1.1. Data Security and Cyber Threats

The most fundamental challenge is to maintain the security of sensitive data contained in or related to e-certificates. These risks include cybersecurity threats, referring to the vulnerability of the system to cyberattacks; business process disruption, referring to disruption to the digital certificate management system, which can impact the Digital Certificate Authority (OSD) business processes; and system reliability violations, referring to the need for continuous efforts to maintain the reliability and security of certificate issuance and management systems.

3.3.1.2. Authenticity and Fraud Prevention

Although e-certificates are intended to increase security over paper certificates, there are major challenges in ensuring the authenticity of documents and preventing counterfeiting. These challenges include vulnerability to digital fraud, which is a serious issue that arises from attempts to compromise e-certificates, and the authenticity verification challenge, which involves developing an efficient and trusted way to verify that the e-certificate presented is genuine and legitimate.

3.3.1.2. Accessibility and Management

The implementation of e-certificates also poses operational and technical challenges related to access and management. These include accessibility, which requires ensuring that certificates are accessible to authorities anytime and anywhere, and risk management, which involves the need for efforts to classify, analyze, and manage risks appropriately to reduce the negative impacts that may arise. This also includes addressing the problem of risk management planning, especially if there is no adequate information security plan in place. These challenges require the development of an integrated and holistic risk mitigation model, which not only focuses on the technical aspects, but also considers the perspectives of stakeholders and operational risks [20].

3.3.2. Risks of e-certificate implementation

The risks of e-certificate implementation are basically divided into three main categories: data security risks, document authenticity risks, and operational/managerial risks.

3.3.2.1. Data and Cyber Security Risks

This is a major risk related to the protection of sensitive information. The implementation of e-certificates is faced with cybersecurity threats that can disrupt systems and data. The main business process of Digital Certificate Management, which is carried out by the Universal Service Digital

Certificate Authority (OSD LU), is at risk of disruption. If this happens, OSD's business processes cannot run smoothly and impact the digital certification process. Risks are related to maintaining the confidentiality and integrity of the data used in the e-certificate system.

3.3.2.2. Authenticity and Trust Risks

Although e-certificates are designed to be more secure, the risks associated with counterfeiting still exist. Risk that the issued certificate may not be original or has been modified illegally. The emergence of issues such as vulnerability to digital fraud. Difficulties in verifying the authenticity of e-certificates quickly and reliably.

3.3.2.3. Managerial and Operational Risks

These risks are related to the planning, management, and implementation of the system itself in the institutional environment. Problems arise especially if there is no information security risk management plan in the implementing agency. The need for efforts to appropriately classify, analyse and manage risks to reduce the negative impacts that may arise to an acceptable level. Risks related to technical or operational issues that impede accessibility for users or authorities.

3.3.3. Mitigation that can be done

In general, risk mitigation for the implementation of e-certificates that can be carried out includes the development of integrated mitigation models, technical security risk mitigation, and mitigation of operational and business process risks.

The most important mitigation is the development of a comprehensive framework. Integrated Mitigation Model: This research aims primarily to develop an integrated risk mitigation model, which enables institutions to make more informational decisions. Holistic Approach: This model not only focuses on the technical aspects, but also considers the perspective of stakeholders and risks from the operational side. Implementation Guide: The developed risk mitigation model will be listed in the form of a guide for the implementation of e-certificates [RR2.1]

It includes measures to strengthen authenticity and prevent cyberattacks. Use of Digital Signatures: Previous research has proposed the use of RSA digital signatures to authenticate electronic certificates and prevent counterfeiting. Implementation of Security Standards: Security risk mitigation in Public Key Infrastructure (PKI) (such as e-Passports) can be improved by implementing protocols such as PACE and following ICAO standards. Information Security Risk Management Planning: Efforts are needed to overcome the problem of risk management planning, especially if there is no adequate information security plan in the implementing environment (e.g. BsrE).

This mitigation is related to improving procedures and overall system management. Risk Classification and Analysis: Efforts are needed to appropriately classify, analyze, and manage these risks in order to reduce the negative impacts that may arise at an acceptable level. Focus on Execution Clusters: Based on business process risk mitigation research, execution clusters (execution) are the top priority in the implementation of mitigation measures. Risk Management (RM) Strategies: Mitigation can involve a Risk Management (RM) strategy selected based on sustainability indicators and the use of scenario modelling techniques (such as Morphological Analysis/MA) to proactively assess critical risk variables.

Data from literature and FGD were merged into three main risk categories aligned with the CIA triad: Data and Cybersecurity Risks (C), Authenticity and Integrity Risks (I), and Operational and Managerial Risks (A). Data and Cybersecurity Risks (C) include Unauthorized access attempts, Weak encryption schemes, and Exposure of certificate metadata. Authenticity and Integrity Risks (I) include Tampering of certificate contents, Forged digital signatures, and Inadequate revocation mechanisms. Operational and Managerial Risks (A) include System downtime, Slow verification processes, and Insufficient policy and governance controls.

Quantitatively, risk mentions were tallied during coding: confidentiality risks (23 mentions), integrity risks (19 mentions), availability risks (17 mentions). These frequencies provide justification for the CIA prioritization in model design.

3.4. Development of Risk Mitigation Models

The development of risk mitigation models for e-certificates that focus on ongoing security handling, especially those related to CIA (Confidentiality, Integrity, Availability) principles, involves a layered approach and lifecycle. Here is a visualization and explanation of the model as shown in figure 2.

Figure 2. A Sustainable Security Model for E-Certificate Implementation

Figure 2 depicts a dynamic risk mitigation model that focuses on the sustainability of CIA (Confidentiality, Integrity, Availability) protection throughout the e-certificate lifecycle. The core components of the model consist of the Sustainable Security Model and the CIA gear.

The Sustainable Security Model is at the heart of the approach, showing that security is not a one-time goal, but a process that is constantly being adjusted and improved. The CIA gear, represented by three interconnected gears, illustrates the principles of Confidentiality, Integrity, and Availability, emphasizing that these three pillars must work together synergistically to achieve solid security.

The model operates in a continuous cycle consisting of four main phases. The first phase is Risk Assessment, which includes identifying and analyzing potential threats to e-certificates. This initial phase involves gathering threat intelligence to understand the current and future threat landscape and identifying how threats may compromise the confidentiality, integrity, or availability of e-certificates.

The second phase is Mitigation Planning, which involves strategizing and prioritizing mitigation actions based on the results of the risk assessment. This phase includes developing specific security controls and planning for the implementation of controls such as the use of blockchain for data integrity, encryption for confidentiality, and strong backups for availability.

The third phase is Deployment and Monitoring, where planned security controls are implemented on the e-certificate system. Once implemented, the performance of these controls is continuously monitored to ensure their effectiveness. This includes implementing digital signatures to ensure integrity, access control for confidentiality, and availability solutions such as data replication.

The fourth phase is Monitoring and Improvement, which focuses on continuous evaluation through audit, feedback, and adaptation. Regular audits are conducted, feedback from security incidents or environmental changes is collected, and adjustments are made to security models or controls. This closes the cycle and ensures the model remains relevant and effective against evolving threats, while evaluating

the effectiveness of all controls related to confidentiality, integrity, and availability, and adapting them over time.

Supporting Technology and Strategy include threat intelligence, digital signatures, access control, blockchain, and a continuous feedback loop. Threat intelligence supplies threat information to the risk assessment phase. Digital signatures are key controls to ensure the integrity and authenticity of e-certificates. Access control is important to maintain confidentiality by restricting access to only authorized parties. Blockchain is a technology that can greatly improve the integrity and universal verifiability of e-certificates by providing an immutable ledger. The continuous feedback loop, represented by interconnected arrows between the phases, demonstrates the iterative and adaptive nature of this model.

This model covers the entire e-certificate lifecycle, including issuance, which is when a certificate is created; usage, which refers to how the certificate is used by the recipient; verification, which is the process of validating the authenticity of the certificate; and archiving, which refers to the long-term storage of certificates. This model emphasizes that e-certificate security is not a completed checklist, but rather an ongoing journey that requires constant risk assessment, planning, implementation, and improvement to keep the CIA pillars strong amid evolving cyber threats.

3.5. Evaluation

Based on the risk mitigation model that focuses on sustainable security handling for e-certificates and CIA (Confidentiality, Integrity, Availability) principles, evaluation is a critical phase that closes the security cycle and ensures that the model remains effective. Evaluation in this model is not done only once, but is an ongoing and iterative process.

The evaluation phase is essentially the Monitoring and Improvement phase (which measures how well the mitigation controls that have been implemented (in the Deployment and Monitoring phase) successfully protect the CIA pillar. The main objective of this evaluation is to achieve sustainable security. Evaluation Methods and Objectives are in Table 1.

Table 1. Evaluation Methods and Objectives

CIA Pillar	Evaluation Focus	Evaluation Method
Confidentiality	Measure the success of access control in preventing unauthorized access to certificate data.	Penetration Testing: Simulates an external attack to find loopholes in access control and encryption. Access Audit: Checks system logs to ensure only authorized users are accessing data.
Integrity	Measure the reliability of document forgery and modification prevention mechanisms.	Digital Signature Audit: Ensures the digital signature mechanism is functioning correctly and that no certificate is modified undetected. Blockchain Verification: If used, verifies the consistency of the ledger data to guarantee the original data.
Availability	Measures the system's ability to operate and be accessed by legitimate users without interruption.	Load Testing: Simulates a high volume of users to test system stability. Disaster Recovery Test: Tests the time it takes to

CIA Pillar	Evaluation Focus	Evaluation Method
		restore systems and data (e-certificate from backup) after a major incident.

The evaluation phase involves three main activities aimed at closing the security cycle, namely routine audit, feedback collection, and adaptation. Routine audit involves conducting periodic checks of all security controls implemented and ensuring that security policies and operational procedures are strictly followed.

Feedback collection involves collecting data on security incidents that occurred during the monitoring period and seeking input from stakeholders (e.g. users, administrators, and regulators) regarding the challenges or shortcomings they face when using the system.

Adaptation involves adjusting and improving the mitigation model based on the results of the audit and feedback. If a new threat emerges (new Threat Intelligence), the mitigation controls are updated, and the mitigation cycle is restarted from the Risk Assessment phase.

Evaluations must be ongoing because of ever-evolving threats, system changes, and the need to ensure security return on investment. Cyberattacks and hacking methods are constantly changing, and evaluation ensures the mitigation model remains relevant against the latest threats. E-certificates and their supporting systems, including cloud infrastructure and software, will undergo updates, and evaluation validates that these updates do not introduce new vulnerabilities. In addition, evaluation helps institutions assess whether investments in mitigation controls provide commensurate protection benefits.

Thus, evaluation serves as a safety valve and a learning mechanism that encourages continuous improvement, guaranteeing that the e-certificate system achieves and maintains the desired level of security.

Based on the modeling proposed in the study, an analysis was carried out with other studies as shown in table 2 below.

Table 2. Comparison with other Studies

No	Modeling	Result	Similarities	Difference
1	International Construction Project Risk Mitigation Modeling [21]	This study on risk mitigation in **international construction projects** carried out by Indian companies resulted in a model that helps construction companies to emphasize several risk mitigation methods	Focuses on developing models that provide guidance or emphasis on **mitigation methods** to reduce risk and improve performance	The proposed e-certificate model focuses on **sustainable security** surrounding the CIA (Confidentiality, Integrity, Availability) pillars, the construction model is more oriented towards project risks in general (e.g. financial, operational, or political risks in an international context) to

No	Modeling	Result	Similarities	Difference
				improve project performance.
2	Order Fulfillment Business Process Risk Mitigation Model [22]	This research on risk mitigation in **the Order Fulfillment business process** in a company resulted in 16 risk sources and 17 mitigation steps grouped into five clusters	This study uses **the Analytic Network Process (ANP) BOCR** (Benefits, Opportunities, Costs, Risks) to determine mitigation priorities. Mitigation clusters are grouped into prework, **execution**, monitoring, regulation, and automation. Execution clusters are the top priority with the highest scores. This is similar to the e-certificate model which emphasizes the importance of **the Deployment and Monitoring** phases (implementation and monitoring)	The proposed e-certificate mitigation model explicitly prioritizes security (CIA) throughout its lifecycle, while the order fulfillment model focuses on optimizing business processes to improve efficiency and reduce operational losses.
3	A Probabilistic Approach to Certificate-Based Security Risk Assessment (Public Key Infrastructure) [23]	This study proposes a **probabilistic** approach to quantitative risk assessment in X.509 Public Key Infrastructure (PKI) to address certificate-based security risks	Discuss security risks in the context of **digital certificates** and Public Key Infrastructure (PKI). The goal is to improve security	The research on PKI uses **a probabilistic quantitative** approach RiskLaine) to assess security risks, while this e-certificate research adopts **a mixed method (qualitative and quantitative)** and a **holistic** approach that focuses not only on technical but also operational and stakeholder approaches.
4	Risk Management Scenario Modeling [24]	This study elaborates and evaluates various Risk Management	Emphasizing the concept **of sustainability, the** e-certificate model uses	The MA research uses **exploratory scenario modeling** through

No	Modeling	Result	Similarities	Difference
		(RM) scenarios using **Morphological Analysis (MA)** techniques to proactively assess critical risk variables, and selects RM strategies based on **sustainability indicators**	the term Sustainable Security Model which shows that mitigation is a dynamic process that continues to adapt.	a custom software package (MORPHOL) to describe all stages of Supply Chain Risk Management (SCRM), while the e-certificate research uses a **four-phase continuous cycle** (Risk Assessment to Improvement) powered by technologies such as Digital Signatures and Blockchain

This research is unique in that it develops an integrated risk mitigation model that focuses specifically on the implementation of e-certificates, combining technical aspects (CIA, Blockchain) with operational/managerial aspects (planning, execution priorities). Based on Table 1, an assessment of all the modelling was carried out, with CIA criteria to demonstrate the achievement of sustainable security. The range of values based on the Likert scale is between 1 to 5 values [25]. Based on these criteria, the average security validation score (asv) is calculated based on the formula:

$$asv = \frac{(c+i+a)}{3} \qquad (1)$$

The resulting asv value provides a quantitative representation of the overall validation results of the model, which allows comparison between different configurations or expert perceptions, asv values above 4.0 (on a 5-point scale) indicate that the model has successful Confidentiality, reliable Integrity, uninterrupted Availability so that sustainable security is achieved. Based on formula (1), the results are obtained as shown in Table 3 below.

Table 3. Modeling calculation results with CIA criteria

No	Modeling	Criterion			asv Score
		C	I	A	
1	International Construction Project Risk Mitigation Modeling	4.5	3.75	4.75	4.33
2	Order Fulfillment Business Process Risk Mitigation Model	4.75	3.75	4.75	4.42
3	A Probabilistic Approach to Certificate-Based Security Risk Assessment (Public Key Infrastructure)	4.5	4.25	4.75	4.50
4	Risk Management Scenario Modeling	4.25	4.5	4.5	4.42

5	Risk mitigation modeling for sustainable security in e-certificate implementation	4.75	4.5	4.75	4.67

Based on Table 3, the results can be seen in the form of a graph as shown in Figure 3.

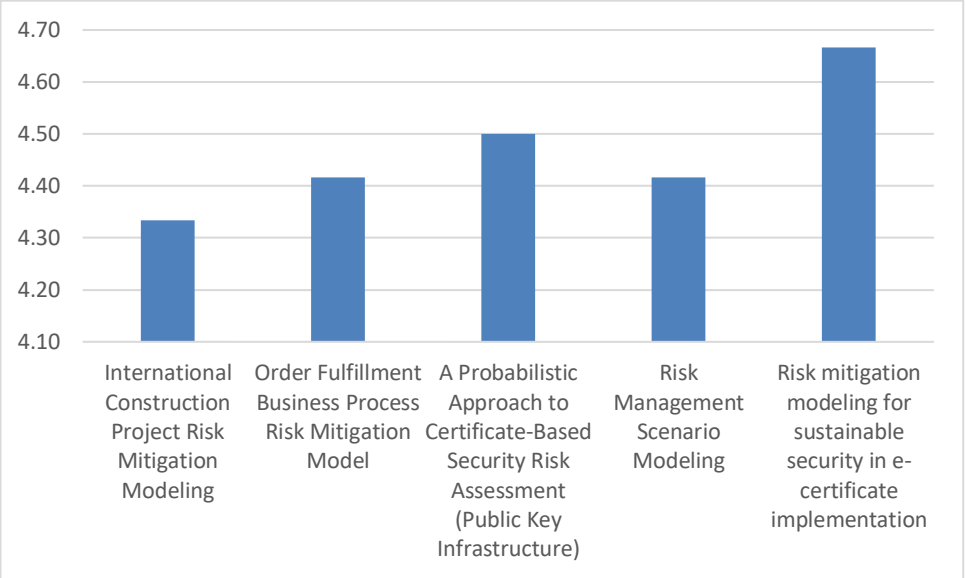

Figure 3. Graph of asv Calculation Results

Based on table 3 and figure 3, it can be seen that the proposed mitigation modeling from this study has an advantage with a result of 4.67. This shows that the risk mitigation modeling developed in this study has successful confidentiality, reliable integrity, and uninterrupted availability so that sustainable security is achieved."

4. Conclusion

This study proposed an integrated Sustainable Security Risk Mitigation Model for e-certificate systems that places the CIA triad—Confidentiality, Integrity, and Availability—at the core of a continuous security lifecycle. Unlike existing approaches that focus on isolated technical or organizational aspects, the proposed model holistically combines stakeholder insights, operational risks, and technical safeguards, resulting in a structured and adaptive framework for secure e-certificate implementation.

The main contribution of this work lies in the development of a CIA-integrated lifecycle model tailored specifically for e-certificate environments, its grounding in empirical stakeholder input, and its validation through expert scoring using a standardized rubric. The model demonstrated strong performance, achieving an asv score of 4.67, indicating robust CIA coverage compared with other existing risk mitigation frameworks.

However, this research has several limitations. The empirical component relied on a single FGD event involving stakeholders from a limited geographical context and a relatively small number of experts. In addition, the evaluation was conducted using expert judgment rather than real-world implementation, and the study did not include longitudinal or simulation-based testing.

Future research should focus on piloting the model across multiple institutions, sectors, and countries to assess its practical effectiveness under different regulatory and operational environments. Further development may also include integration with automated monitoring tools such as SIEM platforms, incorporation of real-time threat intelligence engines, and alignment with international standards such as ISO 27005 or NIST cybersecurity frameworks. Long-term testing and iterative

refinement based on system performance data will be essential to further strengthen the model's sustainability and resilience.

Declaration of AI and AI assisted technologies in the writing process
The authors confirm that this manuscript was prepared without the assistance of artificial intelligence (AI) tools or AI-assisted technologies. All writing, analysis, interpretation, and revision processes were conducted solely by the authors

Declaration of Competing Interest
The 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.

Acknowledgements
Thank you to MarkAny Co.,Ltd., South Korea for providing research funding through the 2025 Research Grant.

References

[1] Winny Wiriani, "Positive Impact of Administrative Modernization in Land in Indonesia," International Journal of Innovative Research in Multidisciplinary Education, vol. 03, no. 06, Jun. 2024, doi: https://doi.org/10.58806/ijirme.2024.v3i6n16.

[2] S. Mubarak, S. Zauhar, S. Suryadi, and E. Setyowati, "Impacts and constraints on implementing e-certification policies in Indonesia," Kasetsart Journal of Social Sciences, vol. 43, no. 3, 2022, doi: https://doi.org/10.34044/j.kjss.2022.43.3.20.

[3] K. Somsuk and M. Thakong, "Authentication system for e-certificate by using RSA's digital signature," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 18, no. 6, p. 2948, Dec. 2020, doi: https://doi.org/10.12928/telkomnika.v18i6.17278.

[4] D. I. Sensuse, A. Syahrizal, F. Aditya, and M. Nazri, "Information Security Risk Management Planning of Digital Certificate Management Case Study: Balai Sertifikasi Elektronik," in 2020 Fifth International Conference on Informatics and Computing (ICIC), IEEE, Nov. 2020, pp. 1–7. doi: https://doi.org/10.1109/ICIC50835.2020.9288593.

[5] A. I. H. bin Suhaimi, N. Noordin, and M. F. bin Ya'kub, "Assessment of Malaysian E-Passport PKI based on ISO 27000 Series International Standards," J Phys Conf Ser, vol. 1551, no. 1, p. 012003, May 2020, doi: https:/doi.org/10.1088/1742-6596/1551/1/012003.

[6] M. F. Hinarejos, F. Almenarez, P. Arias Cabarcos, J. L. Ferrer-Gomila, and A. M. Lopez, "RiskLaine: A Probabilistic Approach for Assessing Risk in Certificate-Based Security," IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 1975–1988, Aug. 2018, doi: https://doi.org/10.1109/TIFS.2018.2807788.

[7] A. R. Rahmika, M. Akbar, D. L. Jayanto, and J. R. Bu'tu, "Cloud governance frameworks: CIA-based security and compliance," *Journal of Embedded Systems, Security and Intelligent Systems*, pp. 379–389, 2025.

[8] M. Elmsalmi, W. Hachicha, and A. M. Aljuaid, "Modeling sustainable risks mitigation strategies using a morphological analysis-based approach: a real case study," *Sustainability*, vol. 13, no. 21, p. 12210, 2021.

[9] A. Aborujilah, J. Adamu, S. A. Mokhtar, A. Z. Al-Othmani, E. Y. Al-Alwi, and D. A. Y. Al-Hidabi, "CIA-based analysis for e-learning systems threats and countermeasures in Malaysian higher education," in *Proc. 2023 17th Int. Conf. Ubiquitous Inf. Manage. Commun. (IMCOM)*, Jan. 2023, pp. 1–8.

[10] M. Zahid, I. Inayat, M. Daneva, and Z. Mehmood, "A security risk mitigation framework for cyber physical systems," *Journal of Software: Evolution and Process*, vol. 32, no. 2, p. e2219, 2020.

[11] C. Adams and S. Farrell, *Understanding Public Key Infrastructure: Concepts, Standards, and Deployment Considerations*, 2nd ed. Indianapolis, IN, USA: Addison-Wesley, 2021. doi: https://doi.org/10.5555/pki.2021.0001.

[12] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile," *IETF RFC 5280*, 2021. doi: https://doi.org/10.17487/rfc5280.

[13] S. K. Singh and A. Chatterjee, "A survey on digital certificate management and PKI security," *IEEE Access*, vol. 10, pp. 116238–116254, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3215530.

[14] Y. Lin, M. A. Madini, and Y. Alghazo, "Blockchain-enabled trusted certificate authentication: A systematic review," *Computers & Security*, vol. 123, p. 102961, 2023, doi: https://doi.org/10.1016/j.cose.2022.102961.

[15] S. S. Alshammari and N. Almakhdhub, "Enhancing digital certificate validation using distributed ledger technology," *Future Generation Computer Systems*, vol. 147, pp. 322–335, 2023, doi: https://doi.org/10.1016/j.future.2023.04.015.

[16] F. Li and H. Kim, "A CIA-based analysis model for evaluating security robustness of digital credential systems," *Information Sciences*, vol. 619, pp. 274–289, 2023, doi: https://doi.org/10.1016/j.ins.2022.10.032.

[17] J. Bajpai, R. S. Singh, and V. Kumar, "Risk assessment of certificate-based authentication systems using CIA-triad modeling," *Journal of Information Security and Applications*, vol. 72, p. 103409, 2022, doi: https://doi.org/10.1016/j.jisa.2022.103409.

[18] A. M. Lone and M. A. Mir, "Survey of cryptographic schemes for secure digital certificates," *ACM Computing Surveys*, vol. 55, no. 8, pp. 1–39, 2023, doi: https://doi.org/10.1145/3514220.

[19] NIST, "Security and Privacy for Digital Identity," *NIST SP 800-63C*, 2022, doi: https://doi.org/10.6028/NIST.SP.800-63c.

[20] P. Arias-Cabrera and J. Ferrer, "Certificate lifecycle vulnerabilities in PKI ecosystems: An empirical study," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 380–392, 2023, doi: https://doi.org/10.1109/TDSC.2022.3146823.

[21] S. K. Viswanathan and K. N. Jha, "Risk mitigation modelling of international construction projects executed by Indian firms: a structural equation modelling approach," Engineering, Construction and Architectural Management, vol. 27, no. 9, pp. 2687–2713, May 2020, doi: https://doi.org/10.1108/ECAM-05-2019-0265.

[22] P. Arias-Cabrera and J. Ferrer, "Certificate lifecycle vulnerabilities in PKI ecosystems: An empirical study," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 380–392, 2023, doi: https://doi.org/10.1109/TDSC.2022.3146823.

[23] M. Elmsalmi, W. Hachicha, and A. M. Aljuaid, "Modeling Sustainable Risks Mitigation Strategies Using a Morphological Analysis-Based Approach: A Real Case Study," Sustainability, vol. 13, no. 21, p. 12210, Nov. 2021, doi: https://doi.org/10.3390/su132112210.

[24] M. Alowais and S. Alsubaie, "Cyber risk modeling for certificate authorities: An extended CIA approach," *International Journal of Information Management*, vol. 69, p. 102576, 2023, doi: https://doi.org/10.1016/j.ijinfomgt.2022.102576.

[25] X. Zhou and L. Chen, "Next-generation PKI architectures: Challenges and future trends," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 4, pp. 2331–2355, 2022, doi: https://doi.org/10.1109/COMST.2022.3194828.