Jurnal of Business and Audit Information System (JBASE)
Versi Online: http://journal.ubm.ac.id/index.php/jbase
DOI: dx.doi.org/ 10.23957/jbase.v8i2.8870

Vol. 8(No.2): 1 – 10. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

Implementasi Audit Internal WebTrust CA/NS pada Perusahaan Penyedia Tanda Tangan Digital

Implementing Internal Audit for WebTrust CA/NS in Digital Signature Companies

Sarah Rosdiana Tambunan[1)]*, Indah Elisa Sihombing[2)], Tiarani Sibarani[3)]
[1) ,2), 3)]Department of Information System, Institut Teknologi Del

Diajukan 24 Juli 2025 / Disetujui 28 Agustus 2025

Abstrak

Audit internal berperan penting dalam memastikan kesiapan dan kepatuhan *Certificate Authority* (CA) terhadap standar keamanan informasi yang diakui secara internasional, salah satunya adalah *WebTrust for Certification Authorities and Network Security*. Topik ini menjadi semakin relevan seiring meningkatnya kebutuhan akan layanan tanda tangan digital yang andal, aman, serta sesuai dengan regulasi nasional dan global. Penelitian ini bertujuan untuk mengkaji secara mendalam penerapan audit internal berbasis standar WebTrust pada perusahaan penyedia layanan tanda tangan digital di Indonesia. Metode yang digunakan adalah pendekatan deskriptif kualitatif, dengan teknik pengumpulan data melalui studi dokumen dan wawancara mendalam kepada personel yang menjalankan fungsi peran terpercaya. Proses audit internal terdiri dari lima tahapan utama, yaitu: penetapan ruang lingkup audit, pemetaan kontrol yang relevan dengan standar, pengumpulan bukti dari proses dan sistem yang berjalan, evaluasi terhadap kesesuaian implementasi, serta penyusunan laporan akhir beserta rekomendasi perbaikan. Hasil audit menunjukkan bahwa sebagian besar temuan berpusat pada aspek pengendalian lingkungan *(CA Environmental Controls)*, yang mencakup pengelolaan aset, keamanan fisik, serta dokumentasi kebijakan dan prosedur. Temuan ini menunjukkan masih adanya area yang perlu diperkuat guna meningkatkan postur keamanan organisasi. Audit internal ini terbukti efektif dalam mengidentifikasi kelemahan secara dini, memberikan rekomendasi perbaikan yang relevan, dan berperan sebagai langkah strategis dalam mempersiapkan perusahaan menghadapi audit eksternal WebTrust. Dengan demikian, audit internal dapat menjadi instrumen penting dalam menjaga keandalan sistem, meningkatkan kapabilitas tata kelola keamanan, dan mempertahankan kepercayaan terhadap layanan tanda tangan digital.
Kata Kunci: *Certificate Authority*, Audit Internal, Standar WebTrust

Abstract

Internal audit play a crucial role in ensuring the readiness and compliance of Certificate Authorities (CAs) with internationally recognized information security standards, particularly the WebTrust for Certification Authorities and Network Security. This topic has become increasingly relevant due to the growing demand for reliable and regulation compliant digital signature services. This study aims to examine the implementation of internal audit based on the WebTrust standard within a digital signature service provider in Indonesia. The research adopts a qualitative descriptive approach, utilizing document analysis and in depth interviews with personnel performing trusted roles. The internal audit process consists of five main stages: defining the audit scope, mapping relevant controls to the standard, collecting evidence from operational processes and systems, evaluating the implementation's conformity, and compiling the final report along with improvement recommendations. The audit findings reveal that most issues are concentrated in CA Environmental Controls, which includes asset management, physical security, and the documentation of policies and procedures. These findings indicate the need for strengthening controls in these areas to enhance the organization's security posture. The internal audit has proven effective in identifying weaknesses early, providing relevant improvement recommendations, and serving as a strategic step in preparing for the external WebTrust audit. Thus, internal audit can be a critical instrument in improving system reliability, strengthening information security governance, and maintaining trust in digital signature services.
Keywords: *Certificate Authority, Internal Audit, WebTrust Standard*

*Corresponding Author:
E-mail: sarah.tambunan@del.ac.id

Vol. 8(No.2): 1 – 10. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

Introduction

In today's digital era, technology has become deeply embedded in multiple aspects of daily life, including financial and non-financial transactions (Gunawan Sudarsono et al., 2023). One of the primary mechanisms for establishing trust in digital transactions is the use of electronic signatures (Tektona & Laoly, 2023). Electronic signatures play a critical role in ensuring both the security and legal validity of information transmitted online. According to Indonesia's Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE), electronic certificates can be utilized to verify identity and guarantee the integrity of data transmitted across networks. A Certificate Authority (CA) functions as the trusted entity responsible for issuing these certificates, thus holding a pivotal position within the trust infrastructure of relevant application systems (Maulani et al., 2021). As emphasized in Article 13 of the UU ITE, the level of trust placed in the CA is a crucial factor in maintaining overall system security.

As of 2025, there are ten certified Certificate Authorities (CAs) in Indonesia, originating from both government and private sectors, all of which comply with the provisions of Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions. As the number of CAs continues to grow, the government has strengthened its oversight through regulations such as Ministry of Communication and Informatics Regulation Number 11 of 2022 and the adoption of security certification schemes by the National Cyber and Crypto Agency. Nevertheless, the rapid evolution of technology and the increasing sensitivity of the data managed by CAs have introduced new challenges. Cyberattack risks are rising, exacerbated by the limited availability of comprehensive historical data to support a holistic understanding of risks and the increasingly diverse and geographically unbounded nature of threat actors (Cremer et al., 2022; Li & Liu, 2021). These developments highlight the need for consistent and strategic mitigation efforts to maintain public trust and ensure compliance with regulations, thereby building a robust and trustworthy digital government ecosystem (Alfi, 2023; Yani et al., 2025). One of the most critical steps in identifying and addressing security gaps is the implementation of WebTrust-based internal audits. Without standardized internal audits, organizations are at risk of reputational damage, financial losses, and a decline in public trust, all of which could jeopardize operational sustainability. Therefore, the urgency of implementing such internal audits is paramount to ensuring data security, maintaining regulatory compliance, and strengthening existing system controls.

WebTrust for Certification Authorities and Network Security (WebTrust for CA/NS), hereafter referred to as WebTrust, is an internationally recognized framework designed to ensure the reliability and security of CA operations (Sahombu et al., 2025)**.** In the process of preparing for external certification, internal audits serve as an essential first step to ensure compliance (Caroline et al., 2023; Doharma et al., 2021)**.** These audits enable continuous monitoring, early identification of vulnerabilities, and the strengthening of security controls across the services provided (Hanifah et al., 2023). Internal audits based on the WebTrust framework aim not only to ensure compliance with existing regulations but also to identify operational weaknesses that could threaten the security and reliability of CA services. Conducting such audits allows organizations to improve internal controls, reduce the risk of cyberattacks, and demonstrate readiness for external audits, which are critical for maintaining certification status and sustaining user trust in digital services.

Internal audit is an organizational activity aimed at adding value and improving performance through the assessment and enhancement of risk management, control, and governance processes (Kanivia et al., 2024; Tannady et al., 2024). Despite its critical role, research on the implementation of WebTrust-based internal audits in digital signature providers remains limited. The majority of existing studies focus on general compliance and conceptual approaches rather than providing an in-depth analysis of the practical application of WebTrust control structures in real-world internal audit settings. For example, Saputra and Kiswara examined WebTrust principles within the context of accounting information systems for electronic banking services using the Technology Acceptance Model to measure user perceptions, rather than directly applying WebTrust control frameworks (Saputra & Kiswara, 2022). Similarly, Jalinka et al. evaluated the compliance level of electronic certification providers with WebTrust management aspects and focused primarily on assessing the

Vol. 8(No.2): 1 – 10. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

conformity of Certification Practice Statements (CPS) and Certificate Policies (CP) without elaborating on the practical implementation of those controls (Jalinka et al., 2023). This reveals a gap in the literature, highlighting the lack of empirical studies exploring the implementation of WebTrust controls in the operational context of digital signature providers, particularly within the Indonesian regulatory environment. Therefore, this study aims to address this gap by conducting an in-depth analysis of WebTrust control implementation through an internal audit framework, providing practical insights that can enhance compliance, strengthen security controls, and improve organizational readiness for external certification.

Given the challenges faced by Certificate Authorities in meeting WebTrust standards and the increasingly stringent regulatory requirements, it is essential for organizations to implement standardized internal audits. This study seeks to address the existing gap in the literature by presenting a practical approach to conducting WebTrust-based internal audits. The findings of this research are expected to serve as a practical guide and provide a concrete framework for organizations to prepare for certification processes and enhance network security.

Research Method

This chapter will methodically explain the approach and stages used during the research. The methodology is designed to ensure that each stage in the internal audit process can be logically described, from planning to follow up.

2.1 Research Approach and Data Collection Techniques

This study employs a descriptive qualitative approach to gain a detailed and in-depth understanding of the implementation of internal audits based on the WebTrust standard. This approach was chosen because it allows the researcher to explore the various complex and contextual aspects of the audit process, focusing not only on the final outcomes but also on the audit process itself, which is directly relevant to the real-world challenges of managing sensitive data and maintaining system security within Certificate Authorities (CAs). The selection of a qualitative approach is appropriate because WebTrust internal audits involve multiple technical and procedural steps that require a deep understanding of field conditions that cannot be adequately explained using numerical data. The main issue addressed in this study is the necessity to ensure that the systems used by CAs comply with international standards for data security and integrity. Therefore, this approach is considered the most suitable for uncovering the operational context and the implementation of internal controls that align with established procedures and regulations.

In addition to the qualitative approach, this study also employs a direct audit method. The direct audit method was chosen because it provides firsthand insight into how controls are implemented in practice, enabling the researcher to validate the conformity of control execution with the applicable procedures and to identify issues that might not be revealed through secondary data alone. This is particularly important because the challenges faced by organizations are often complex and context-specific, requiring a more thorough approach to uncover the root causes of these issues. Data collection techniques were conducted using two primary methods: document review and structured interviews. Document review included the examination of relevant internal documents, previous audit reports, and working papers used by auditors. Structured interviews were conducted to validate the implementation of controls in the field and to evaluate their compliance with existing procedures. These two techniques complement each other and assist the researcher in identifying gaps or weaknesses in the implementation of existing controls, which may constitute the root causes of compliance issues with the WebTrust framework.

2.2 Subjects and Observation Units

The subject of this research is a digital signature service provider company that implements Public Key Infrastructure (PKI) and functions as a Certification Authority (CA) and Network Security (NS) system manager. The focus of the research is the management of Public Key Infrastructure (PKI) with actual implementation in the CA environment. This area includes key processes such as

Vol. 8(No.2): 1 – 10. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

issuing and managing digital certificates, securing cryptographic keys, access control, activity logging systems and network moniroting, and information security policy documentation. This scope is explicitly defined in the audit program on which the internal audit is based.

2.3 Research Flow

The research flow was carried out through five main stages arranged in sequence: (1) determining the scope and audit plan, (2) mapping WebTrust controls and preparing working papers, (3) collecting audit evidence, (4) evaluating the suitability of controls for implementation, and (5) preparing reports and recommendations for improvement. These five stages are illustrated in Figure 1 as a representation of the internal audit process flow. Each stage has a clearly defined objective to ensure that security issues and compliance gaps related to WebTrust are identified and addressed with appropriate solutions, ultimately supporting the organization's readiness for external audits.

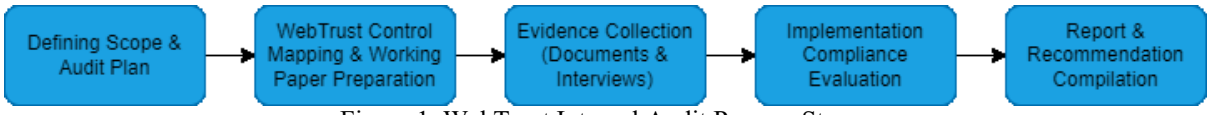

Figure 1. WebTrust Internal Audit Process Stages

2.4 Data Validity

Data validity is ensured through source and method triangulation techniques, which involve comparing reviewed documents and interview results to confirm the authenticity of the data. In addition to triangulation, the validation process also involves direct confirmation with the auditee to minimize interpretation errors and ensure that the information used in the evaluation process aligns with actual conditions. With this approach, the audit process is verified, and its results are accountable.

Result and Discussion

This section presents an in-depth analysis of the implementation of WebTrust-based internal audits at digital signature providers. Unlike descriptive presentations, the main focus is on evaluating the effectiveness of the audit process and the implications of key findings. The implementation of internal audits has proven effective in identifying system weaknesses and compliance gaps at an early stage. The structured audit process, from scope design to recommendation preparation, has proven capable of producing critical findings centered on CA Environmental Controls (Control 3.0) aspects.

The selection of a scope focused on Public Key Infrastructure (PKI) and trusted roles was a strategic move because this area is directly related to the core principles of WebTrust and has implications for service reliability. Thus, the internal audit was not only administrative in nature, but also directed at the most sensitive areas that affect overall system security.

The evidence collection methodology, which combined document studies and structured interviews, demonstrated the effectiveness of data triangulation. The review of policies and SOPs was then validated through operational practices in the field. This approach ensured that the audit findings were objective, accurate, and accountable.

The evaluation results show that the majority of Non-Conformities (NC) were found in control 3.0, such as the absence of an access rights review mechanism, weak password policies, and unauthorized access to the repository. These critical findings indicate significant gaps in operational security governance that could jeopardize the integrity of the CA if not addressed immediately. Meanwhile, the Opportunity for Improvement (OFI) category, such as the need to disseminate malware reporting procedures and improve session timeouts, illustrates the potential for strengthening controls through continuous improvement.

Overall, this internal audit not only detects non-conformities but also serves as a strategic mechanism for the organization to strengthen its security posture. Classifying findings as NC and OFI helps management prioritize corrective actions and allocate resources appropriately. These findings

Vol. 8(No.2): 1 – 10. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

also form the basis for developing relevant and specific improvement recommendations, ensuring that audit results are not merely documentation but also drive tangible change within the organization

3.1 Defining Scope and Audit Plan

Internal audit begins with defining the scope and developing a structured audit plan. The scope of the audit focuses on the management of the Public Key Infrastructure (PKI) within the Certificate Authority (CA), as outlined by the auditor in the Audit Program document, which is an internal document that details the objectives, scope, and resources, audit approach, and timeline. This area was selected because it is a critical component of digital signature services and is directly related to the fulfillment of controls in the WebTrust standard. An illustration of the Audit Program document is presented in Table 1.

Table 1: Illustration of Audit Program Document

Audit Name	Objectives	Scope	Resources	Audit methodology	Time
			Audit A		
WebTrust Audit	To assess the adequacy and effectiveness of controls used by Certification Authorities (CA).	Management of Public Key Infrastructure (PKI) on Certificate Authority (CA).	1. Lead Auditor 2. Auditor 3.Technical Expert (additional) 4.Technical Audit Intern	1. Document Review 2. Interview	(8 Weeks)
			Audit B		

The audit scope does not cover the entire organizational unit but is limited to those directly involved in the operations and control of the CA. These roles are classified as trusted roles, referring to personel who are authorized to perform sensitive PKI functions. These individuals hold access rights and responsibilities concerning the security and integrity of the CA infrastructure, thus not all divisions within the company serve as auditees in this audit process.

The Audit Plan includes a structured interview schedule with the auditees, tailored to the functions of each trusted roles to ensure that the audit captures the implementation of controls relevant to their respective responsibilities. An illustration of the Audit Plan document is presented in Table 2.

Table 2: Illustration of Audit Plan Document

Auditee	WebTrust Principles & Criteria	Date	Time	Auditor
Dept. A	1, 2	March 10, 2025	10:00 AM - 12:00 PM	• Lead Auditor
Dept. B	3, 1	March 11, 2025	1:00 PM - 3:00 PM	• Auditor 1
Dept. C	3, 4, 5, 6	March 12, 2025	10:00 AM - 12:00 PM	• Audtor 2
Dept. D	3, 6, 8	March 13, 2025	2:00 PM - 6:00 PM	

To ensure the auditees are willing, the auditor will send an official email to each auditee to confirm their availability to attend the interview sessions. The entire audit process lasts for approximately eight weeks, and this duration is designed considering the complexity of the system and the number of auditees, making it adequate to complete all stages of the audit.

3.2 WebTrust Control Mapping and Working Paper Preparation

After the audit scope and plan are established, the next step is to map the relevant WebTrust controls. This process involves reviewing policy documents, SOPs, system logs, previous audit reports, and other internal documentation to match each control with supporting evidence. The auditor also prepares supporting documents such as a document request list and working papers as tools for analysis and documentation.

Vol. 8(No.2): 1 – 10. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

The working paper is structured in a tabular format and divided into two sections: auditee and auditor. The auditee section includes the control number, WebTrust control description, implementation owner, references to internal documents, and types of supporting evidence such as logs or meeting minutes. Meanwhile, the auditor section includes evaluations based on the CP/CPS and internal policies and procedures, audit findings, auditee responses, and the final assessment results (conformity, non-conformity, or opportunity of improvement).

The preliminary filling of the working paper is carried out by the auditee, then during the interview session the auditor will confirm the responses that have been provided. The entire process is documented in the working paper that has been prepared in advance. Based on the data contained in the working paper, the auditor will have additional documentation to identify and determine findings related to the audited division. This control mapping and working paper development serve as a critical foundation for internal audit to ensure compliance with standards, evaluate control effectiveness, and support preparation for external audit. An example of WebTrust control mapping and working paper is presented in Table 3.

Table 3: Example of WebTrust Control Mapping and Working Paper

No	Control	PIC	Type of Document	Type of Evidence	Observation based CP/CPS	Auditor Evaluation	Result
1	3.5.1 CA operating procedures are documented and maintained for each functional area.	Dept. A	Internal policy document related to CA operations.	Internal audit evidence (logs, forms, system records).	Relevant policies are available.	The policy does not include a mechanism for annual review.	*To be completed by the auditor during the control compliance evaluation stage.*
2	3.10.1 The CA generates automatic (electronic) and manual audit logs in accordance with the requirements of the CP and/or CPS	Dept. B	Internal procedure related to logging processes.	Samples of electronic audit logs and manual documentation.	Logging is outlined in the general policy.	Manual logs are not recorded consistently	*To be completed by the auditor during the control compliance evaluation stage.*
3	5.1.3 Subscriber key generation performed by the CA (or RA) uses a prime number generator as specified in an ANSI X9 or ISO standard	Dept. C	Key generation security procedures based on industry standards.	Records of implementation and system logs for the key generation process.	The procedure documentation is available but not complete.	Documentation lacks detail and needs improvement.	*To be completed by the auditor during the control compliance evaluation stage.*
4	6.2.6 The CA or the RA	Dept. D	Procedure for	System logs for	Validation mechanism	The digital signature	*To be complete*

	validate the signature on the Certificate Renewal Request	validating certificate renewal requests.	certificate request verification .	is described in the general policy.	verification process has been implemented according to procedure.	*d by the auditor during the control complian ce evaluatio n stage.*

3.3 Evidence Collection

Evidence is collected to verify the implementation of the previously mapped WebTrust controls, ensuring that the controls outlined in the working paper are supported by verified data and actual operational practices. The audit begins by reviewing the previous WebTrust audit working paper, as it can serve as an initial reference for controls that have already been implemented. If there are updates to document versions or specific controls, the working paper is revised accordingly to reflect the most recent implementation.

Document review is a key component in evidence collection. The documents reviewed include, but are not limited to, PKI operational policies and procedures, Certificate Policy (CP), Certification Practice Statement (CPS), key management procedures, incident response plans, access control documentation, and network security guidelines. The objective of this review is to ensure that the mapped controls are not only defined but also properly documented and aligned with the WebTrust standards.

Next, structured interviews are conducted with auditees as specified in the previously developed audit plan. These interviews aim to verify whether actual practices align with established policies, with questions tailored to each auditee's role, focusing on core process implementation, understanding of procedures, and potential gaps between policy and practice. The combination of document review and interviews ensures that the audit evidence gathered is sufficient to support the conformity evaluation process.

3.4 Implementation Compliance Evaluation

After all evidence has been collected, an evaluation is conducted to assess the conformity of control implementation with the WebTrust standards. As part of maintaining data validity, the auditor performs direct confirmation with the auditee to ensure that each recorded finding is accurately understood and reflects the actual operational context. This verification process aims to minimize misinterpretation and ensure that the information used in the evaluation truly represents current conditions. The assessment is categorized into three main classifications, namely:

- Conformity (C): The implementation is in accordance with the established control.
- Non-conformity (NC): There is a deviation or failure to meet one or more audit criteria.
- Opportunity for Improvement (OFI): No violation is found, but there is potential for enhancing the effectiveness of the control.

This classification not only serves as an indicator of compliance status, but also helps in prioritizing follow up actions and identifying areas that require special attention. The NC category requires immediate corrective action as it has the potential to become a weak point in the system, while the OFI category encourages continuous improvement as part of the security reinforcement cycle. The results of this evaluation are then recorded in the audit findings table as part of the audit report documentation. An example of an internal audit finding based on the evaluation results is presented in Table 4.

Table 4: Example of Internal Audit Findings on WebTrust Control Implementation

No	Control	Finding	Category
1	2.0: CA Business Practices Management	There is no explanation or documentation regarding the annual review of the CPS.	NC
2	3.0: CA Environmental	There is no defined retention period for	NC

Vol. 8(No.2): 1 – 10. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

	Controls	archived audit logs in the risk register.	
3	3.0: CA Environmental Controls	Access rights review on the application has not been conducted, and there is no guideline for performing such reviews.	NC
4	3.0: CA Environmental Controls	The use of 8 character passwords does not comply with current security standards.	NC
5	3.0: CA Environmental Controls	Improvement planning is needed regarding session timeout attempts on devices used by verifiers.	OFI
6	3.0: CA Environmental Controls	FIM has not yet monitored the archive directory; it is recommended to include it in the monitoring scope.	NC
7	3.0: CA Environmental Controls	There is no provision governing the periodic evaluation of network devices.	NC
8	3.0: CA Environmental Controls	Unauthorized users were found to have OS level access to the repository.	NC
9	3.0: CA Environmental Controls	Endpoint device rollout for branch offices has not yet been carried out.	NC
10	3.0: CA Environmental Controls	Awareness on malware reporting procedures and the availability of accessible guidelines for all employees needs to be improved.	OFI
11	3.0: CA Environmental Controls	The key asset logbook document has not been included in the asset inventory list.	NC
12	3.0: CA Environmental Controls	The security procedure for vault access needs to be updated to reflect current conditions.	NC
13	6.0: Certificate Lifecycle Management	There is no defined method for retrieving archived records.	NC

The dominant findings in control 3.0 indicate that both physical and logical environmental aspects are major weaknesses that require priority attention. For example, the absence of access rights reviews on applications has the potential to open up opportunities for unauthorized access that could threaten the integrity of certificate data. Similarly, the policy of using passwords with a minimum of 8 characters that does not comply with international standards poses a risk of brute force exploitation.

Findings related to OS access by unauthorized users indicate a failure in basic access control, which should be the foundation of the CA security system. If this is not corrected immediately, the risk of compromise to the cryptographic key repository could increase significantly.

Meanwhile, findings in the OFI category, such as the lack of socialization of malware reporting procedures, indicate that although basic procedures are in place, user awareness still needs to be improved. This highlights the importance of a human-centric security approach to complement technical controls. Thus, the results of this audit illustrate that formal compliance is not enough, and organizations need to build a more mature security culture.

3.5 Report and Recommendation Compilation

After all findings have been evaluated, the next step is to prepare an internal audit report. This report is not only a documentation of the audit process, but also a basis for management to follow up on the findings. The report contains a summary of the audit objectives and scope, a list of auditees, the audit methods used, and a list of findings detailed based on WebTrust controls. For findings categorized as non-conformities and OFIs, the report lists the controls that were violated and provides a detailed description of the findings.

In addition to the report, the auditor also issues a Request for Corrective Action (RCA) document for each non-conformity and OFI finding, which must be completed by the relevant auditee. The document includes a description of the finding, the WebTrust controls that were violated, proposed corrective actions, and the deadline for completing the corrective actions. The document

Vol. 8(No.2): 1 – 10. Th.2025
p-ISSN: 2615-6431
e-ISSN: 2620-7907

will be signed by the supervisor of the auditee to verify whether the corrective actions have been implemented properly and proven effective in resolving the findings. All RCA documents will be stored and reviewed periodically as they are an important reference for continuous monitoring and prevention of recurring findings.

Conclusion

This research shows that the implementation of WebTrust based internal audit contributes significantly to strengthening the governance and operational security of CA operators. A structured approach, starting from planning, mapping controls, to evaluating implementation, enables early identification of non-compliance and opportunities for improvement. The audit findings, which are mostly in control section 3.0, namely CA Environmental Controls, emphasize the importance of strengthening control over the physical and logical environment of the CA infrastructure. One of the advantages of implementing this audit is its ability to produce documentation and evidence that is systematically documented and accountable to both auditors and auditees. This supports the organization's readiness to face external audit, particularly in obtaining WebTrust certification. Overall, this internal audit not only enhances the company's operational readiness but also strengthens stakeholders' confidence in the company's commitment to maintaining information security and compliance with applicable standards.

In terms of academics, this research contributes by presenting an empirical case study on the implementation of WebTrust-based internal audits, which has rarely been discussed in the literature. By emphasizing critical analysis of non-conformity findings and opportunities for improvement, this research enriches the understanding that internal audits not only serve as a compliance mechanism but also as a strategic instrument to encourage continuous improvement in information security governance. This opens up space for further research that can develop a quantitative evaluation model or a more measurable compliance benchmarking framework in the future.

From a practical standpoint, this research provides tangible benefits for digital signature service providers. Audit results and improvement recommendations can be used as adaptive operational guidelines to strengthen security controls, particularly in the area of CA Environmental Controls, which have proven to be the most vulnerable. Furthermore, the findings of this study can support management in preparing the documentation, evidence of compliance, and follow-up mechanisms necessary to face external audits, thereby not only improving internal systems but also increasing stakeholder confidence in the services provided.

Recommendation

This research is limited to one object of study and uses a descriptive qualitative approach. Therefore, future research is recommended to expand the scope of the object by involving more than one Certificate Authority (CA), so as to obtain a more diverse and representative comparison of implementation. In addition, a quantitative approach is also recommended to measure the level of compliance and risk through a score or index-based scoring system. For example, further research could use the risk rating model from NIST SP 800-300 or ISO/IEC 27005 to classify the level of non-conformities found during audit. Such assessments can also be integrated with frameworks such as COBIT 5 or ISO/IEC 27001 to produce a more structured evaluation and enable quantitative comparisons between organizations. Thus, audit findings can be analyzed based on their potential impact on the operational security of the system.

Bibliography

Alfi, M. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. *Jurnal Kajian Stratejik Ketahanan Nasional*, *6*(2). Available at: https://doi.org/10.7454/jkskn.v6i2.10082

Caroline, E., Kuntadi, C., & Pramukty, R. (2023). Pengaruh Pengalaman Auditor, Dukungan

Manajemen Dan Efektivitas Pengendalian Internal Terhadap Efektivitas Fungsi Audit Internal. *Jurnal Economina*, *2*(6), 1487–1497. Available at: https://doi.org/10.55681/economina.v2i6.641

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Papers on Risk and Insurance: Issues and Practice*, *47*(3), 698–736. Available at: https://doi.org/10.1057/s41288-022-00266-6

Saputra, D. D., & Kiswara, E. (2022). Penerapan Prinsip-Prinsip WebTrust Audit dalam Sistem Informasi Akuntansi dengan Elektronik Banking berdasarkan Technology Acceptance Model (Studi kasus pada Bank Syariah Indonesia Branch Office Lingkup Kota Semarang). *Diponegoro Journal of Accounting*, *11*(4), 1–9. Available at: http://ejournal-s1.undip.ac.id/index.php/accounting

Doharma, R., Prawoto, A. A., & Andry, J. F. (2021). Audit Sistem Informasi Menggunakan Framework Cobit 5 (Studi Kasus: Pt Media Cetak). *Journal of Business and Audit Information Systems (JBASE)*, *4*(1), 22–28. Available at: https://doi.org/10.30813/jbase.v4i1.2730

Gunawan Sudarsono, B., Ananda, V. R., & Kardi, M. R. (2023). Audit Aplikasi Keuangan Menggunakan Framework Cobit 5.0 Domain Dss Studi Kasus Perusahaan Peralatan Tambang Audit of Financial Applications Using the Cobit 5.0 Domain Framework Case Study of Mining Equipment Companies. *Jurnal of Business and Audit Information System (JBASE)*, *6*(1), 23–36. Available at: http://journal.ubm.ac.id/index.php/jbase

Hanifah, A. M., Kuntadi, C., & Pramukty, R. (2023). Literature Review: Pengaruh Sistem Pengendalian Internal, Peran Audit Internal, Komitmen Manajemen Terhadap Good Corporate Governance. *Jurnal Economina*, *2*(6), 1318–1330. Available at: https://doi.org/10.55681/economina.v2i6.605

Jalinka, M., Winarno, W. W., & Susanti, P. (2023). Compliance Analysis of Perum Peruri as an Electronic Certification Provider in Implementing Business Practices Management Webtrust Certification Authorities. *Journal of Computer Networks, Architecture and High Performance Computing*, *5*(2), 434–443. Available at: https://doi.org/10.47709/cnahpc.v5i2.2477

Kanivia, A., Puspitarini, D. A., Dewi, D. K., Akbari, S., & Chandra, A. K. (2024). Implementasi Teknologi Informasi Terhadap Kualitas Audit Internal. *Jurnal Digit*, *14*(2), 170. Available at: https://doi.org/10.51920/jd.v14i2.409

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. Available at: https://doi.org/10.1016/j.egyr.2021.08.126

Maulani, G., Gunawan, G., Leli, L., Ayu Nabila, E., & Yestina Sari, W. (2021). Digital Certificate Authority with Blockchain Cybersecurity in Education. *International Journal of Cyber and IT Service Management*, *1*(1), 136–150. Available at: https://doi.org/10.34306/ijcitsm.v1i1.40

Sahombu, J. M., Wafa, Z., Airawaty, D., & As, H. (2025). Information System Audit : A Case Study of Bank Syariah Indonesia. *Journal of Management Studies, 5*(04), 619–627. Available at: https://doi.org/10.58471/jms.v5i04

Tannady, H., Wiedjaya, H., Brainard, A., Arron, R., Fernandes Andry, J., & Francka Sakti Lee, dan. (2024). Tata Kelola IT pada Website Bisnis Kuliner Foodpedia Menggunakan COBIT 5 Domain EDM & APO. *Jurnal of Business and Audit Information System (JBASE)*, *7*(1), 13–25. Available at: http://journal.ubm.ac.id/index.php/jbase

Tektona, R. I., & Laoly, S. R. (2023). Kepastian Hukum Tanda Tangan Digital Pada Platform Privyid Di Indonesia. *Acta Diurnal Jurnal Ilmu Hukum Kenotariatan Dan Ke-PPAT-An*, *6*(2), 245–253. Available at: https://doi.org/10.23920/acta.v6i2.1141

Yani, A., Ruseno, N., Santoso, G., Informasi, S. T., Teknologi, U., & Jakarta, M. (2025). Mitigasi Serangan Siber, Data Science, dan Database dalam Infrastruktur Jaringan Pemerintahan Digital. *Journal of Information Systems and Technology, 1*(01), 54–62. Available at: https://doi.org/10.9000/jupasti.v1i1.1