International Journal of Safety and Security Engineering
Vol. 15, No. 2, February, 2025, pp. 287-296
Journal homepage: http://iieta.org/journals/ijsse

DRSA: A New Framework for Reliability Audit of Electronic Transaction Document Security in Electronic-Based Government Information Systems in Indonesia

Irfani Ahmad[1,2*], Purwanto Purwanto[1], Agus Widodo[3]

[1] Doctoral Program in Information Systems, Diponegoro University, Semarang 50241, Indonesia
[2] Center for Artificial Intelligence and Cyber Security Research, National Research and Innovation Agency, Jakarta 10340, Indonesia
[3] Center for Process and Manufacturing Technology Research, National Research and Innovation Agency, Jakarta 10340, Indonesia

Corresponding Author Email: irfaniahmad3147@students.undip.ac.id

https://doi.org/10.18280/ijsse.150209

Received: 23 November 2024
Revised: 28 January 2025
Accepted: 13 February 2025
Available online: 28 February 2025

Keywords:
reliability audit, e-government, data security, framework, Trustmark, ISO/IEC 27001

ABSTRACT

An electronic-based government system (EBGS) facilitates access to public services and accelerates both administration and decision-making processes. However, with the increasing complexity of information systems, ensuring system reliability becomes a critical aspect to maintain services that are consistent, secure, and error-free, thereby safeguarding both the community and the government. This study aims to develop a comprehensive and practical information system reliability audit model for EBS in Indonesia. The audit model proposed in this study involves various components such as authentication, access control, audit trails, and disaster recovery, all of which play essential roles in ensuring the reliability and security of government information systems. The result of this study is a framework for ensuring the reliability of personal data security and electronic transactions within EBS. By adopting this model, it is anticipated that government agencies can mitigate potential risks in their systems and implement more structured and measurable improvement steps, thereby increasing stakeholders' trust in their information systems.

1. INTRODUCTION

In the era of globalization and rapid advancement of information technology, the electronic-based government system (EBGS) has become a crucial component in enhancing the efficiency, transparency, and accountability of government administration in Indonesia. Implementing EBGS not only facilitates access to public services but also accelerates administration and decision-making processes [1]. However, as information systems become increasingly complex, ensuring system reliability is crucial to provide consistent, secure, and error-free services that protect both the public and the government.

Information system reliability in EBGS covers various dimensions, including availability, integrity, security, and performance [2]. Reliability audits are necessary to assess and ensure that these systems meet established standards and operate optimally to support government functions. However, developing an information system reliability audit model in Indonesia faces various challenges, such as limited competent human resources, lack of uniform standards, and the dynamic nature of technology [3].

An e-government audit's role is to assess the conformity between ICT and established standards through information security audits and performance audits [4]. The growing digital transformation will inevitably affect the role of information technology (IT) audits [5].

Data and information are vital assets for any organization, and it is essential to ensure their quality so that they can be effectively managed within information systems that also guarantee quality [6]. A data quality audit process, including data profiling, data cleansing, and data validation, is important to ensure the data used are accurate, complete, and timely, thereby avoiding errors that could affect decision-making [7, 8].

Information system audit criteria may vary depending on the purpose and scope of the audit, but generally include functionality, system reliability, security, availability, integrity, efficiency, control, and regulatory compliance.

The main problems identified in this study include several critical aspects. First, significant threats to electronic data security, including cyber-attacks and information leaks, can compromise the integrity of the security system. In addition, the lack of clear standards and guidelines for system reliability audits causes uncertainty in assessing such reliability. This contributes to low public trust in government e-services, as people often hesitate to use these services due to concerns about security and transparency. In this context, the implementation of Trustmark becomes highly relevant.

Trustmark, a symbol of trust, indicates that a system or service meets specific security, quality, and reliability standards.

Trustmark certification was developed in the late 1990s to build consumer trust through websites. The entity that provides the Trustmark guarantee is an independent, trusted third party that offers electronic system reliability audit services to online sellers or electronic system organizers managing electronic transactions and their customers' data [9]. Challenges also arise in implementing Trustmark certification, including determining the appropriate criteria and certification processes. Finally, the low level of public understanding and awareness of the importance of data security and electronic transactions can affect the adoption of digital services. By identifying these problems, it is hoped that solutions can be provided to improve reliability and trust in the EBGS security system.

This research aims to develop a reliability audit model for document security systems and electronic transactions through Trustmark certification in EBGS in Indonesia, and identify associated opportunities and challenges. This model is expected to increase the trust of EBGS users by ensuring that electronic transactions are carried out safely and optimally. With Trustmark certification, users can be more confident that the implemented security system meets established criteria, thereby increasing public trust in government services and encouraging wider adoption of digital technology.

2. RELATED WORK

This study references several prior literature studies, particularly those related to the development of an audit model for the reliability of electronic document and transaction security systems in Indonesia's Electronic Based Government System (EBGS). The scope of the literature review includes data security and electronic transactions, Trustmark implementation, audit models and security standards, and the implementation of electronic-based government systems in Indonesia.

2.1 Data security and electronic transactions

Data security and electronic transactions are significant concerns in today's digital age. The theories underlying this field include several vital principles. First, the confidentiality model emphasizes the importance of keeping information inaccessible to unauthorized parties. Integrity ensures that data remain accurate and unaltered without authorization, while availability ensures that information is always accessible when needed [10]. Research conducted by Kautenburger [11] identifies potential risks and challenges in maintaining information security during transactions. Key findings highlight security challenges in electronic transactions and the importance of proactive measures to protect user data.

Personal data protection is another critical issue as governments increasingly collect and process large amounts of personal information. Research conducted by Sarjito [12] explores and evaluates the challenges faced by governments regarding personal data protection. The study's findings underscore that continuous evaluation and improvement of data protection frameworks are essential for maintaining effectiveness in addressing evolving security challenges.

Effective security control requires management to first examine the organization's security level. Existing criteria for evaluating the security level are often limited to external security risks and have inappropriate cut-off points for addressing the security risks that can merge and increase within an organization. In their paper, Kim et al. developed a security evaluation model that focuses on the risk of information leakage from within the organization [13]. The findings of this study include 26 detailed evaluation items that consider security requirements to prevent technical information leakage.

2.2 Trustmark implementation

Implementing Trustmark in information system security is an important step toward increasing user trust in digital services. Trustmark also enhances transparency by providing information regarding the security measures taken, privacy policies, and data handling procedures [14].

Öksüz et al. [15] discussed how trust can be transmitted through technology and how the trust relationship between users and technology providers can be understood. Their critical finding is that trust is a crucial factor in managing users' risk perceptions when using digital technology. Users must feel confident that technology and service providers can be trusted to protect their data and privacy.

Thompson et al. [16] studied how the use of trust marks affects consumer trust and consumer risk perception, and consequently, their purchase intentions. The study found that trust marks can increase consumer trust and purchase intentions while reducing the risk of online transactions. Recent advances in sensor technology and communication device have significantly improved information systems (IS). However, the security of these devices and the trustworthiness of the information they produce cannot be guaranteed. These objects are vulnerable to fraud or control by malicious third parties, presenting new challenges regarding the level of trust one can have in the data, sensors, and information systems themselves. Costé et al. [17] proposed considering information system security assurance through trust assessment, providing new insights into the relationship between information system security and user trust.

2.3 Audit models and security standards

Audit models and security standards are essential for managing risk and ensuring the integrity of information systems, especially data security [18]. The audit model evaluates and assesses the effectiveness of security controls implemented in an organization [19]. Security standards ensure that organizations implement best practices in protecting their data and systems. These standards provide explicit references for preventing threats and vulnerabilities and ensuring compliance with applicable regulations [20].

Several commonly used information system audit models, include COBIT (Control Objectives for Information and Related Technologies), which was developed by ISACA to help organizations manage and control information and technology by providing comprehensive guidance on risk management and compliance. In addition, ISO/IEC 27001 is an international standard that specifies requirements for an information security management system (ISMS); audits based on this standard assess the implementation of policies and controls to protect sensitive information. Another relevant model is the NIST (National Institute of Standards and Technology) SP 800 series, which provides guidelines for risk management and information security with a focus on proper risk assessment. ITIL (Information Technology Infrastructure

Library) also plays a role in security audits, though it focuses more on IT service management, helping organizations manage standardized IT services. Furthermore, SABSA (Sherwood Applied Business Security Architecture) emphasizes the importance of integrating security into the business architecture, while the Risk IT framework, also developed by ISACA, combines risk management with IT management. Each model has a different approach and focus, but overall, they aim to ensure that information systems remain secure, efficient, and compliant with applicable regulations. Selecting the suitable audit model depends on the specific needs of the organization, the risks it faces, and its business objectives.

Regulating IT utilization in both central and regional governments (EBGS) brings numerous benefits or value to the organization but also presents various problems and obstacles. In his research, Novianto [21] developed a Control Objective for Information and Related Technology (COBIT) framework model to determine the level of maturity in the information technology governance process.

Effective information technology (IT) governance has a significant impact on overall performance and outcomes. The COBIT framework, currently known as COBIT 2019, is widely adopted by IT auditors to assess IT governance in organizations. However, a comprehensive understanding of IT governance also requires assessing organizational culture as part of the audit approach. Wijanarko et al. [22] analyzed the application of the COBIT 2019 framework to improve IT performance. Their study found that applying the COBIT 2019 framework, especially in the DSS (Deliver, Support, and Service) domain, can identify several deficiencies in IT governance performance. The researchers recommend developing an IT governance strategy tailored for each service provider to meet user requirements and comply with the maturity level set by COBIT 2019.

ISO/IEC 27001 is an international standard that specifies requirements for an information security management system (ISMS) [23]. This standard is designed to help organizations manage and protect their sensitive information in a structured and systematic way. ISO/IEC 27001 covers a wide range of aspects, from identifying, assessing, and managing information security risks, to developing the necessary policies and procedures to protect data. However, despite ISO 27001 providing a strong framework for managing information security risks, its implementation is not always smooth.

Kitsios et al. [24] found that many companies with ISO 27001 certification do not periodically document their operational procedures. This oversight results in numerous information security risks that remain unrecognized and unaddressed.

Cybersecurity threats continue to evolve, necessitating a strong and mature cybersecurity posture for organizations. Irawan et al. [25] proposed a cybersecurity maturity assessment framework design that utilizes two established standards: the Cybersecurity Framework (CSF) v1.1 from the National Institute of Standards and Technology (NIST) and Controls v8 from the Center for Internet Security (CIS). Based on the results of mapping NIST CSF to CIS Controls v8, 44 NIST CSF and 108 subcategories of NIST CSF are mapped to 124 sub controls of CIS Controls v8. This integration is categorized into each NIST CSF function: identify, protect, detect, respond, and recover. This study recommends further research to identify additional frameworks to fill in unmapped NIST subcategories.

Tanjung et al. [26] conducted similar research, designing information security in electronic government systems using NIST CSF 2.0, ISO/IEC 27001:2022, and CIS Control. This study found that applying the three frameworks, NIST CSF 2.0, ISO/IEC 27001:2022, and CIS Controls v8, resulted in 22 elements that can be combined to improve information system security for government agencies.

Information protection and cybersecurity are challenging tasks for all organizations. Cyber attacks can damage reputation, brand, stakeholder satisfaction, business operations, and result in financial losses. Jayanthi [27] proposed a systematic approach to information security strategic planning using the Defense in Depth (DID) mechanism. The findings in his study highlight the importance of reengineering information security and integrating it into an organization's data governance strategy to mitigate cybercrime threats. Organizations must invest adequate time in developing a mature and forward-looking information security strategic plan that addresses both internal and emerging external threats.

Organizations often face various cyber attacks daily, necessitating regular audits. However, there is currently no integrated tool to perform the typically expensive and time-consuming task of cyber security audits. Al-Matari et al. [28] developed a cybersecurity framework to conduct cybersecurity audit processes within organizations. The proposed framework clarifies security issues through output reports that identify cybersecurity gaps. In addition, this framework helps practitioners in developing integrated tools to support cybersecurity auditors in securing organizations and finding mechanisms to carry out cybersecurity audit tasks effectively.

2.4 Implementation of electronic-based government systems in Indonesia

The rapid development of Electronic Government Systems (ESGs) has significantly improved the efficiency and accessibility of public services. However, the increasing reliance on these systems has also raised concerns about their security and the potential impact of security incidents on government operations and citizen trust.

Prastowo and Sudiana [29] proposed a framework for handling security incidents using the ISO/IEC 27035:2023 standard on information security incident management at the Ombudsman of the Republic of Indonesia. The findings indicated a probability score of 3, an impact score of 5, and a risk level of 22 (Very High). A root cause analysis revealed that the root cause of the risk was the absence of an incident response plan.

Another challenge to implementing the EBGS in Indonesia is the issue of interoperability and the lack of human resources trained in information technology. A study conducted by Akbar et al. [30] identified six dominant themes that need full attention: interoperability, governance, services, technology, information systems, and frameworks.

3. METHODOLOGY

This study focuses on developing a framework model to assess and ensure the reliability of securing electronic transaction documents in EBGS in Indonesia with stages as shown in Figure 1.

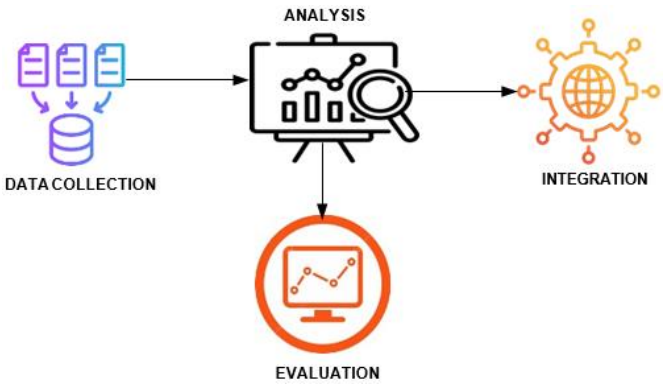

Figure 1. Research stages

Based on Figure 1, the stages carried out in this research are as follows:

1. Standard Document Data Collection and Control Framework related to Personal Data Security and Information Security Management:

-Identification of relevant international and national standards, such as:

-ISO/IEC 27001 (Information Security Management Systems).

-NIST Cybersecurity Framework.

-Information Security Technical Guidelines from BSSN.

-Integration of the standards with relevant frameworks to suit the security needs within the EBGS scope in Indonesia.

2. Analysis of Regulations and Guidelines Related to Personal Data Security and Information Security Management

-Identification of relevant regulations and guidelines, such as Regulation of the Minister of Communication and Informatics No. 16 of 2022, the PDP Law, and regulations related to personal data security and information security management in Indonesia.

-Comparison of applicable regulations and audit tools established by the National Cyber and Crypto Agency (BSSN) and the National Research and Innovation Agency (BRIN).

3. Preparation of Integrated Control and Audit Framework (DRSA)

-Preparation of document security reliability audits (DRSA), which serve as a control integration model to ensure:

-Reliability of electronic systems following SPBE regulations; and

-Personal data security according to information security standards.

-Drafting through an iterative approach involving:

-Determination of the main control components based on the analysis results in the previous step;

-Modeling of the audit framework using top-down and bottom-up approaches to accommodate the complexity of the EBGS environment; and - validation test of the framework through simulation or case studies on EBGS implementation.

4. DRSA Model Validation and Evaluation Test

-Pilot testing of the DRSA framework in a specific EBGS environment to ensure its reliability and suitability to practical needs.

-Evaluation through analysis of audit results, stakeholder interviews, and user feedback.

-Utilization of evaluation results to refine the DRSA framework.

4. RESULTS AND DISCUSSION

Figure 2 illustrates the proposed framework model for auditing the reliability of securing electronic transaction documents. As shown in Figure 1, the audit process for evaluating the reliability of electronic system documentation within an EBGS is based on three basic principles of data security and electronic transactions: confidentiality, integrity, and availability. These principles include several main components to ensure that the document is safe, original, verified, and accessible as needed. Ensuring the reliability of documentation during electronic transactions indicates that the electronic system used for such transactions is trustworthy and well-managed in terms of security.

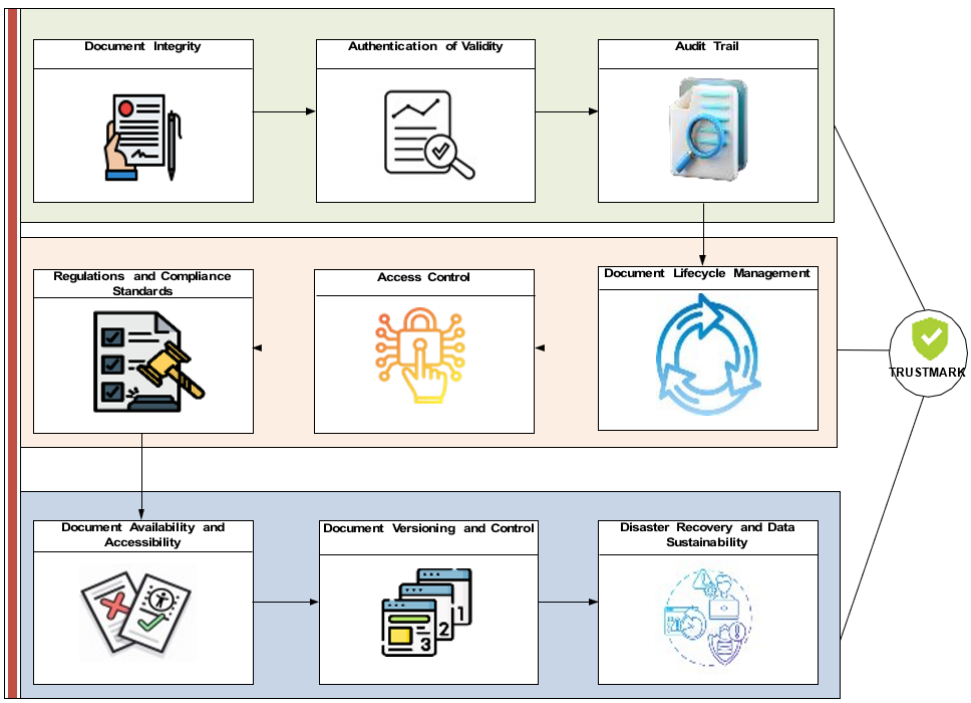

Figure 2. Proposed framework for document security reliability audits (DRSA)

Table 1 shows a description of each component of the DRSA framework. These components include: Integrity (IN), Authentication of Validity (AV), Audit Trail (AT), Document Lifecycle Management (LC), Access Control (AC), Compliance (RS), Document Availability and Accessibility (DA), Document Versioning and Control (DV), Disaster Recovery and Data Sustainability (DR).

Table 1. DRSA framework component description

ID	Component	Description
IN	Document Integrity	Ensuring that documents are not subject to unauthorized changes and remain intact from creation to storage or access.
AV	Authentication of Validity	Assessing the use of digital signatures or other authentication methods to verify that documents are creates or approved by authorized parties.
AT	Audit Trail	Reviewing audit logs to maintain a complete record of all activity, identifying who accessed or modified documents and when it occurred.
LC	Document Lifecycle Management	Verifying document lifecycle policies to ensure that documents are retained and deleted according to established rules, and check backup and data retention procedures.
AC	Access Control	Verifying access and permission settings, evaluating encryption methods, and ensuring only authorized users can access or modify documents.
RS	Regulations and Compliance Standards	Ensuring document management complies with applicable standards and regulations (such as ISO 27001 or related government regulations), and conducting regular compliance evaluations.
DA	Document Availability and Accessibility	Testing backup and recovery systems to ensure documents are accessible during emergencies, and document formats are easily accessible to all authorized stakeholders.
DV	Document Versioning and Control	Ensuring the document management system supports version control, reviewing change history, and verifying that only relevant and valid versions are accessed.
DR	Disaster Recovery and Data Sustainability	Assessing existing disaster recovery plans, performing backup testing, and ensuring all critical documents can be recovered as needed.

Table 2. Audit working paper for document integrity check

No.	Component ID	Examination Aspect	Status	Information
1	DI-1	Document Format and Structure	[X/√]	[Information]
2	DI-2	Recording and Storage System	[X/√]	[Information]
3	DI-3	Document Encryption and Protection	[X/√]	[Information]
4	DI-4	Document Activity Log	[√/X]	[Information]
5	DI-5	Validity of Document Content	[√/X]	[Information]
6	DI-6	Validity of Documents	[√/X]	[Information]

4.1 Document integrity (DI)

Document integrity is a critical component in the audit of the reliability of electronic-based government information systems, ensuring that documents do not undergo unauthorized changes during their life cycle, from creation to storage, distribution, and deletion [31]. In the context of government, document integrity refers to documents remaining original, intact, and unaltered since their initial creation. This is essential because damaged or altered documents can lead to errors in decision-making, legal violations, or loss of public trust.

To maintain document integrity, various supporting technologies are employed, including encryption, checksums (a method of checking a file's integrity through a hash or code generated from its contents), and digital signatures. Digital signatures ensure that documents cannot be changed after they are signed because any alteration will modify the hash or document identification code, making it immediately detectable. During the audit process, auditors check whether important documents have used digital signatures or other security marks to ensure integrity. This involves technically checking the document hash and comparing it with the initial hash generated when it was first created or authorized. Any discrepancies indicate the possibility of unauthorized changes, necessitating further investigation to determine the cause. In addition, document integrity in government systems is maintained by recording every instance a document is opened, changed, or accessed, including by whom and when. These measures enable government systems to maintain the reliability of information and ensure that documents used in decision-making remain accurate and unaltered by unauthorized changes.

Table 2 presents the audit working paper draft for checking document integrity.

4.2 Authentication of validity (AV)

The authentication validation audit process for electronic-based government information systems aim to ensure that authentication methods, such as passwords and two-factor authentication (2FA), are implemented with adequate security standards. The auditor examines the various authentication methods, including verifying password management policies (e.g., length, complexity, and frequency of password changes) and ensuring additional authentication, such as 2FA, for users with sensitive access. If the system uses biometric authentication or single sign-on (SSO), the auditor will also evaluate the security of the configuration of these methods.

Table 3 presents an example of an audit working paper for authentication validation.

4.3 Audit trail

An audit trail is a record that tracks all user activities within a system, including access, changes, or deletion of data. In

electronic government information systems, audit trails are essential for maintaining security, data integrity, and compliance with audit standards. The primary function of an audit trail is to document all user actions, enabling auditors to assess whether the system has been used in accordance with applicable policies and procedures. Audit trails help detect suspicious activity or security breaches by recording important information, such as user identity, access time, actions taken, and data changed. Table 4 presents an example of an audit trail worksheet.

4.4 Document lifecycle management (DLM)

DLM is the process of managing documents throughout their life cycle, from creation to destruction. In electronic government information systems, DLM ensures that documents are managed in accordance with applicable security, integrity, and compliance standards. This management includes control over access, storage, distribution, and destruction of documents efficiently and securely. Audits of DLM aim to ensure that documents are stored, updated, and deleted according to established procedures, maintaining data integrity and accuracy throughout the document life cycle. Table 5 presents an example of DLM audit working paper used in an electronic government system audit.

4.5 Access control

Access control limits and regulates access to data or resources in a system based on user authorization. In an electronic-based government information system, access control aims to protect critical data and resources from unauthorized access or misuse. Through access control, organizations can determine who is allowed to view, edit, delete, or create specific data within the system. The goal of access control in auditing is to ensure that access rights are granted only to authorized users, aligned with their job requirements, and to minimize security risks that may arise from unauthorized access. Table 6 presents an example of audit working paper for access control.

4.6 Regulations and compliance standards

Organizations must adhere to regulations and compliance standards to ensure that their operations and information systems meet legal, ethical, and security requirements. In the context of governments or large organizations, compliance with relevant standards and regulations is critical to maintaining transparency, data security, and efficient operations. These regulations may include government regulations or international standards designed to ensure the security, privacy, accessibility, and integrity of systems. Examples of commonly applied rules in government information systems include the General Data Protection Regulation (GDPR), ISO/IEC 27001 on information security management, and other local standards applicable in specific regions or countries.

The audit of regulations and compliance standards aims to ensure that the information system meets all applicable requirements.

This audit assesses compliance with each provision set, including privacy policies, data security, and data management practices in accordance with standards. Table 7 presents an example of audit working paper for regulations and compliance standards.

Table 3. Audit working paper for authentication validation

No.	Component ID	Examination Aspect	Status	Information
1	AV-1	Authentication Method	[X/√]	[Information]
2	AV-2	Password Management Policy	[X/√]	[Information]
3	AV-3	Two-Factor Authentication (2FA)	[X/√]	[Information]
4	AV-4	Biometric or Other Authentication	[√/X]	[Information]
5	AV-5	SSO (Single Sign-On) Authentication	[√/X]	[Information]
6	AV-6	Session Management and Automatic Logout	[√/X]	[Information]

Table 4. Audit working paper for audit trail

No.	Component ID	Examination Aspect	Status	Information
1	AT-1	User Access Logging	[X/√]	[Information]
2	AT-2	Recording Data Changes	[X/√]	[Information]
3	AT-3	Data Deletion Recording	[X/√]	[Information]
4	AT-4	Failed Access Event Tracking	[√/X]	[Information]
5	AT-5	Audit Trail Access Monitoring	[√/X]	[Information]

Table 5. Audit working paper for document lifecycle management

No.	Component ID	Examination Aspect	Status	Information
1	LC-1	Document Creation and Recording	[√/X]	[Information]
2	LC-2	Document Access and Security Control	[√/X]	[Information]
3	LC-3	Document Storage and Archiving	[√/X]	[Information]
4	LC-4	Document Maintenance and Updating	[√/X]	[Information]
5	LC-5	Distribution and Version Control	[√/X]	[Information]
6	LC-6	Document Retention and Destruction	[√/X]	[Information]

Table 6. Audit working paper for access control

No.	Component ID	Examination Aspect	Status	Information
1	AC-1	User Identification	[√/X]	[Information]
2	AC-2	Role-Based Access Authorization	[√/X]	[Information]
3	AC-3	User Activity Logging	[√/X]	[Information]
4	AC-4	Access Time Restrictions	[√/X]	[Information]
5	AC-5	Removal or Deactivation of Access	[√/X]	[Information]

Table 7. Audit working paper for regulations and compliance standards

No.	Component ID	Examination Aspect	Status	Information
1	RS-1	Compliance with Privacy Regulations	[√/X]	[Information]
2	RS-2	Compliance with Security Standards	[√/X]	[Information]
3	RS-3	Compliance with Data Retention Policy	[√/X]	[Information]
4	RS-4	Procedure Data Deletion	[√/X]	[Information]
5	RS-5	Managing Regulatory Changes	[√/X]	[Information]
6	RS-6	Incident Recording and Reporting	[√/X]	[Information]

Table 8. Audit working paper for document availability and accessibility

No.	Component ID	Examination Aspect	Status	Information
1	DA-1	Document Availability	[√/X]	[Information]
2	DA-2	Document Backup	[√/X]	[Information]
3	DA-3	Document Search and Accessibility	[√/X]	[Information]
4	DA-4	Digital Accessibility for All Users	[√/X]	[Information]
5	DA-5	Document Storage in a Safe Place	[√/X]	[Information]

Table 9. Audit working paper for document versioning and control

No.	Component ID	Examination Aspect	Status	Information
1	DV-1	Implementation of Document Versioning System	[√/X]	[Information]
2	DV-2	Change History Recording	[√/X]	[Information]
3	DV-3	Revision Approval Procedure	[√/X]	[Information]
4	DV-4	Storing and Managing Previous Versions	[√/X]	[Information]

Table 10. Audit working paper for disaster recovery and data sustainability

No.	Component ID	Examination Aspect	Status	Information
1	DR-1	Implementation of Disaster Recovery Policy	[√/X]	[Information]
2	DR-2	System and Data Recovery Plan	[√/X]	[Information]
3	DR-3	Data Backup	[√/X]	[Information]
4	DR-4	Data Sustainability	[√/X]	[Information]

4.7 Document availability and accessibility

In auditing the reliability of electronic-based government information systems, document availability and accessibility are essential aspects that must be evaluated to ensure that the information system manages documents effectively and that they can be accessed according to applicable needs and regulations. The reliability of the information system includes its ability to provide the required documents at any time without disruption, as well as ensuring that only authorized parties can access the records. Table 8 presents an example of an audit working paper for document availability and accessibility.

4.8 Document versioning and control

Document versioning and control in information systems refers to managing changes occurring throughout a document's life cycle. This is essential to maintaining the integrity and transparency of the document, ensuring that any changes are recorded, and providing the ability to track, recover, or compare different document versions. Document versioning refers to assigning a version number or specific identifier to each revision or change made to a document. Table 9 presents an example of an audit working paper for document versioning and control.

4.9 Disaster recovery and data sustainability

Disaster recovery refers to the policies and procedures designed to recover data and systems disrupted by disasters or system failures. This includes any threat that could disrupt operations, such as natural disasters, cyberattacks, or technical failures. The primary goal of disaster recovery is to ensure that data and systems can be restored as quickly as possible, minimizing downtime and reducing the impact on public services. A robust recovery policy should include a regular data backup strategy, systematic recovery testing, and efficient and well-planned system recovery processes.

Meanwhile, data sustainability focuses on an organization's ability to ensure that data remain secure, available, and accessible without interruption, even during emergencies or disasters. This involves data management that prioritizes both short-term protection and long-term data management, ensuring that data remain usable and accessible to authorized parties. Data sustainability includes secure storage policies,

data backup management, and the continuation of effective data use despite technical disruptions. Table 10 presents an example of an audit working paper for disaster recovery and data sustainability.

4.10 Trustmark implementation

Implementing Trustmark in electronic-based government information systems assures that the system meets specific standards for security, reliability, document validity, and regulatory compliance. Trustmark functions not only as a quality indicator but also as a tool that integrates various elements in the document reliability audit framework, from authentication and data recovery to document management. With Trustmark, government systems can better manage essential documents and data, providing the security and transparency needed to support excellent and accountable governance. The Trustmark labeling mechanism is based on the assessment standards that have been conducted.

The final evaluation results are calculated using the following formula:

$$\text{Total Final Score} = \sum \text{Weighted Score of } Each\ Component \quad (1)$$

Table 11 presents an example of an audit evaluation summary of the reliability of transaction document security.

Based on Table 11, the subsequent step is to provide a reliability rating based on Trustmark using the provisions outlined in Table 12.

Table 11. Example of audit evaluation summary of transaction document security reliability

Component	Category	Comment	Scale (1-5)	Weight (1-50)
Document Integrity	Fulfilled	Documents are protected with digital signatures and encryption.	5	50
Authentication of Validity	Fulfilled	Two-factor authentication for access is implemented.	5	50
Audit Trail	Fulfilled	Audit logs are complete and accessible to auditors.	5	50
Document Lifecycle Management	Fulfilled	Regulatory retention policy, automatic deletion.	5	50
Access Control	Fulfilled	Role-based access control (RBAC) and encryption.	5	50
Regulations and Compliance Standards	Fulfilled	Compliance with ISO 27001 and government regulations	5	50
Document Availability and Accessibility	Fulfilled	Periodic backup and recovery within 4 hours.	5	50
Document Versioning and Control	Fulfilled	Any changes made to the document are automatically recorded.	5	50
Disaster Recovery and Data Sustainability	Fulfilled	The system has a comprehensive disaster recovery plan.	5	50
Total			**45**	**450**

Table 12. Trustmark categories

Category	Score	Description
Less Reliable	0-149	The system has serious weaknesses in reliability, security, or regulatory compliance. It is at high risk due to inadequate or incompletely implemented basic security, authentication, and disaster recovery controls.
Reliable	150-299	The system meets basic reliability standards. There is adequate protection for document security, access, and compliance. However, there are areas for improvement, such as audit trails, disaster recovery, or document lifecycle management.
Very Reliable	300-450	The system is highly reliable and meets all security, integrity, access, compliance, and recovery standards. It implements strict and complete controls in authentication, document management, audit trails, and disaster recovery.

Based on the findings, along with audit examples for each component, there are significant implications for the e-government system in Indonesia, especially in improving the reliability of the electronic-based government information system (EBGS). The practical application of the DRSA framework can ensure that documents and data within the government system are well managed, their integrity is guaranteed, and they are protected from unauthorized access. For example, implementing technologies such as digital signatures and encryption will prevent unauthorized changes to documents, ensuring that the information used for decision-making remains accurate and reliable. In addition, employing strong authentication such as two-factor authentication (2FA) and role-based access control (RBAC) will ensure that only authorized parties can access or modify sensitive data. A complete audit trail is also crucial, as it records every activity within the system, enabling the detection and swift resolution of any violations or suspicious activities. Furthermore, effective document lifecycle management (DLM) ensures that documents are managed from creation to destruction in accordance with applicable policies, maintaining data security and integrity throughout their lifecycle. Compliance with international standards, such as ISO 27001, will also enhance transparency and ensure that e-government systems comply with applicable regulations.

5. CONCLUSIONS

The development of the document reliability and security audit (DRSA) framework is a significant contribution to ensuring the reliability and security of electronic transaction documents within Indonesia's electronic-based government system. DRSA integrates crucial components such as document integrity, authentication, access control, audit transparency, and disaster recovery, supporting more secure and guaranteed information management.

The main innovation in DRSA lies in its ability to address security and transparency challenges often faced in government information systems, while ensuring compliance with global security standards, such as ISO 27001. This framework enables government agencies to be more effective

in identifying system weaknesses, reducing the risk of data manipulation, and strengthening public trust in digital services. In addition, DRSA offers a more comprehensive approach to system audits, focusing on disaster recovery and operational continuity through efficient recovery procedures and automatic backups.

ACKNOWLEDGMENT

My deepest gratitude goes to Prof. Purwanto, my dissertation promoter, who guided me in compiling a comprehensive concept and direction. I am equally grateful to my copromoter, who provided detailed guidance on critical issues that I had not understood. I would also like to thank my colleagues at the institution and my college friends for their openness in sharing knowledge, which greatly helped me in compiling this paper as part of my dissertation.

REFERENCES

[1] Birowo, C.T., Istanti, D. (2023,). Implementation of E-government in accelerating bureaucratic reform in Indonesia. In Proceedings of the Fourth International Conference on Administrative Science (ICAS 2022), pp. 338-348. https://doi.org/10.2991/978-2-38476-104-3_33

[2] Gupta, P., Hooda, A., Jeyaraj, A., Seddon, J.J., Dwivedi, Y.K. (2024). Trust, risk, privacy and security in e-Government use: Insights from a MASEM analysis. Information Systems Frontiers. https://doi.org/10.1007/s10796-024-10497-8

[3] Soraya, N., Muda, I., Sampetoding, E.A. (2023). Analysis of challenges and difficulties in implementing information systems audit: A narrative literature review. Jurnal Inovasi Akuntansi, 1(2): 114-120. https://doi.org/10.36733/jia.v1i2.7753

[4] Ameen, A.A., Ahmad, K. (2017). Information systems strategies to reduce financial corruption. In Leadership, Innovation and Entrepreneurship as Driving Forces of the Global Economy: Proceedings of the 2016 International Conference on Leadership, Innovation and Entrepreneurship (ICLIE), pp. 731-740. https://doi.org/10.1007/978-3-319-43434-6_65

[5] Aditya, B.R., Hartanto, R., Nugroho, L.E. (2018). The role of IT audit in the era of digital transformation. IOP Conference Series: Materials Science and Engineering, 407(1): 012164. https://doi.org/10.1088/1757-899X/407/1/012164

[6] Cichy, C., Rass, S. (2019). An overview of data quality frameworks. IEEE Access, 7: 24634-24648. https://doi.org/10.1109/ACCESS.2019.2899751

[7] Samitsch, C. (2014). Data Quality and Its Impacts on Decision-Making: How Managers can Benefit from Good Data. Springer.

[8] Hassenstein, M.J., Vanella, P. (2022). Data quality—concepts and problems. Encyclopedia, 2(1), 498-510. https://doi.org/10.3390/encyclopedia2010032

[9] Danidou, Y., Schafer, B. (2012). Legal environments for digital trust: Trustmarks, trusted computing and the issue of legal liability. Journal of International Commercial Law and Technology, 7(3), 212-222.

[10] Ganji, D., Kalloniatis, C., Mouratidis, H., Gheytassi, S.M. (2019). Approaches to develop and implement ISO/IEC 27001 standard-information security management systems: A systematic literature review. International Journal on Advances in Software, 12(3): 228-238.

[11] Kautenburger, T. (2000). Sicherheit im electronic commerce/security in electronic commerce. it-Information Technology, 42(3): 26-31. https://doi.org/10.1524/itit.2000.42.3.26

[12] Sarjito, A. (2024). Data security and privacy in the digital era: Challenges for modern government. JIAN-Jurnal Ilmiah Administrasi Negara, 8(3): 1-13.

[13] Kim, J., Lee, C., Chang, H. (2020). The development of a security evaluation model focused on information leakage protection for sustainable growth. Sustainability, 12(24): 10639. https://doi.org/10.3390/su122410639

[14] Antón, A., Blough, D.M., Reddick, E.A., Swire, P. (2014). Trustmarks and privacy. https://bpb-us-e1.wpmucdn.com/sites.gatech.edu/dist/3/3097/files/2015/08/trustmarks-and-privacy.pdf.

[15] Öksüz, A., Walter, N., Distel, B., Räckers, M., Becker, J. (2016). Trust in the information systems discipline. In Trust and Communication in a Digitized World: Models and Concepts of Trust Research, pp. 205-223. https://doi.org/10.1007/978-3-319-28059-2_12

[16] Thompson, F.M., Tuzovic, S., Braun, C. (2019). Trustmarks: Strategies for exploiting their full potential in e-commerce. Business Horizons, 62(2): 237-247. https://doi.org/10.1016/j.bushor.2018.09.004

[17] Costé, B., Ray, C., Coatrieux, G. (2019). Trust assessment for the security of information systems. Advances in Knowledge Discovery and Management, 8: 159-181. https://doi.org/10.1007/978-3-030-18129-1_8

[18] Pereira, T.S.M., Santos, H. (2010). A security framework for audit and manage information system security. In 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, Toronto, ON, Canada, pp. 29-32. https://doi.org/10.1109/WI-IAT.2010.244

[19] Herath, H.S., Herath, T.C. (2014). IT security auditing: A performance evaluation decision model. Decision Support Systems, 57: 54-63. https://doi.org/10.1016/j.dss.2013.07.010

[20] Spremic, M. (2011). Standards and frameworks for information system security auditing and assurance. In Proceedings of the World Congress on Engineering, London, U.K., pp. 251-266.

[21] Novianto, F. (2020). Electronic government development strategies using frameworks COBIT 5. Proceeding International Conference on Science and Engineering, 3: 263-271. https://doi.org/10.14421/icse.v3.511

[22] Wijanarko, R.P., Audina, I., Saputri, D.A.E., Rabbanii, N.A.N., Suryanto, T.L.M. (2023). Implementation of the Cobit 2019 framework to improve information technology performance in Tokopedia. IJEEIT: International Journal of Electrical Engineering and Information Technology, 6(2): 51-62. https://doi.org/10.29138/ijeeit.v6i2.2245

[23] Bârsan, M. (2017). Aspects regarding the implementation of information security standards in organizations. Revista Română de Biblioteconomie și Știința Informării, 13(1): 21-26. https://doi.org/10.26660/rrbsi.2017.13.1.21

[24] Kitsios, F., Chatzidimitriou, E., Kamariotou, M. (2023).

The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector. Sustainability, 15(7): 5828. https://doi.org/10.3390/su15075828
[25] Irawan, H., Muhammad, A.H., Nasiri, A. (2024). Design of cybersecurity maturity assessment framework using NIST CSF v1.1 and CIS controls v8. Jurnal Inovtek Polbeng Seri Informatika, 9(1): 126-139. https://doi.org/10.35314/isi.v9i1.3973
[26] Tanjung, D.F., Nurhayati, O.D., Wibowo, A. (2024). Design information security in electronic-based government systems using NIST CSF 2.0, ISO/IEC 27001: 2022 and CIS control. International Journal of Innovative Science and Research Technology, 9(6): 523-530. https://doi.org/10.38124/ijisrt/IJISRT24JUN1212
[27] Jayanthi, M.K. (2017). Strategic planning for information security-DID mechanism to befriend the cyber criminals to assure cyber freedom. In 2017 2nd International Conference on Anti-Cyber Crimes (ICACC), Abha, Saudi Arabia, pp. 142-147. https://doi.org/10.1109/Anti-Cybercrime.2017.7905280
[28] Al-Matari, O.M., Helal, I.M., Mazen, S.A., Elhennawy, S. (2021). Integrated framework for cybersecurity auditing. Information Security Journal: A Global Perspective, 30(4): 189-204. https://doi.org/10.1080/19393555.2020.1834649
[29] Prastowo, S.L., Sudiana, D. (2024). Recommendations for a framework for handling security incidents of electronic-based government systems (SPBE) using the ISO/IEC 27035: 2023 standard. JINAV: Journal of Information and Visualization, 5(1): 107-114.
[30] Akbar, P., Nurmandi, A., Irawan, B., Loilatu, M.J. (2022). Research trends in e-Government interoperability: Mapping themes and concepts based on the scopus database. JeDEM-eJournal of eDemocracy and Open Government, 14(2): 83-108. https://doi.org/10.29379/jedem.v14i2.707
[31] Anyanwu, A., Olorunsogo, T., Abrahams, T.O., Akindote, O.J., Reis, O. (2024). Data confidentiality and integrity: A review of accounting and cybersecurity controls in superannuation organizations. Computer Science & IT Research Journal, 5(1): 237-253. https://doi.org/10.51594/csitrj.v5i1.735

NOMENCLATURE

IN Integrity
AV Authentication of Validity
AT Audit Trail
LC Lifecycle Management
AC Access Control
RS Regulations and Compliance Standards
DA Document Availability and Accessibility
DV Document Versioning and Control
DR Disaster Recovery and Data Sustainability