JGSP
Jurnal Greenation Sosial dan Politik
+62 81210467572 https://greenationpublisher.org/JGSP greenation.info@gmail.com
GREENATION PUBLISHER

DOI: https://doi.org/10.38035/jgsp.v4i2

Digital Fiscal Government and State Financial Data Protection: A New Legal Framework for Digital Auditing in Indonesia

KMS Herman[1], Iqbal Ramadhan[2], Pan Panissa Barlian[3], Surya[4], Hendry Juanda[5]
[1]Universitas Borobudur, Jakarta, Indonesia, kms_herman@borobudur.ac
[2]Universitas Borobudur, Jakarta, Indonesia, iqbalramadhan89@gmail.com
[3]Universitas Borobudur, Jakarta, Indonesia, pan.barlian@gmail.com
[4]Universitas Borobudur, Jakarta, Indonesia, surya.obe88@gmail.com
[5]Universitas Borobudur, Jakarta, Indonesia, juandahendry178@gmail.com

Corresponding Author: kms_herman@borobudur.ac[1]

Abstract: *The digital transformation of public administration has significantly altered the management of state finances in Indonesia. The integration of information technology into budgeting, revenue collection, expenditure management, and financial reporting has given rise to the concept of digital fiscal government, which relies on data-driven governance to improve efficiency, transparency, and accountability. Alongside these developments, the increasing dependence on digital systems has generated new legal challenges concerning the protection of state financial data, particularly within the implementation of digital auditing. Existing regulations governing public finance, electronic systems, and data protection remain fragmented and have not yet established a comprehensive legal framework capable of addressing the complexities of digital audits. This study aims to examine the development of digital fiscal government in Indonesia, identify legal issues related to the protection of state financial data in digital auditing, and formulate a legal framework that supports effective and accountable digital audit practices. The research employs a normative juridical method using statutory, conceptual, and comparative approaches. Legal materials are analyzed qualitatively through the interpretation of legislation, legal doctrines, and relevant scholarly works concerning public finance governance, digital government, and data protection. The findings indicate that the rapid digitalization of fiscal administration has not been accompanied by specific regulations governing digital auditing. This regulatory gap creates legal uncertainty regarding data access authority, cybersecurity standards, accountability for technology-based audit mechanisms, and the protection of strategic state financial information. Furthermore, the growing use of data analytics and artificial intelligence in auditing raises concerns regarding transparency, reliability, and legal responsibility for algorithm-based decisions. Therefore, a new legal framework is required to integrate principles of state financial data protection, cybersecurity, technological accountability, and digital governance. Such a framework is essential to ensure legal certainty and strengthen the effectiveness of digital auditing within Indonesia's evolving fiscal governance system.*

Keyword: *digital fiscal government, digital auditing, state financial data protection, public finance, digital governance.*

Abstrak: Transformasi digital dalam pengelolaan keuangan negara telah mengubah pola hubungan antara pemerintah, data fiskal, dan mekanisme pengawasan publik. Integrasi berbagai sistem elektronik dalam pengelolaan anggaran, penerimaan negara, serta pelaksanaan belanja negara mendorong munculnya *konsep digital fiscal government* yang menempatkan data sebagai instrumen utama pengambilan keputusan dan pengawasan. Di sisi lain, peningkatan penggunaan teknologi digital juga menimbulkan persoalan hukum baru, khususnya berkaitan dengan perlindungan data keuangan negara dalam pelaksanaan audit digital. Kerangka hukum yang berlaku saat ini masih tersebar dalam berbagai peraturan sektoral sehingga belum mampu memberikan kepastian hukum mengenai akses data, keamanan informasi, pertanggungjawaban penggunaan teknologi, dan batas kewenangan auditor dalam lingkungan digital. Penelitian ini bertujuan untuk menganalisis perkembangan *digital fiscal government* di Indonesia, mengidentifikasi permasalahan hukum yang muncul dalam perlindungan data keuangan negara, serta merumuskan konstruksi hukum yang dapat mendukung pelaksanaan audit digital secara efektif dan akuntabel. Penelitian menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan komparatif. Bahan hukum dianalisis secara kualitatif melalui penafsiran terhadap norma-norma yang mengatur pengelolaan keuangan negara, pemerintahan digital, dan perlindungan data. Hasil penelitian menunjukkan bahwa perkembangan digitalisasi fiskal belum diikuti dengan pembentukan regulasi yang secara khusus mengatur audit digital sebagai instrumen pengawasan keuangan negara. Kekosongan pengaturan tersebut berpotensi menimbulkan risiko penyalahgunaan akses data, kebocoran informasi strategis negara, serta ketidakjelasan pertanggungjawaban hukum dalam penggunaan teknologi audit berbasis algoritma. Diperlukan kerangka hukum baru yang mengintegrasikan prinsip keamanan data, akuntabilitas teknologi, transparansi algoritma, dan perlindungan kepentingan fiskal negara guna mewujudkan sistem audit digital yang responsif terhadap perkembangan teknologi informasi.

Kata Kunci: digital fiscal government, audit digital, data keuangan negara, perlindungan data, keuangan negara.

INTRODUCTION

Digital transformation has become one of the defining characteristics of contemporary public governance. Advances in information and communication technologies have reshaped not only public service delivery but also governmental planning, decision-making, oversight, and resource management. Within modern governance systems, digitalization has encouraged the emergence of data-driven, integrated, and efficiency-oriented public administration models. These developments are particularly evident in the field of public financial management, which serves as a fundamental instrument through which governments deliver public services, implement development programs, and maintain economic stability.

In Indonesia, the digital transformation of the public sector has been manifested through the implementation of various electronic systems supporting fiscal administration. The adoption of Electronic-Based Government Systems (SPBE), Regional Government Information Systems (SIPD), the State Treasury and Budget System (SPAN), and other digital financial platforms demonstrates the increasing reliance on technology throughout the public financial management cycle, including planning, budgeting, execution, reporting, evaluation, and oversight. As a result, government financial activities generate vast amounts of interconnected and continuously expanding digital data.

These developments have contributed to the emergence of the concept of digital fiscal government, which refers to a model of fiscal governance that relies on digital technologies, integrated information systems, data analytics, and automated administrative processes to enhance the effectiveness and efficiency of public financial management. Within this framework, data functions as a strategic asset that supports evidence-based policymaking, promotes transparency, and strengthens governmental accountability. State financial data encompasses information relating to public revenues, expenditures, procurement activities, intergovernmental transfers, development financing, and other fiscal policies that significantly influence national economic performance.

As the complexity and volume of governmental financial data continue to increase, conventional oversight mechanisms face significant limitations. Traditional auditing methods, which largely depend on manual document reviews and sampling techniques, are often unable to effectively examine the entirety of digital and real-time financial transactions. This situation has encouraged the development of digital auditing as an innovative approach to public financial oversight. Digital auditing utilizes information technology, data analytics, artificial intelligence (AI), machine learning, and automated monitoring systems to identify risks, detect anomalies, and conduct continuous supervision of governmental financial activities.

The implementation of digital auditing offers substantial advantages compared with conventional auditing practices. The ability to analyze entire populations of financial transactions rather than selected samples increases the comprehensiveness and reliability of audit findings. Advanced analytical tools facilitate the early detection of irregularities that may indicate fraud, corruption, inefficiencies, or misuse of public resources. Furthermore, integration between auditing systems and governmental financial platforms enables real-time monitoring, transforming financial oversight from a reactive mechanism into a proactive and preventive governance instrument.

Despite these advantages, the adoption of digital auditing presents significant legal and regulatory challenges. Expanded access to governmental financial data raises concerns regarding the scope of auditors' authority, inter-agency data sharing, confidentiality obligations, and legal accountability for the collection, processing, and utilization of digital information. These concerns are particularly important because state financial data constitutes a strategic national asset whose unauthorized disclosure or misuse may affect public trust, economic stability, and national security.

Additional challenges arise from the growing prevalence of cybersecurity threats targeting government information systems. Incidents involving cyberattacks and data breaches have demonstrated that digital transformation, while improving administrative efficiency, simultaneously creates vulnerabilities related to unauthorized access, data manipulation, information theft, and operational disruptions. Within the context of digital auditing, these risks become even more significant because auditors require access to highly sensitive financial information that contains strategic governmental data.

The increasing use of artificial intelligence and algorithmic decision-making systems in audit processes also raises concerns regarding transparency, accountability, and the reliability of audit outcomes. AI-based systems are capable of generating audit findings, risk assessments, and recommendations through complex data analysis processes. However, reliance on algorithmic technologies creates questions regarding the legal validity of automated decisions, algorithm verification mechanisms, potential systemic biases, and the allocation of responsibility when technological systems produce inaccurate or misleading results.

These developments reveal a substantial gap between technological innovation and the existing legal framework governing public financial management in Indonesia. Regulations concerning state finance, public financial audits, electronic government administration, data protection, and information security remain fragmented across multiple legal instruments developed for different regulatory purposes. Consequently, Indonesia currently lacks a comprehensive legal framework specifically governing digital auditing as a mechanism of public financial oversight. Existing state finance legislation was enacted before the widespread adoption of data-driven auditing technologies and therefore provides limited guidance regarding digital audit systems, artificial intelligence, and large-scale governmental data processing. Similarly, existing data protection regulations primarily focus on personal data rights and do not specifically address the protection of state financial data as a strategic public asset. This situation reflects a significant normative gap that requires further legal examination.

At the international level, many jurisdictions have introduced regulatory frameworks addressing government data governance, technology-driven auditing, public-sector cybersecurity, and the use of artificial intelligence in financial oversight. These developments illustrate a global trend toward establishing legal systems capable of balancing technological innovation with data protection, accountability, and public interest considerations. Indonesia faces a similar challenge in developing a legal framework that supports the digital transformation of fiscal governance while ensuring the integrity, security, and accountability of state financial data.

Against this background, this study addresses two principal research questions. First, how is the protection of state financial data currently regulated within the implementation of digital auditing in Indonesia? Second, what legal framework is required to support digital auditing while simultaneously ensuring adequate protection of state financial data? Accordingly, this study aims to analyze the existing legal framework, identify normative challenges arising from the implementation of digital auditing, and formulate a legal framework capable of supporting effective, accountable, and secure digital audit practices. The findings are expected to contribute to the development of public finance law, technology law, and digital governance scholarship while providing normative recommendations for future legal reforms concerning digital auditing in Indonesia.

METHOD

This study employs a normative legal research method, focusing on the analysis of legal norms governing public financial management, state financial audits, digital government, data protection, and information security in the context of digital auditing. This approach is considered appropriate because the study aims to evaluate the adequacy of the existing legal framework and formulate a legal model capable of supporting the implementation of digital auditing within Indonesia's public financial management system.

The research applies three complementary approaches: the statutory approach, the conceptual approach, and the comparative approach. The statutory approach involves an examination of relevant legislation, including Law No. 17 of 2003 on State Finance, Law No. 1 of 2004 on State Treasury, Law No. 15 of 2004 on the Audit of State Financial Management and Accountability, Law No. 27 of 2022 on Personal Data Protection, as well as regulations governing Electronic-Based Government Systems (SPBE) and public-sector information security.

The conceptual approach is utilized to analyze theoretical and legal concepts related to digital fiscal government, digital auditing, data governance, cybersecurity, data protection, and technological accountability. Meanwhile, the comparative approach examines legal frameworks and regulatory practices concerning digital auditing and public financial data protection in selected jurisdictions that have implemented advanced digital government systems. The comparative analysis aims to identify best practices that may serve as references for legal development in Indonesia.

The study relies on primary, secondary, and tertiary legal materials. Primary legal materials consist of legislation, official government documents, and other legally binding instruments. Secondary legal materials include academic books, scholarly journal articles, research reports, and expert opinions relevant to the subject matter. Tertiary legal materials comprise legal dictionaries, encyclopedias, and other supporting references.

Legal materials were collected through library research and analyzed qualitatively using legal interpretation, legal construction, and legal reasoning methods. The analysis seeks to identify normative legal issues, assess the adequacy of existing regulations, and formulate recommendations for a comprehensive legal framework that supports effective digital auditing while ensuring the protection of state financial data in the digital era.

RESULT AND DISCUSSION

Legal Regulation of State Financial Data Protection in the Implementation of Digital Auditing in Indonesia

Digital transformation has fundamentally changed the way governments manage, store, and utilize fiscal information. The implementation of various electronic systems, including the Electronic-Based Government System (SPBE), the Regional Government Information System (SIPD), and the State Treasury and Budget System (SPAN), demonstrates that digital technology has become a core foundation of public financial governance in Indonesia (Presidential Regulation No. 95 of 2018; Heeks, 2018). This digitalization has generated massive volumes of financial data that continue to expand in scale and complexity, creating an increasing need for governance mechanisms capable of ensuring data security, integrity, and accountability.

From the perspective of modern public governance, state financial data should no longer be viewed merely as an administrative product but rather as a strategic asset possessing economic, political, and legal value. Such data encompass information related to state revenues, public expenditures, intergovernmental fiscal transfers, public procurement activities, state asset management, and various fiscal policy instruments that serve as the basis for governmental decision-making (Law No. 17 of 2003; Mardiasmo, 2021). Consequently, the protection of state financial data constitutes an essential component of ensuring governmental accountability and maintaining national economic stability.

Advances in information technology have encouraged the transformation of public financial oversight from conventional auditing methods to digital auditing systems. Digital auditing employs information technology, big data analytics, artificial intelligence (AI), and continuous auditing mechanisms to enhance the effectiveness of public financial examinations (Vasarhelyi, Kogan, & Tuttle, 2015). Through these technologies, auditors are no longer limited to traditional sampling techniques but are capable of analyzing entire populations of financial transactions in a more efficient and accurate manner (Chan & Vasarhelyi, 2022).

Despite these advantages, the implementation of digital auditing raises complex legal concerns. Digital auditing requires extensive access to governmental databases integrated across various electronic systems. Such access creates questions regarding the scope of auditors' authority, data utilization procedures, and legal accountability for information obtained during audit processes. Within this context, the protection of state financial data emerges as a central issue requiring special attention in the development of digital auditing systems.

The findings of this study indicate that Indonesia currently lacks a specific legal framework governing the protection of state financial data in the context of digital auditing. Existing regulations remain fragmented across various legal instruments concerning state finance, public financial audits, digital government, and general data protection. This fragmentation creates legal uncertainty and may hinder the effective implementation of digital auditing practices.

Law No. 17 of 2003 on State Finance serves as the primary legal foundation for public financial management in Indonesia. The law establishes that state finances must be managed in an orderly, lawful, efficient, effective, transparent, and accountable manner (Law No. 17 of 2003). These principles indirectly provide a normative basis for protecting state financial data because effective fiscal governance depends heavily on the accuracy and security of information used in governmental administration (Sutedi, 2022). However, the law does not explicitly regulate digital data security, financial database governance, or information protection mechanisms within digital government environments.

Similar regulatory limitations are found in Law No. 1 of 2004 on State Treasury. Although the statute governs budget execution, treasury management, and financial accountability, it does not adequately address data protection issues arising from the digitalization of treasury operations. This gap is significant considering that most contemporary treasury activities are conducted through electronic systems that generate large volumes of highly sensitive financial data.

From an oversight perspective, Law No. 15 of 2004 on the Audit of State Financial Management and Accountability grants auditors the authority to obtain documents, data, and information necessary for conducting audits (Law No. 15 of 2004). While this authority is essential for effective financial oversight, the legislation was enacted before the widespread adoption of digital auditing technologies. Consequently, it provides limited guidance regarding access to electronic databases, data analytics technologies, or the protection of information obtained through digital audit procedures.

In practice, expanded auditor access to digital information must be balanced by obligations to maintain confidentiality and information security. Such a balance represents a fundamental principle of digital audit governance. Nevertheless, this study finds that Indonesian law has yet to establish a comprehensive framework governing the relationship between access rights and data protection obligations (Yusuf, 2020; Mulyadi, 2021).

The development of SPBE has further accelerated data integration among government institutions, enabling more efficient information exchange and evidence-based decision-making (Presidential Regulation No. 95 of 2018; Indrajit, 2021). While data integration enhances administrative efficiency and audit effectiveness, increasing interconnectivity simultaneously expands risks associated with unauthorized access, data breaches, and information misuse. These risks demonstrate that digital transformation must be accompanied by adequate legal safeguards for state financial data (Arum & Falaakh, 2023).

The enactment of Law No. 27 of 2022 on Personal Data Protection represents a significant advancement in Indonesia's digital governance framework. The law establishes data subject rights and imposes obligations on entities processing personal data (Law No. 27 of 2022). However, its scope does not fully address the protection needs of state financial data. Much of the information processed within public financial systems does not constitute personal data but rather strategic governmental information related to fiscal policy, budgeting, and national interests (Soponyono, 2023). Therefore, state financial data protection requires a distinct legal approach beyond the conventional framework of personal data protection.

Furthermore, digital auditing faces substantial cybersecurity challenges. Digital audit systems depend on technological infrastructures consisting of software applications, databases, communication networks, and electronic storage systems. Any disruption affecting these components may compromise audit quality and threaten the security of state financial information. From an information security perspective, effective protection requires the preservation of confidentiality, integrity, and availability—the three foundational principles of information security governance (Stallings, 2019; ISO/IEC 27001, 2022).

Cyber threats such as hacking, data theft, malware, and ransomware attacks demonstrate that state financial data protection cannot be separated from broader national cybersecurity policies. Accordingly, the legal framework governing digital auditing must integrate data protection requirements with nationally and internationally recognized information security standards (Government Regulation No. 71 of 2019; ISO/IEC 27001, 2022).

Legal Challenges of Digital Auditing and State Financial Data Protection

The implementation of digital auditing in public financial management involves not only technological transformation but also complex legal challenges that require further regulatory development. The transition from document-based auditing toward data-driven auditing has created a need for a legal framework capable of balancing effective oversight mechanisms and the protection of strategic state information.

One of the primary legal issues in digital auditing concerns the authority to access state financial data. Auditors require extensive access to various governmental information systems to obtain a comprehensive understanding of financial transactions and fiscal activities. Such access is necessary to ensure accurate examinations and to identify potential irregularities at an early stage. However, expanded access to financial information may also create risks if it is not accompanied by clear governance mechanisms.

From the perspective of administrative law, every authority granted to supervisory institutions must be exercised based on the principles of legality and accountability. The authority of auditors to obtain financial information should not be interpreted as unlimited power but rather as a regulated authority restricted by audit objectives, information necessity, and data protection principles (Yusuf, 2020). Therefore, regulations are required concerning data usage limitations, audit data retention, and confidentiality obligations.

Another significant issue relates to the classification of state financial data. Not all financial information possesses the same level of sensitivity. Certain categories of financial information may be considered public information due to transparency and public accountability requirements. However, other information may have strategic characteristics directly related to national interests and therefore require stronger protection.

Law No. 14 of 2008 on Public Information Disclosure establishes that public information is generally accessible to citizens, while certain categories may be restricted when disclosure threatens state interests (Law No. 14 of 2008). This demonstrates that state financial data governance requires a clear classification mechanism distinguishing between public, restricted, and confidential information.

The absence of a comprehensive data classification framework may create uncertainty in digital auditing practices. Auditors may face difficulties in determining which categories of data may be accessed, stored, or shared during audit processes. Conversely, government institutions require legal certainty regarding their obligations to provide information to auditors.

Beyond access and classification issues, cybersecurity represents a major challenge in digital auditing implementation. Digitally connected state financial systems face various cyber risks, including data theft, information manipulation, attacks against technological infrastructure, and disruption of governmental services.

Information security in digital auditing must preserve three fundamental principles: confidentiality, integrity, and availability (Stallings, 2019). Confidentiality ensures that information is accessible only to authorized parties. Integrity guarantees that data remains accurate and protected from unauthorized modification. Availability ensures that information can be accessed when required for audit activities (ISO/IEC 27001, 2022).

These cybersecurity threats demonstrate that protecting state financial data cannot rely solely on administrative approaches. Effective protection requires integration between legal regulation, technological security standards, and institutional capacity development. Digital audit systems require risk management mechanisms capable of preventing, detecting, and responding to information security incidents.

The development of artificial intelligence (AI) in digital auditing also introduces new legal challenges. AI technologies enable auditors to analyze millions of transactions within a short period and identify patterns potentially associated with financial irregularities (AICPA & CIMA, 2022). Nevertheless, AI implementation raises concerns regarding transparency, analytical validity, and legal responsibility when automated systems generate inaccurate results.

Algorithm-based systems often produce decisions that are difficult to explain when their internal processes lack transparency. This phenomenon is commonly referred to as the “black box algorithm” problem, where users understand the outcome but cannot fully understand the reasoning process behind the decision (Pasquale, 2015). In public sector auditing, this issue may affect the legitimacy of audit findings because auditors must be able to explain the basis of their conclusions.

Therefore, the use of AI in digital auditing must comply with principles of transparency and accountability. Algorithmic audit results must be explainable, verifiable, and legally accountable. This approach aligns with global developments emphasizing responsible artificial intelligence governance within public sector digital transformation (European Commission, 2019).

Comparative Analysis of Digital Auditing Regulation and State Financial Data Protection

The development of digital auditing in public financial management is not limited to Indonesia but has become part of broader public governance reforms worldwide. Comparative legal analysis is necessary to examine how different countries establish relationships between fiscal digitalization, technological auditing systems, and the protection of public financial data. This comparative approach is important because digital transformation in the public sector generates similar legal challenges, particularly regarding data security, access authority, and technological accountability.

One country frequently recognized for its advanced digital government development is Estonia. The country has implemented electronic governance through a digital government model that places data integration and system interoperability as fundamental elements of public administration. Digital identity systems and inter-agency data exchange mechanisms enable government institutions to provide faster and more data-driven public services.

Estonia’s experience demonstrates that successful digital government transformation depends not only on technological infrastructure but also on legal frameworks governing data governance. Digital systems require mechanisms ensuring information security, transparency in data utilization, and supervision over entities with access to governmental information systems (Heeks, 2018).

In the context of digital auditing, Estonia’s model highlights the importance of integrating government financial systems with technology-based oversight mechanisms. Auditors can conduct examinations more effectively because financial information is available within structured digital environments. However, access remains controlled through security mechanisms and authorization systems to prevent unauthorized use of sensitive information.

Singapore also represents a successful example of digital government development. The Singaporean government has adopted a smart government approach by treating data as a strategic national asset. Inter-agency data integration is implemented through technological standards and strict information governance frameworks.

Singapore’s experience demonstrates that fiscal digitalization requires strong institutions, reliable digital infrastructure, and consistent information security standards. The utilization of technology in public financial audits must be supported by adequate human resources, cybersecurity capacity, and regulations providing certainty regarding governmental data usage.

The European Union has also placed significant emphasis on data protection within digital transformation. Through the General Data Protection Regulation (GDPR), the European Union developed data protection principles emphasizing transparency, purpose limitation, secure data processing, and accountability of data controllers.

Although GDPR primarily regulates personal data protection, its principles are highly relevant to state financial data governance. Principles of accountability, transparency, and secure information processing may serve as foundations for developing Indonesia's digital auditing legal framework.

The comparative analysis demonstrates that successful digital auditing depends not only on technological capabilities but also on the quality of legal frameworks regulating relationships among governments, auditors, and data. Indonesia therefore requires a comprehensive legal framework integrating principles of public finance, auditing authority, data protection, and cybersecurity.

Legal Framework for Digital Auditing Based on State Financial Data Protection

Based on the analysis of digital fiscal government development and legal challenges in digital auditing implementation, Indonesia requires a new legal framework capable of addressing technology-based public financial oversight. Such a framework must balance transparency requirements, audit effectiveness, and the protection of strategic state information.

First, specific regulations concerning the classification of state financial data are necessary. Financial information should be categorized based on accessibility and sensitivity levels. Public data may serve transparency objectives, while restricted and confidential data require stronger protection through controlled access mechanisms.

Second, strengthening data governance principles in public financial management is essential. Every process involving data collection, utilization, storage, and exchange must have a clear legal basis. Data governance should include authorization mechanisms, user activity records, and supervision over information usage.

Third, digital auditing requires national information security standards. Encryption, multi-factor authentication, access control mechanisms, and security monitoring systems should become mandatory components of state financial data management (ISO/IEC 27001, 2022).

Fourth, the utilization of artificial intelligence in digital auditing requires regulations concerning algorithmic transparency and legal accountability. AI-based audit systems must be capable of explaining the basis of their analytical processes and recommendations.

Fifth, strengthening digital auditor competencies is essential. Future auditors must possess not only accounting and legal expertise but also capabilities in data analytics, cybersecurity, and information technology.

Therefore, Indonesia's digital auditing legal framework should be developed based on principles of transparency, accountability, security, and data protection. Such a framework would support an adaptive public financial oversight system capable of responding to technological developments.

Implications for Legal Reform and Public Financial Governance in Indonesia

Based on the findings of this study, the development of digital fiscal government has fundamentally transformed the management and oversight of public finances. This transformation demonstrates that public financial law can no longer be understood solely through conventional administrative approaches but must adapt to technological development, data integration, and the use of artificial intelligence in governmental processes.

The primary issue identified in this research is the gap between the advancement of digital auditing technologies and the existing regulatory framework. Current regulations on state finance and public financial audits provide fundamental principles for financial management and oversight but do not specifically regulate digital data governance, information security, and automated technologies in audit processes (Law No. 17 of 2003; Law No. 15 of 2004).

This situation demonstrates the necessity of legal reform capable of addressing public financial oversight requirements in the digital era. Such reform does not necessarily require entirely new legislation but may be achieved through harmonization of existing regulations to establish a comprehensive and integrated legal framework.

One of the most important regulatory developments concerns the recognition of state financial data as a distinct legal object with unique characteristics. State financial data differs from personal data because it relates to public interests, fiscal policies, and national economic stability. Therefore, its protection requires a legal approach combining transparency principles and national security considerations.

Regulatory strengthening is also required concerning the relationship between auditors and digital government systems. Auditors must have legal certainty regarding their authority to access electronic information, while simultaneously being subject to appropriate oversight mechanisms ensuring that data utilization remains within audit purposes.

In this context, the concept of continuous digital auditing represents a potential future direction for public financial oversight. This model enables continuous monitoring of financial transactions through real-time data analysis. Unlike traditional auditing conducted after activities are completed, digital auditing allows governments to identify risks earlier and implement corrective measures before financial losses occur (Chan & Vasarhelyi, 2022).

However, the implementation of continuous auditing requires institutional transformation. Auditors will no longer function merely as evaluators after financial activities occur but will become risk-based supervisors utilizing advanced data analytics. Such transformation requires enhanced auditor competencies and adaptation of audit standards.

Beyond regulatory aspects, reform must also address institutional capacity. Increasingly integrated state financial data systems require stronger coordination among governmental institutions. Every institution generating, storing, or processing financial information must comply with consistent data governance standards.

Human resource development is equally important. Digital auditing technologies cannot function effectively without auditors possessing adequate knowledge of information systems, data analytics, cybersecurity, and artificial intelligence. Therefore, strengthening digital competencies among auditors becomes a crucial element of public financial oversight reform.

Accordingly, digital audit reform should focus on developing a legal ecosystem integrating three essential components: technology, regulation, and institutional capacity. These elements must operate harmoniously to ensure that digital transformation improves public financial accountability while maintaining adequate protection of strategic state information.

CONCLUSION

Digital transformation in public financial management has fundamentally changed fiscal governance and governmental oversight mechanisms. The development of the concept of digital fiscal government demonstrates that data has become a strategic element throughout the entire cycle of public financial management, including planning, budgeting, implementation, reporting, and accountability processes. This transformation has shifted the traditional auditing paradigm toward digital auditing systems that utilize information technology, data analytics, automation, and artificial intelligence to improve the effectiveness and quality of public financial examinations.

Based on the findings of this study, it can be concluded that the protection of state financial data in the implementation of digital auditing in Indonesia does not yet have a specific, comprehensive, and integrated legal framework. Regulations concerning public finance management, financial audits, electronic government systems, information disclosure, and data protection remain distributed across various legal instruments. Although these regulations provide fundamental legal foundations for public financial governance and digital government transformation, they have not fully addressed the complexity of legal issues arising from technology-based auditing practices.

Law No. 17 of 2003 on State Finance establishes fundamental principles requiring state financial management to be conducted in an orderly, transparent, efficient, effective, and accountable manner. Furthermore, Law No. 15 of 2004 on the Audit of State Financial Management and Accountability grants audit institutions authority to obtain documents, information, and data required for examination processes. However, these regulations do not specifically regulate electronic data governance, limitations on auditor access to governmental digital systems, protection mechanisms for audit data, or the utilization of artificial intelligence-based analytical technologies in auditing.

Meanwhile, Law No. 27 of 2022 on Personal Data Protection provides a legal foundation for protecting data processed through electronic systems. Nevertheless, state financial data differs from personal data because it does not merely concern individual identities but also includes fiscal policies, government transactions, budget management, state assets, and strategic national interests. Therefore, protecting state financial data requires a specialized legal approach capable of balancing public information transparency with national security interests.

The implementation of digital auditing creates several legal challenges, particularly regarding auditor access authority, classification of financial information, information security, artificial intelligence utilization, and legal responsibility for technological failures or data misuse. These challenges demonstrate that digital transformation in public financial management cannot rely solely on technological advancement but requires a legal framework that provides certainty, accountability, and adequate protection.

An effective lEgal framework for digital auditing should be developed based on principles of data governance, information security, technological accountability, and protection of public interests. Such regulations should address the classification of state financial data according to sensitivity levels, authority-based data access mechanisms, cybersecurity standards, algorithmic transparency, and allocation of responsibilities among auditors, system administrators, and government institutions. Through such regulation, digital auditing can become an effective instrument for strengthening transparency and accountability in public financial management.

Accordingly, the government and legislators should strengthen regulations specifically governing digital auditing within public financial management systems. Such regulations should provide legal certainty regarding the status of state financial data, limitations on auditor access to digital information, data protection obligations, and security standards required for governmental institutions managing financial information.

In addition to regulatory strengthening, Indonesia requires a clear classification system for state financial data that distinguishes between public information, restricted information, and strategic state information. This classification is necessary to determine the level of legal protection and procedures for data utilization in digital audit processes.

Audit institutions and public financial authorities should also strengthen information security capabilities through cybersecurity standards, access control mechanisms, data encryption, and continuous monitoring of digital systems. Data protection requires not only legal instruments but also strong technological and institutional support.

The utilization of artificial intelligence in digital auditing must also be accompanied by regulations concerning algorithmic transparency, analytical reliability, and legal accountability mechanisms. Technology-based audit systems must be capable of explaining their analytical processes to ensure that audit decisions remain verifiable and legally accountable.

Therefore, the development of digital auditing within Indonesia's public financial management system requires synergy between regulation, technology, and institutional capacity. Adaptive legal reform that responds to digital transformation will strengthen public financial oversight while ensuring adequate protection of strategic state information in the era of electronic government.

REFERENCE

AICPA & CIMA. (2022). *Audit Analytics and Artificial Intelligence: Transforming the Future of Assurance*. New York: Association of International Certified Professional Accountants.

Alfarisi, Muhammad Salman. (2023). "Cyber Security dan Perlindungan Data Pemerintah di Indonesia." Jurnal Legislasi Indonesia, 20(2).

Alfarisi, Muhammad Salman. (2023*). "Keamanan Siber dan Perlindungan Data Pemerintah dalam Era Transformasi Digital."* Jurnal Legislasi Indonesia, 20(2).

Arrsa, Ria Casmi. (2023*). "Digital Governance dan Tantangan Regulasi di Indonesia."* Jurnal RechtsVinding, 12(2).

Arum, Nenden Sekar. (2023). *"Klasifikasi Informasi dan Perlindungan Data dalam Tata Kelola Pemerintahan Digital."* Jurnal RechtsVinding, 12(2).

Asshiddiqie, Jimly. (2021). *Pengantar Ilmu Hukum Tata Negara*. Jakarta: Rajawali Pers.

Atmadja, I Dewa Gede, & Budiartha, I Nyoman Putu. (2018). *Teori-Teori Hukum*. Malang: Setara Press.

Chan, David Y., & Vasarhelyi, Miklos A. (2022). "*Innovation and Practice of Continuous Auditing."* International Journal of Accounting Information Systems, 25.

Chan, David Y., & Vasarhelyi, Miklos A. (2022). *Innovation and Practice of Continuous Auditing*. London: Routledge.

Clarke, Richard A., & Knake, Robert K. (2019). *Cyber War: The Next Threat to National Security and What to Do About It.* New York: HarperCollins.

European Commission. (2019). *Ethics Guidelines for Trustworthy Artificial Intelligence*. Brussels: European Commission.

Friedman, Lawrence M. (2009). *The Legal System: A Social Science Perspective*. New York: Russell Sage Foundation.

Gupta, Sunil. (2020). *Driving Digital Strategy: A Guide to Reimagining Your Business*. Boston: Harvard Business Review Press.

Indrajit, Richardus Eko. (2021). *Electronic Government: Konsep dan Strategi Pelayanan Publik Berbasis Teknologi Digital*. Yogyakarta: Andi.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems Requirements. Geneva: ISO.

ISACA. (2021). Information Systems Auditing: Tools and Techniques Creating Audit Programs. Illinois: ISACA Press.

Mahmudi. (2021). *Manajemen Keuangan Daerah*. Yogyakarta: UPP STIM YKPN.

Mardiasmo. (2021*). Akuntansi Sektor Publik*. Yogyakarta: Andi.

Mulyadi, Lilik. (2021). *Pengawasan dan Pemeriksaan Keuangan Negara*. Bandung: Citra Aditya Bakti.

Nurdin, Ismail. (2022). *Sistem Informasi Manajemen Pemerintahan Digital*. Jakarta: Kencana.

Pasquale, Frank. (2015). *The Black Box Society: The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Schneier, Bruce. (2015). *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons.

Soponyono, Eko. (2023). *"Perlindungan Data dan Tata Kelola Pemerintahan Digital di Indonesia."* Jurnal Media Hukum, 30(1).

Stallings, William. (2019). *Effective Cybersecurity: A Guide to Using Best Practices and Standards.* Boston: Pearson.

Sutedi, Adrian. (2022*). Hukum Keuangan Negara*. Jakarta: Sinar Grafika.

Sutiyoso, Bambang. (2024). *"Pertanggungjawaban Hukum dalam Pemanfaatan Kecerdasan Buatan di Sektor Publik."* Jurnal Hukum Ius Quia Iustum, 31(1).

Vasarhelyi, Miklos A., Kogan, Alexander, & Tuttle, Brad. (2015). "*Big Data in Accounting: An Overview."* Accounting Horizons, 29(2).

Wendel, W. Bradley. (2022). *The Rule of Law and the Accountability of Artificial Intelligence*. Cambridge: Cambridge University Press.

Yusuf, M. (2020). *Hukum Pemeriksaan Keuangan Negara di Indonesia*. Jakarta: Prenadamedia Group.

Republik Indonesia. (2003). Undang-Undang Nomor 17 Tahun 2003 tentang Keuangan Negara. Lembaran Negara Republik Indonesia Tahun 2003 Nomor 47.

Republik Indonesia. (2004). Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara. Lembaran Negara Republik Indonesia Tahun 2004 Nomor 5.

Republik Indonesia. (2004). Undang-Undang Nomor 15 Tahun 2004 tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara. Lembaran Negara Republik Indonesia Tahun 2004 Nomor 66.

Republik Indonesia. (2008). Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik. Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61.

Republik Indonesia. (2018). Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182.

Republik Indonesia. (2019). Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185.

Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196.