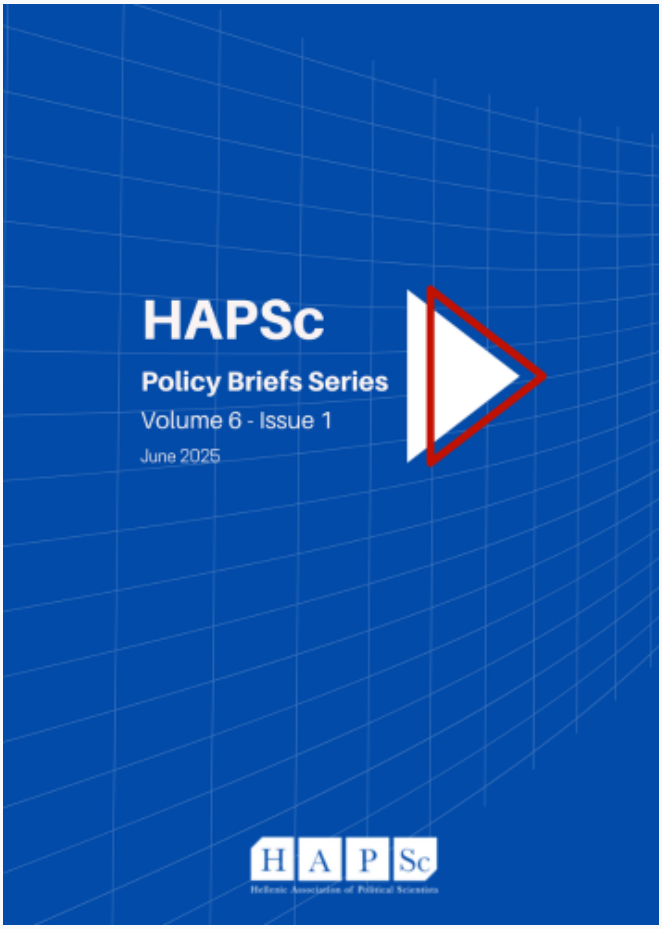
HAPSc Policy Briefs Series

Vol 6, No 1 (2025)

HAPSc Policy Briefs Series



Fraud Risks and Corruption in Public Organizations: Rethinking Governance through Fintech

Evangelia Pappa, Panagiotis Georgitseas, Georgios Tantis, George Georgiou

doi: 10.12681/hapscpbs.43148

To cite this article:

Pappa, E., Georgitseas, P., Tantis, G., & Georgiou, G. (2025). Fraud Risks and Corruption in Public Organizations: Rethinking Governance through Fintech. *HAPSc Policy Briefs Series*, *6*(1), 8–16. https://doi.org/10.12681/hapscpbs.43148

Fraud Risks and Corruption in Public Organizations: Rethinking Governance through Fintech[1]

Evangelia Pappa[2], Panagiotis Georgitseas[3], Georgios Tantis[4] & George Georgiou[5]

Abstract

Good governance in public organizations ensures efficiency, transparency, accountability, and public trust. In today's complex and rapidly evolving environment, public sector institutions face a growing range of risks and challenges that threaten the achievement of their objectives and the protection of the public interest. The implementation of effective control mechanisms is critical for identifying both internal and external risks and responding to emerging governance threats. Under this context, the integration of digital technologies - particularly Financial Technology (Fintech) and Blockchain - has emerged as a promising strategy to enhance transparency, reduce fraud, and improve operational efficiency. However, their adoption also presents new risks related to data protection, algorithmic opacity, legal framework and regulatory uncertainty. This paper examines both the potential and limitations of these technologies, highlighting the governance conditions necessary for their effective implementation. It argues that digital innovation alone is insufficient, and that sustainable improvements require integration into broader institutional frameworks grounded in ethics, legal safeguards, accountability, and civic participation.

Keywords: Governance, Public Sector, Fraud and Corruption, Fintech, Blockchain, Digital Transformation, Regulation.

JEL Classification: H83, M48, M42, G32, G38, D73, G18.

Introduction

Public sector governance plays a fundamental role in ensuring trust and efficiency in democratic societies. Governance refers to the way an organization makes and implements decisions, and the procedures through which it directs its activities, ensures oversight, and maintains accountability (IIA, 2012: 9). In the public sector, governance focuses on how available resources are managed to achieve strategic objectives. The transformation of public resources into measurable outcomes must be carried out in a manner that ensures institutional credibility, equitable service delivery, and the integrity and ethical behavior of public officials (IIA, 2017: 4).

Although public sector entities may differ in structure, size, budget, and the nature of services provided, the principles governing their administration are largely uniform and horizontally

[1] To cite this paper in APA style: Pappa, E., Georgitseas, P., Tantis, G., & Georgiou, G. (2025). Fraud Risks and Corruption in Public Organizations: Rethinking Governance through Fintech. *HAPSc Policy Briefs Series, 6*(1), 8-16. https://doi.org/10.12681/hapscpbs.43148
[2] Hellenic Open University, Greece & Open University of Cyprus.
[3] Panteion University of Social and Political Sciences, Greece.
[4] Panteion University of Social and Political Sciences, Greece.
[5] Ministry of National Economy and Finance, CGAP, CFE, CICA, CCS, Accredited on Audit Quality, Greece.

applicable. These principles include: (a) the formulation of policies aligned with national strategies and embedded in the organization's strategic and operational planning; (b) the promotion of ethical standards and the establishment of clear lines of accountability; (c) the oversight of outcomes to ensure that public sector activities comply with legal and institutional frameworks; and (d) the correction of errors and failures through appropriate remedial actions and interventions (Goodson, Morey & Lapointe, 2012).

The aim of this article is to explore the evolving risks of fraud and corruption in public sector governance and to examine how emerging digital technologies—specifically Financial Technology (Fintech) and Blockchain—can serve as tools for strengthening transparency, accountability, and institutional resilience. By analyzing key governance challenges and presenting international case studies, the article seeks to provide a multidimensional understanding of the conditions under which these technologies can be effectively integrated into public administration. Ultimately, the goal is to highlight both the opportunities and limitations of technological innovation in combating systemic vulnerabilities and to propose a framework for more responsive and ethical governance.

The remaining of the paper is as follows: Section 2 analyzes fraud risks and corruption and the next section describes the challenges of governance in the public sector. Section 4 presents the technological challenges and opportunities with special emphasis on Fintech and Blockchain in public sector governance and Section 5 provides risk management framework under the COSO model. The last Section offers the concluding remarks.

Fraud Risks and Corruption

One of the most pressing issues in the governance of organizations today is the identification, assessment, management, and monitoring of risks. A risk is defined as the probability of an adverse event occurring—an incident or situation that may negatively affect the organization's ability to achieve its objectives, potentially causing direct or indirect losses. Two core attributes of risk are uncertainty and exposure (Cendrowski & Mair, 2009: 9).

The recent global report Risk in Focus 2024 identifies the most critical risks currently affecting the private sector and challenging especially internal auditors. These include cyberattacks and information security threats, difficulties in attracting and retaining talent, geopolitical instability, frequent changes in legal and regulatory frameworks, and problems associated with digital transformation and emerging technologies. Additional concerns include crisis management and business continuity, financial liquidity constraints, disruptions in supply chains, and third-party

risks—all of which demand increasing attention and effort from internal control units (Risk in Focus, 2024: 9).

Many of these risks are equally relevant to public sector organizations. According to the Global Risk Management Survey 2023, the top-ranked risk—moving up in significance from the 2021 edition—is cyber risk, including data breaches and attacks amid growing geopolitical instability. Other key concerns include reputational damage, failure to attract or retain top talent, regulatory and legislative volatility, financial instability, and cash flow or liquidity challenges (Global Risk Management Survey, 2023).

Governance Challenges in the Public Sector

In the public sector, the volatility and complexity of risks—cutting across all levels of governance—make effective risk management a critical necessity. Through a structured framework, targeted policy, and methodical approach, combined with the establishment of appropriate governance mechanisms, organizations can address a range of emerging challenges (NAO, 2023: 4), including:

- Understanding the trade-offs between short-term efficiency and long-term resilience, ensuring that gains in one area do not unintentionally increase risks or costs in another;
- Developing institutional capacity and expertise, and improving the quality and qualifications of public sector personnel;
- Adapting to the requirements of digital transformation;
- Modernizing public services and eliminating unnecessary bureaucratic procedures;
- Taking measures to address the impacts of climate change;
- Strengthening mechanisms for the prevention and suppression of corruption and fraud, especially as such phenomena tend to intensify under adverse economic and social conditions.

Technological Challenges and Opportunities: Fintech and Blockchain in Public Sector Governance

Emerging technologies such as Financial Technology (Fintech) and Blockchain are redefining the contours of public sector governance, especially in the areas of fraud prevention, transparency, and accountability (Pappa et al., 2024). These innovations are frequently promoted as tools for modernizing state institutions and addressing corruption vulnerabilities. However, their deployment presents new governance challenges, especially where institutional capacity and regulatory oversight remain weak or fragmented (Pappa et al., 2023).

On one hand, Fintech solutions provide significant opportunities for increasing efficiency and reducing corruption through automation, digital identity verification, and direct benefit transfers. A notable example is the implementation of digital wallets for distributing social welfare benefits, as seen in India's Aadhaar system, which leveraged biometric authentication and Fintech tools to significantly reduce fraud and leakage of funds (World Bank, 2016). Similarly, in countries like Kenya and Nigeria, mobile-based financial services like M-Pesa have been used to disburse government subsidies and monitor spending with improved traceability (Arner, Barberis & Buckley, 2016; Daskalakis, Georgitseas, 2023).

On the other hand, Blockchain technology introduces the possibility of decentralized and tamper-resistant record-keeping, which can significantly reduce administrative opacity (Daskalakis & Georgitseas, 2020). In Georgia, for instance, the government adopted blockchain-based land registry systems in collaboration with the private sector to combat corruption and fraudulent transactions related to property rights (Aarvik, 2022). Similar experimentation occurred in Chile, where blockchain was tested in public procurement to prevent manipulation and promote trust in public contracting processes (OECD, 2020). Other pilot programs have explored the use of blockchain in procurement systems, public budgeting, and digital voting to reduce opportunities for manipulation (OECD, 2020). Estonia represents another advanced case, showcasing a fully integrated e-governance model that uses blockchain infrastructure for managing digital identity, health records, voting systems, and legal archives. It demonstrates how strategic investments in digital infrastructure can lead to sustained transparency and citizen trust (Tapscott & Tapscott, 2016).

Table 1: Use cases of Technology in Public Governance

Country	Technology	Use Case	Objective	Outcome / Notes
India	Fintech + Biometric ID (Aadhaar)	Social welfare distribution	Eliminate fraud and fake beneficiaries	40%+ reduction in ghost recipients; concerns raised about data protection
Georgia	Blockchain	Land/property registry	Increase transparency and reduce forgery	Became a global model; successful anti-corruption pilot
Estonia	Blockchain + e-Gov	Digital identity and public registries	Full digital governance and transparency	Regarded as the world leader in e-governance infrastructure.
Chile	Blockchain	Public procurement	Mitigate favoritism and political corruption	Trialled successfully; limited but promising reach

Nigeria	Fintech	COVID-19 relief payments	Track spending and reduce leakages	Improved oversight, but weak regulatory monitoring remains a challenge

Source: Authors' collaboration.

Despite these promising use cases, as reported in Table 1, both Fintech and blockchain present serious governance and implementation challenges. Poorly regulated Fintech platforms can become channels for misuse, such as identity fraud or data leaks, especially in contexts where digital rights protections are weak. While blockchain is often assumed to be secure by design, vulnerabilities in smart contract code or in governance structures surrounding its use can still result in breaches or manipulation (OECD, 2020; Pappa et al., 2023).

To successfully integrate these technologies, public sector organizations must address several key areas:

- Develop technology-specific risk assessment frameworks
- Build interoperable and secure infrastructures
- Enhance digital skills and capacity among civil servants
- Establish clear ethical standards and transparency guidelines for AI, blockchain, and automated decision-making tools

Moreover, the adoption of these technologies requires significant institutional readiness, including:

- The establishment of regulatory sandboxes to test innovation under supervised conditions,
- The development of risk-based auditing tools that can analyze blockchain transactions,
- The integration of ethics-by-design principles in algorithmic governance, and
- The upskilling of civil servants in digital literacy, cybersecurity, and tech policy (OECD, 2020; UNODC, 2021).

In many cases, technological "solutionism" - the assumption that technology alone can resolve governance failures - can obscure deeper issues such as lack of political will, entrenched clientelism, or weak legal frameworks. Thus, technological tools must be embedded in a broader institutional reform agenda that includes transparency laws, whistleblower protections, citizen participation, and independent oversight mechanisms.

In conclusion, Fintech and blockchain technologies can serve as catalysts for integrity and reform in public governance. However, without comprehensive risk governance frameworks, inclusive design, and regulatory foresight, these same technologies can exacerbate existing inequalities and create new forms of fraud, opacity, and exclusion.

Risk Management in the Governance of Public Organisations

In the 1950s, internal and external auditors recognised the need for strong controls to address risks (Moeller, 2011: xi). It was not until the early 1990s that the COSO (Committee of Sponsoring Organizations of the Treadway Commission) issued the COSO Internal Control System Framework which provided a widely accepted definition of an internal control system and control safeguards, enabling private sector organizations to effectively manage and supervise their environment. In May 2013, the updated Framework (Figure 1) was issued, which continues to be based on five pillars, but introduces seventeen principles and is now widely applicable to public organisations.

Figure 1: COSO Framework

Source: COSO (2013:6).

The COSO framework is presented as a three-dimensional cube with distinct but overlapping categories of objectives that allow organizations to focus on different aspects of controls. First, operational/functional objectives relate to the effectiveness and efficiency of the entity's operations, with a focus on operational and financial performance and safeguarding of assets. Second, reporting objectives relate to the results of operations and the reliability of reporting, and include internal and external reporting as well as financial and non-financial reporting. Third, compliance objectives relate to adherence to laws and regulations. The COSO framework applies to the entire organization as well as to each division, department, and function (COSO, 2013).

The building blocks of the COSO Framework are the Control Environment, the foundation of the construct, with the key principles of demonstrating commitment to integrity and ethical values, oversight of the Internal Control System, defining structures, authorities and responsibilities, demonstrating commitment to competencies and implementing accountability, describing a culture of risk awareness. It communicates the 'tone at the top'. Risk Assessment identifies appropriate objectives, identifies and analyses risks, assesses fraud/corruption risks and identifies and analyses

significant changes. The organisation must be able to identify new risks as they emerge and change the significance of risks already identified.

In the Control Processes pillar, control processes are selected and developed at all levels of the hierarchy, ICT control networks and specific policies and procedures are implemented in order to limit the organization's exposure to risk. In Information & Communication, quality and adequate information is used and carried out within and outside the organisation so that the parties involved are aware of the risks and the problems they pose, adopt measures to address them and make the best possible decisions. Finally, in the Monitoring & Supervision pillar, the principle of continuous and targeted evaluation is adopted, as well as the assessment and communication of the deficiencies of the Internal Control System (Koutoupis and Pappa, 2018; COSO, 2013).

Highlighting the weaknesses of the internal control system is one of the main missions of internal and external audit. Through independent and objective assessment, auditors identify weaknesses and gaps that may increase the risk of financial losses, corruption or inefficient management of resources. According to Rezaee and Riley (2019), the audit process helps improve decision-making by providing managers with critical information on potential risks and the actions needed to mitigate them.

In addition, auditing enhances transparency and accountability, elements that are crucial for trust in the governance of the Agencies. Power (2004) argues that auditing allows citizens and stakeholders to have confidence in financial management and efficient allocation of resources. In addition, public organisations are often required to incorporate audit findings into their risk management practices, reducing the operational and strategic risks that may arise. Organizations that undergo regular external audits improve their practices and reduce the likelihood of risks occurring (Arwinge, 2013). Auditing, therefore, acts as a mechanism to prevent, identify and reduce risks, contributing to the overall improvement in the efficiency of public organizations.

Finally, we note that as audits include performance elements, the stronger their contribution to risk management, since performance audits examine the causes and pathologies as well as the impact of risks, in order to eliminate or reduce them with the necessary corrective actions (Georgiou and Bousios, 2021).

Conclusion

The governance of public organizations faces increasingly complex risks that demand comprehensive and forward-looking management strategies. This paper has highlighted the evolving nature of fraud and corruption risks in both private and public sector, along with the institutional and operational challenges that hinder effective prevention and response. The integration of innovative technologies

such as Fintech and Blockchain holds great promise for enhancing transparency, reducing bureaucratic inefficiencies, and mitigating fraud. However, their successful application depends not only on technical capacity but also on regulatory foresight, rules and guidelines designed to ensure compliance, ethical design, and institutional readiness.

Strengthening public sector governance requires a holistic approach—one that combines internal and external control mechanisms, invests in digital infrastructure and human capital, and aligns technological innovation with accountability, legal safeguards, and citizen trust. As digital transformation continues to reshape public administration, governments must remain vigilant to ensure that efficiency does not come at the expense of resilience, equity, or democratic integrity.

References

Aarvik, P. (2022). Anti-corruption reforms have been successful in Georgia, but blockchain is stealing the limelight. U4 Anti-Corruption Resource Centre. Available at: https://www.u4.no/blog/anti-corruption-reforms-successful-in-georgia-blockchain-stealing-limelight (Accessed: 14/05/2025).

AON (2023). *Global Risk Management Survey*, 9th edition.

Arner, D. W., Barberis, J., & Buckley, R. P. (2016). The evolution of fintech: A new post-crisis paradigm? *Georgetown Journal of International Law*, 47, 1271–1319.

Arwinge O. (2013). *Internal control: A study of concepts and themes*. Springer Science & Business Media.

Cendrowski, H., & Mair, W. C. (2009). *Enterprise risk management and COSO: A guide for directors, executives and practitioners*. John Wiley & Sons.

Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2013). *Internal Control – Integrated Framework, Executive Summary, Framework and Appendices, Illustrative Tools for Assessing Effectiveness of a System of Internal Control.* Jersey City: Committee of Sponsoring Organizations of the Treadway Commission.

COSO (2013). Internal Control Self-Assessment Checklist, Guidance on Internal Control-Integrated Framework (2013), Committee of Sponsoring Organizations of the Treadway Commission.

Daskalakis N., Georgitseas P. (2023). *Fintech and Cryptoeconomy*. Athens: Propobos Publications (In Greek).

Daskalakis, N., & Georgitseas, P. (2020). *An introduction to cryptocurrencies: the crypto market ecosystem*. London: Routledge.

ECIIA (2024). Risk in Focus. Hot topic for internal auditors.

ECIIA/FERMA (2013) Guidance on the 8th EU Company Low Directive, article 41, IIA Position Paper, The Three Lines of Defense in effective Risk Management and Control.

Georgiou, G. and Bousios, T. (2021). *Performance Audits*. Athens: Papazisis Publications (in Greek).

Goodson, S., Morey, K. & Lapointe, J. (2012). *Supplemental Guidance: The role of Internal Auditing in the Public Sector Governance*. Altamore Springs, Florida: The Institute of Internal Auditors, Global.

Koutoupis, A. G., & Pappa, E. (2018). Corporate governance and internal controls: a case study from Greece. *Journal of governance & regulation*, 7 (2), 91-99.

Moeller, R. R. (2011). *COSO enterprise risk management: establishing effective governance, risk, and compliance processes*. John Wiley & Sons.

National Audit Office (NAO) (2023). Overcoming challenges to managing risks in government.

OECD (2020). The impact of blockchain technology on finance: A catalyst for change. OECD Blockchain Policy Series.

Pappa, E., Georgitseas, P., & Tantis, G. (2023). Exploring the Role of Blockchain Technology in Anti-Money Laundering. *J. Legal Ethical & Regul. Isses*, 27, 1.

Pappa, E., Georgitseas, P., Tantis, G., & Kyriakogkonas, P. (2024). Audit ESG Reports through Blockchain Technology in Business Enterprises. Chapter 6 in the Book: *Business, Management and Economics: Research Progress* (5), 90–107.

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. Demos.

Rezaee, Z. & Riley, R. (2019). *Financial statement fraud: Prevention and detection*. John Wiley & Sons.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world.* London: Penguin.

The Institute of Internal Auditors (2012). Supplemental Guidance: Public Sector Definition and The Role of Auditing in Public Sector Governance, 2nd edition.

The Institute of Internal Auditors (2017). International Standards for the Professional Practice of Internal Auditing (Standards).

UNODC (2021). ICT as a Tool for Citizen Participation in Anti-Corruption Efforts. United Nations Office on Drugs and Crime.

World Bank (2016). *World development report 2016: Digital dividends*. Washington, DC: World Bank Group.