Journal of
Information System and Technology Auditing

Research Paper

Risk Management within the Governance Framework of Digital Trust Ecosystems[1,2]

Rahi Zandifar[3]

Journal of Information System and Technology Auditing
Iranian Information Technology Audit Scientific Association
Vol. 1, No. 1, Spring & Summer 2025
pp. 18-25

Received: 2025.02.17
Revised: 2025.08.09
Accepted: 2025.09.02

1. Introduction

In the digital economy, organizational success depends on establishing trustworthy relationships and interactions. Digital trust plays a crucial role in enabling resilient and sustainable digital ecosystems, ensuring secure and transparent engagements among stakeholders. This research explores the digital trust ecosystem and introduces a governance framework that integrates risk management as a key trust factor.

Traditional human trust is built through honesty, consistency, and mutual understanding, but in digital environments, it relies on system transparency, cybersecurity measures, and regulatory compliance. Digital trust ensures confidence in the reliability and integrity of digital platforms, transactions, and services. The rise of Industry 4.0 and the transition toward Industry 5.0 have further emphasized its importance, as emerging technologies like artificial intelligence (AI), blockchain, and the Internet of Things (IoT) reshape business operations.

A key distinction exists between digital trust and digital security. While digital security focuses on encryption, authentication, and

---

[1] https://doi.org/10.22034/JISTA. 2025.506948.1017
[2] Selected Paper of 2nd Congress of IT Audit and Digital Trust
[3] PhD Student, Department of Management and Economics, Tarbiat Modares University, Tehran, Iran. Email: zandifar.rahi@modares.ac.ir

access controls, digital trust extends beyond technical measures to include ethical governance and responsible data practices. Additionally, the “zero trust” model, which follows the principle of "trust nothing, verify everything," strengthens security by eliminating implicit trust. However, digital trust complements zero trust by ensuring a balance between security, usability, and ethical compliance.

Given these complexities, this research adopts the Digital Trust Ecosystem Framework (DTEF) to provide a structured governance model. DTEF is a hierarchical framework that incorporates risk management within its Direct and Monitor domain, bridging organizational strategy with process implementation.

2. MATERIALS AND METHODS

This research is applied in nature and focuses on the practical development of knowledge in the field of digital trust ecosystems through a phenomenological approach. The phenomenological method seeks to understand the experiences and perceptions of various actors when interacting with a specific phenomenon. In this study, data were collected from an extensive review of online resources, scholarly articles, and indirect expert interviews by analyzing video content and comparing practitioners’ experiences with established digital trust frameworks to extract key patterns within digital ecosystems.

The selection of the Digital Trust Ecosystem Framework (DTEF) as the core governance model emerged from a phenomenological process that involved iterative exploration of expert perspectives, industry practices, and regulatory considerations. In the initial stage, to conceptualize the emerging idea of digital trust ecosystems, up-to-date literature and indirect experiential inputs from international specialists—obtained via professional networks and platforms such as YouTube—were systematically reviewed. For example, a targeted search for the term “digital trust ecosystem” on YouTube yielded 259 videos. Assuming that search algorithms prioritize relevance, the top 100 results were analyzed: 67% were directly related to digital trust ecosystems, 27% addressed digital trust in general, and the remainder were unrelated. Notably, 28% of the

ecosystem-related content referred to the DTEF framework, underscoring its significance within phenomenological analysis. Other results focused on domain-specific frameworks such as Hyperledger or proprietary blockchain architectures, which lack broad applicability across industries.

The practical insights gathered from specialists, organizations, and researchers indicated that DTEF not only encompasses all critical components of digital ecosystems but also offers a flexible and adaptable model for managing trust and risks at multiple levels. In the subsequent stage, the selection of an appropriate risk management model for the fourth layer of the DTEF hierarchy was also guided by phenomenological analysis. A comparative review of practical implementations revealed that the ISO/IEC 27005:2022 standard is the most relevant and widely adopted in the context of digital trust, given its compatibility with information security structures. This standard follows a systematic process comprising context establishment, risk assessment, and risk treatment. Risk assessment itself includes risk identification, risk analysis, and risk evaluation. Two additional cross-cutting activities—communication and consultation, and monitoring and review—affect all stages of the risk management process.

The DTEF itself consists of six hierarchical layers: (1) nodes (people, processes, technology, and organization), (2) domains (culture, Emergence, human factors, direct and monitor, architecture, and enabling and support), (3) trust factors, (4) methods, (5) activities, and (6) outcomes. Within this structure, risk management is positioned as a trust factor in the “Direct and Monitor” domain, bridging organizational governance with operational processes. The framework is designed to be compatible with a broad range of governance and compliance models such as COBIT, ITIL, GDPR, ISO, and NIST, allowing for tailored adaptation to organizational needs. By situating ISO/IEC 27005-based risk management methods in the fourth layer (methods) and their corresponding activities in the fifth layer (activities), the research operationalizes the conceptual model into actionable governance mechanisms for digital ecosystems.

3. RESULTS AND DISCUSSION

The research findings highlight that integrating DTEF with ISO/IEC 27005 enhances risk management in digital ecosystems. The application of structured risk management practices in AI-driven banking yields three key outcomes. First, proactive risk management significantly reduces cybersecurity incidents, unauthorized access, and fraud-related activities. By systematically identifying vulnerabilities and addressing threats, organizations enhance system resilience. Second, transparent governance and well-defined risk management policies foster greater stakeholder confidence. Customers, regulators, and business partners trust organizations that demonstrate clear accountability and effective security controls. Third, aligning risk management with ISO standards ensures compliance with data protection laws and financial regulations, reducing legal risks and improving regulatory oversight. Beyond risk management, the study reveals governance challenges in digital trust ecosystems. Traditional centralized trust models, where a dominant entity regulates trust mechanisms, are increasingly inadequate. While centralized structures offer clear oversight, they lack adaptability in dynamic digital environments. Decentralized governance models, by contrast, distribute trust management among multiple stakeholders, promoting transparency and fairness. However, they also introduce complexities such as aligning stakeholder interests, addressing cross-border regulatory inconsistencies, and overcoming organizational inertia.

To navigate these challenges, organizations must integrate governance frameworks effectively. DTEF facilitates structured governance by offering adaptable metrics and controls, which, when combined with COBIT (a detailed IT governance framework), bridge the gap between strategic decision-making and operational implementation. The findings further suggest that digital trust ecosystems require a balanced approach between strict security measures and operational efficiency. Overly rigid controls may hinder innovation, while insufficient security exposes organizations to cyber threats and reputational damage. Adaptive governance models ensure both risk mitigation and business agility.

4. CONCLUSION

This research underscores that digital trust extends beyond technical security, incorporating ethical, cultural, and organizational elements that determine the reliability of digital interactions. The Digital Trust Ecosystem Framework (DTEF) provides a structured approach to integrating digital trust into governance, ensuring security and operational integrity. Organizations that adopt comprehensive governance models create a foundation for transparent, secure, and resilient digital interactions, fostering long-term stakeholder confidence.

The study demonstrates that leveraging DTEF alongside risk management standards such as ISO/IEC 27005 strengthens cybersecurity while maintaining usability. Structured risk management practices help balance protection with accessibility. Aligning risk management with international standards enhances regulatory compliance, ensuring that organizations meet legal and industry requirements. Additionally, ethical and transparent governance structures reinforce long-term digital trust by establishing clear accountability and responsible data management practices.

The findings highlight the dynamic interplay between cybersecurity, decentralized governance, and digital trust. As businesses increasingly rely on AI, blockchain, and IoT, adopting comprehensive governance models becomes critical. The integration of digital trust frameworks with risk management strategies enhances competitive advantage, customer loyalty, and the long-term sustainability of digital ecosystems. Organizations that effectively implement these frameworks strengthen resilience against emerging threats while remaining adaptable in evolving digital landscapes.

Future research should expand DTEF applications across industries, develop quantitative trust metrics, and refine decentralized governance mechanisms. Further exploration is needed to understand how evolving regulations impact digital trust strategies, particularly in cross-border digital transactions. Addressing these areas will help organizations enhance their resilience in the digital era, enabling them to build sustainable and

secure digital ecosystems where trust remains a fundamental pillar of innovation and transformation.

Keywords: Digital Trust; Digital Ecosystem; Risk Management; Ecosystem Governance; Direct and Monitor; Digital Trust Ecosystem Framework.

JEL classification: *M15, G34, D81.*

References

Abdelsalam, O; Chantziaras, A; Joseph N. L; & Tsileponis, N. (2024). Trust matters: A global perspective on the influence of trust on bank market risk. *Journal of International Financial Markets, Institutions and Money*, *92*, 101959.

Aguiar, M; Kiderman, J; Shekar, H. C; & Schilke, O. (2023). Safeguarding trust in a digital ecosystem. *Journal of Business Strategy*, (ahead-of-print).

Baker-Brunnbauer, J. (2021). TAII framework for trustworthy AI systems. ROBONOMICS*: The Journal of the Automated Economy*, *2*, 17.

Balan, A; Tan, A. G; Kourtit, K; & Nijkamp, P. (2023). Data-Driven Intelligent Platforms—Design of Self-Sovereign Data Trust Systems. *Land*, *12*(6), 1224.

Chang, W. (2024). The Impact of Trust on Digital Banking Services. *Americas Conference on Information Systems (AMCIS) 2024, Proceedings*. 1.

Chatterjee, J; Damle M; & Aslekar, A. (2023). Digital Trust in Industry 4.0 & 5.0: Impact of Frauds. In *2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 922-928). IEEE.

Digitalswitzerland. (2022). Building a Swiss Digital Trust Ecosystem, Discussion Input.

Firdaus, F; & Tobing, A. N. (2022). The Digital Ecosystem Risk in Digital Banking: a Case Study. *Risk Governance & Control: Financial Markets & Institutions*, *12*(4).

Gupta, V; & Shukla, S. (2024). Consumer Trust in Digital Banking: A Qualitative Study of Legal and Regulatory Impacts. *Interdisciplinary Studies in Society, Law, and Politics*, *3*(2), 18-24.

Hazam, G. (2023). Extending Zero Trust to the End User Ecosystem, *ISACA Journal*, Issues 2023, vol. 1.

Herzog, C; Blank, S; & Stahl, B. C. (2024). Towards trustworthy medical AI ecosystems–a proposal for supporting responsible innovation practices in AI-based medical innovation. *AI & SOCIETY*, 1-21.

ISACA. (2024). Using the Digital Trust Ecosystem Framework to Achieve Trustworthy AI. White Paper.

ISO/IEC 27005:2022. (2022). Information security, cybersecurity and privacy protection: Guidance on managing information security risks, Publication date : 2022-10.

Javan Amani, V; & Akbari, H. (2022). The Effect of Quality of Banking Services on Customer Satisfaction using SERVQUAL Model (Case study: Maskan Bank Branches in Tehran). *Journal of Islamic Economicis & Banking*, 11 (40). (In Persian)

Kaya, F. (2025). Decentralized Governance Design: A Model-Based Approach. *PhD-Thesis - Research and graduation internal*, Vrije Universiteit Amsterdam.

Khashei Varnamkhasti, V; Ebrahimi, M; Khalil Nezhad, Sh; & Motahari Nezhad, F. (2024). Generative Mechanisms of Digital Banking Ecosystem Evolution, *Journal of Business Intelligence Management Studies*, 12(48), 33-81. (In Persian)

Khorsandi Shamir, H. (2024). Electronic banking services and customer loyalty: An analysis of the mediating role of trust in the branches of Ayandeh bank in Mashhad. *Novel Explorations in Computational Science and Behavioral Management*, 2(1), 23-41. (In Persian)

Kulova, M. R. (2020). Trust and Security in the Digital Economy. *In International Session on Factors of Regional Extensive Development* (FRED 2019) (pp. 271-274). Atlantis Press.

Malik , P. K. (2024). The Role of Digital Trust in Enhancing Cyber Security Resilience. *Transforming Industry using Digital Twin Technology* (pp. 59-67). Cham: Springer Nature Switzerland.

Pakdel, M; Haghighat Monfared, J; & Aligholi, M. (2024). Presenting a native model of factors affecting the formation of digital trust using a data-based approach and theory, *Development and Transformation Management Journal* , No. 56 (Spring 1403). (In Persian)

Reiners, S. (2022, June). Trust and its Extensions in Digital Platform Ecosystems: Key Concepts and Issues for Future Research. In *2022 IEEE 24th Conference on Business Informatics (CBI)* (Vol. 2, pp. 1-8). IEEE.

Roy, S. (2024). Understanding Zero-Trust vs. Digital Trust: Demystifying Cybersecurity Paradigms, *IDM Technologies*.

Rychkova, I; Zdravkovic, J; & Stirna, J. (2023). Implications of trust in digital business ecosystem design: A systematic analysis of roles. *PoEM Companion*.

Shahzad, K; & Shahid, H. (2022). Digital trust in business ecosystem collaboration: Leveraging digital technologies to develop a framework. *Trust, Digital Business and Technology: Issues and Challenges*, 242- 254. Routledge Studies in Trust Research. New York: Routledge.

Strazzullo, S. (2024). Fostering digital trust in manufacturing companies: Exploring the impact of industry 4.0 technologies. *Journal of Innovation & Knowledge*, 9(4), 100621.

Thomas, M; Witte, G; & Von Roessing, R. (2024). Digital Trust Ecosystem Framework a Valuable Complement to COBIT, Other Frameworks.

Yusof, A. M; Zaini, M. K; Khairuddin, I. E; & Uzir, N. A. (2024). Modeling a Digital Trust Framework to Address Cybersecurity Issues in Malaysia's Digital Economy, *International Transaction Journal of Engineering, Management, & Applied Sciences & Technologies*, 15(4), 15A4B, 1-12.

Zarepour Nasirabadi, E; & Ghamaripoor N. (2024). Investigating the relationship between the components affecting customer trust and satisfaction in mobile banking ecosystems. *Management Research in Iran*, 28(1), 131-154. (In Persian)