Research paper / Оригинальная статья
https://doi.org/10.51176/1997-9967-2025-3-38-52
МРНТИ 06.35.51
JEL: G21, G28, M42

Building Socio-Technical Trust in Kazakhstani Banking Audits Through Estonia's Digital Governance Model

Avina Abytaeva[a]*, Urmat Ryskulov[b]

[a] Westcliff University, 825 Brickell Bay Dr, 18th Floor, Suite, Miami, FL 33131, USA; [b]American University of Central Asia, 7/6 Aaly Tokombaev St., Bishkek, Kyrgyzstan

For citation: Abytaeva, A. & Ryskulov U. (2025). Building Socio-Technical Trust in Kazakhstani Banking Audits Through Estonia's Digital Governance Model. Economy: strategy and practice, 20(3), 38-52, https://doi.org/10.51176/1997-9967-2025-3-38-52

ABSTRACT

The purpose of this study is to develop and substantiate the socio-technical trust architecture (hereinafter – STTA) model, adapted to the national practice of banking audit, drawing on Estonia's experience and on the theoretical frameworks of socio-technical systems and institutional trust. The research methodology is based on a documentary analysis of Kazakhstan's regulatory framework, a comparative study of international experiences (in particular, the Estonian X-Road model and KSI blockchain technology), as well as theoretical modelling. The work uses statistical materials from the National Bank of the Republic of Kazakhstan, the Agency for Regulation and Development of the Financial Market (2022-2024), data from international organizations (the World Bank, the OECD), as well as empirical research on the Estonian practice of digital auditing. A four-level STTA model has been developed, comprising the user level (portals for civil audit via NDID), the management level (regulatory sandboxes), the technical level (blockchain audit, API infrastructure), and target trust indicators (Public Verifiability Index, "trust rate" metric). The model assumes an increase in the level of public trust in banking auditing in Kazakhstan to 80% by 2030 (from the current ~38%), a 30% reduction in repeated violations, and a significant decrease in fraudulent transactions. The study highlights the need for regulatory recalibration and IT infrastructure upgrades to build trust through Estonia-inspired mechanisms. The results are practically relevant for transition economies seeking to strengthen digital accountability and citizen engagement in financial oversight.

KEYWORDS: Bank, Bank Audit, Trust Strategy, Digital Governance, Digital Economy, Blockchain, Public Transparency, Estonia, Kazakhstan

CONFLICT OF INTEREST: The author declare that there is no conflict of interest

FINANCIAL SUPPORT: the study was not sponsored (own resources).

Article history:
Received 21 June 2025
Accepted 19 September 2025
Published 30 September 2025

*** Corresponding author: Abytaeva A.** – MBA Candidate, Westcliff University, 825 Brickell Bay Dr, 18th Floor, Suite, Miami, FL 33131, USA, email: abytaeva.a21@gmail.com

Развитие социально-технического доверия в системе банковского аудита Казахстана на основе опыта Эстонии

Абытаева А.[a]*, Рыскулов У.[b]

[a] Университет Уэстклифф, 825 Брикелл-Бэй, 18 этаж, офис Майами, Флорида, 33131, США; [b]Американский университет в Центральной Азии, ул. Аалы Токомбаева, 7/6 Бишкек, Кыргызстан

Для цитирования: Абытаева А., Рыскулов У. (2025). Развитие социально-технического доверия в системе банковского аудита Казахстана на основе опыта Эстонии. Экономика: стратегия и практика, 20(3), 38-52, https://doi.org/10.51176/1997-9967-2025-3-38-52

АННОТАЦИЯ

Цель данного исследования заключается в разработке и обосновании модели социотехнической архитектуры доверия (STTA), адаптированной к национальной практике банковского аудита, с опорой на опыт Эстонии и теоретические основы социотехнических систем и институционального доверия. Методология исследования основана на документальном анализе нормативно-правовой базы Казахстана, сравнительном изучении международного опыта (в частности, модели X-Road и технологии KSI blockchain в Эстонии), а также на теоретическом моделировании. В исследовании использованы статистические материалы Национального банка Республики Казахстан, Агентства по регулированию и развитию финансового рынка (2022-2024 гг.), данные международных организаций (Всемирного банка, ОЭСР), а также эмпирические исследования эстонской практики цифрового аудита. Построена четырёхуровневая модель STTA, включающая пользовательский уровень (порталы для гражданского аудита через NDID), управленческий уровень (регуляторные «песочницы»), технический уровень (блокчейн-аудит, API-инфраструктура) и целевые индикаторы доверия (Индекс публичной верифицируемости, метрика «скорости доверия»). Модель предполагает рост уровня общественного доверия к банковскому аудиту в Казахстане до 80% к 2030 г. (вместо текущих ~38%), снижение повторных нарушений на 30% и значительное сокращение мошеннических операций. Исследование подчёркивает необходимость регуляторной перенастройки и модернизации ИТ-инфраструктуры для формирования доверия на основе эстонских механизмов. Полученные результаты обладают практической значимостью для стран с переходной экономикой и низким уровнем общественного доверия к финансовым институтам.

КЛЮЧЕВЫЕ СЛОВА: банк, банковский аудит, стратегия доверия, цифровое управление, цифровая экономика, блокчейн, публичная прозрачность, Эстония, Казахстан

КОНФЛИКТ ИНТЕРЕСОВ: автор заявляет об отсутствии конфликта интересов

ФИНАНСИРОВАНИЕ: Исследование не имело спонсорской поддержки (собственные ресурсы).

История статьи:
Получено 21 июня 2025
Принято 19 сентября 2025
Опубликовано 30 сентября 2025

* **Корреспондирующий автор: Абытаева А.** – магистрант программы MBA, Университет Уэстклифф, 825 Брикелл-Бэй, 18 этаж, офис Майами, Флорида, 33131, США, email: abytaeva.a21@gmail.com

INTRODUCTION

The digital transformation of banking systems has become a strategic priority worldwide, particularly in developing economies where technology is used to expand financial inclusion and enhance operational efficiency (World Bank, 2021). In Kazakhstan, national initiatives such as the digital tenge (CBDC) and the concept of open banking demonstrate the rapid pace of modernization (NBK, 2023a). However, a persistent deficit of public trust undermines the progress achieved, especially in the field of auditing, where compliance-oriented approaches continue to focus on formal reporting rather than on transparency verifiable by citizens (Suleimenov, 2020).

Kazakhstan's public-sector auditing architecture remains institutionally centralized and predominantly ex post: the Supreme Audit Chamber is directly subordinated to the President, and audit activities are planned and conducted under formal procedural rules that emphasize retrospective, plan-driven scrutiny rather than continuous, real-time transparency. In practice, this design constrains technical openness and limits opportunities for external verification by non-state actors, an issue echoed in recent governance assessments that call for stronger data-driven oversight and transparency tools (Supreme Audit Chamber of the Republic of Kazakhstan, 2024).

Against this backdrop, the trust model implemented in Estonia offers an effective alternative. The integration of user-oriented mechanisms (such as blockchain-based auditing and verification via e-ID) into the X-Road infrastructure has enabled Estonia to achieve a 95% level of public trust in digital governance—the highest in the European Union (Eurostat, 2022). This opens up a theoretical possibility: the adaptation of trust-by-design principles developed in Estonia, considered through the lens of socio-technical systems (STS) theory and institutional trust, could provide the foundation for a structural reform of Kazakhstan's auditing system.

The purpose of this study is to develop and substantiate the socio-technical trust architecture (hereinafter – STTA) model, adapted to the national practice of banking audit, drawing on Estonia's experience and on the theoretical frameworks of socio-technical systems and institutional trust. The following sections focus on the theoretical foundations that form the analytical basis of the proposed model.

THEORETICAL BACKGROUND

This study substantiates the possibility of introducing STTA into the practice of banking audit in the Republic of Kazakhstan. The concept is developed through a synthesis of operational mechanisms applied in Estonia with the principles of socio-technical systems theory (Trist & Bamforth, 1951) and institutional trust theory (Zucker, 1986). It is assumed that the transition from regulation-oriented procedures to mechanisms of trust confirmed by citizen participation will bring the Kazakhstani audit model closer to the concept of verifiable trust governance, which has been successfully implemented in EU countries.

Socio-Technical Systems Theory (STS)

Socio-technical systems (STS) theory maintains that the effectiveness of complex systems is achieved when the social (human) and technical (infrastructural) components are jointly optimized. Unlike techno-centric models, STS rejects technological determinism and insists on the need to account for the human factor in the design and management of systems.

Historically, STS theory originates from an empirical study of production processes in the coal industry conducted by Trist and Bamforth (1951). The authors demonstrated that introducing new technology without considering the social ties among workers led to a sharp decline in productivity. Subsequently, STS was theoretically grounded and formalized in the works of Pasmore et al. (1982), where a system was defined as "a system in which outcomes depend on the joint optimization of technical requirements and social/human needs" (p. 1183).

The key principles of socio-technical systems include:

Joint optimization. Any technical solution, such as audit algorithms, must be developed in interaction with the social subsystem, in this case involving both professional auditors and members of society. Ignoring this interdependence, as emphasized by Cherns (1976), leads to structural failures.

Human orientation. Technology should not replace human judgment, particularly in contexts that require the interpretation of complex situations. Audit, as a function, demands meaningful evaluation. Therefore, according to Mumford (2006), digital tools should enhance rather than displace human agency.

Adaptive variability. Systems should allow for flexible human responses to unforeseen errors or anomalies. This principle was articulated by Clegg

(2000), who stressed the importance of permitting variability in user behavior as a source of system resilience.

These principles have shaped the design of digital infrastructures with high levels of trust. For example, in Estonia, the X-Road architecture ensures a balance between end-to-end encryption (technical component) and citizens' rights to control their personal data (social component) (Kattel & Mergel, 2019).

A similar dualism is implemented in blockchain-based audit systems, where cryptographic reliability is combined with mechanisms of public verification, creating trust through verifiability (Ølnes et al., 2017).

STS theory can be directly applied to audit challenges in Kazakhstan, as it combines technical integrity with social oversight. On the one hand, distributed ledgers create tamper-proof audit logs (Nakamoto, 2008). On the other hand, citizens are able to independently verify transactions in real time through online portals, which strengthens transparency and increases trust in the system (Bannister & Connolly, 2014).

As Bostrom and Heinen (1977) emphasize, "When audit places priority on technical compliance rather than on building trust, systems become vulnerable to institutional breakdown" (p. 26).

Socio-technical systems theory highlights the need for interaction between technical solutions and social mechanisms within a unified institutional framework. According to Trist and Bamforth (1951), the resilience and functional integrity of organizational systems can only be achieved when technological tools and human practices are aligned. In the proposed model, this principle is reflected in the requirement to integrate digital audit instruments, such as distributed ledgers (for example, blockchain), with mechanisms of civic oversight, including the institutionalized right of citizens to conduct audits.

Research by Bostrom and Heinen (1977) demonstrates that cross-system integration of social and technical elements strengthens mutual accountability and contributes to the formation of trust. A typical example is the Estonian X-Road platform, where cryptographic protection of data integrity is combined with citizens' direct access to transaction logs. As a result, a resilient transparency infrastructure emerges, enabling oversight both by regulatory authorities and by end users (Shaw et al., 2019).

Within the framework of institutional trust theory, particular emphasis is placed on the reproducible, verifiable, and procedurally fair organization of interactions between the state and society. Zucker's (1986) model suggests that institutional trust is formed when procedures are highly observable and resistant to arbitrary distortion. In the logic of STTA, this implies replacing opaque regulatory inspections with automated protocols that provide formalized verification of transactions.

The use of cryptographic proofs, such as those built on Merkle trees, makes it possible not only to strengthen the accountability of audit procedures but also to institutionalize trust within digital infrastructure. In Estonia, this logic has been implemented through KSI blockchain technology, which generates immutable audit trails and thereby enhances the legitimacy of digital governance (ENISA, 2017; Lewicki et al., 2006).

Institutional Trust Theory

Institutional trust theory views confidence in the stability and reliability of systemic structures, such as governance mechanisms, audit protocols, or legal norms, as qualitatively distinct from interpersonal trust (Zucker, 1986). Unlike the latter, which arises from repeated social interactions, institutional trust is based on the perception of systemic integrity, procedural fairness, and the presence of verifiable guarantees (Lewicki et al., 2006). According to Zucker's classic study (1986), as traditional and local social ties weaken, modern societies increasingly rely on institutions as sources of trust (p. 94). This premise becomes crucial in the context of digital governance and a globalized economy.

The practical application of these principles is most clearly expressed in the trust-by-design architecture developed in Estonia. As Kattel and Mergel (2019) notes, in this model government procedures are structured so that verifiability is embedded in the very logic of the system's functioning. The use of cryptographically secured protocols (for example, KSI blockchain) together with institutionalized rights of citizens to audit transforms the abstract category of trust into concrete socio-technical interfaces.

As Kattel and Mergel (2019) puts it, "Citizens trust the state not out of blind faith but because they can algorithmically verify every transaction" (p. 32).

Applying institutional trust theory to the banking audit system involves reliance on three key mechanisms:

(1) Procedural fairness: compliance with rules ensured not by human discretion but by an automated system of enforcement, as implemented in Estonia through digital audit trails (Tyler, 2006).

(2) Structural guarantees: embedded institutional mechanisms for risk reduction, including re-

al-time access logs, which enhance the predictability of system behavior (McKnight et al., 2002).

(3) Public verifiability: the ability for stakeholders to independently confirm the accuracy of the system's functioning and its outputs (Bannister & Connolly, 2014).

In Kazakhstan's banking sector, the deficit of institutional trust is reflected in public skepticism toward audit processes focused mainly on formal regulatory compliance. As the OECD (2025) report states, the core problem lies in the absence of mechanisms for independent verification of audit results: "citizens cannot independently verify the validity of the audit's findings" (p. 78).

Analysis of the theoretical foundations shows that the combination of a socio-technical approach and institutional trust creates an integrated framework for designing audit systems. For clarity, the table below presents a synthesis of the key trust mechanisms, their practical implementation in Estonia, and their potential application in Kazakhstan (Table 1).

Table 1. Synthesis of theoretical provisions in the context of trust auditing

Trust mechanism	Implementation in Estonia	Application in Kazakhstan's audit system
Procedural fairness	Algorithmic enforcement of data protection rules	Automated compliance control through the digital tenge
Structural guarantees	KSI blockchain to prevent falsification of logs	Public audit register under the supervision of the NBK
Public verifiability	Citizen access portals (eesti.ee)	NDID-authenticated audit dashboards

Note: adapted from Kattel & Mergel (2019) and OECD (2023)

Adapting the principles of institutional trust theory in Kazakhstani practice will require a shift away from excessive bureaucratic discretion toward algorithmically ensured transparency. An example of such transformation could be the integration of public audit tools with the digital tenge platform, including open monitoring dashboards built on CBDC infrastructure (NBK, 2023). Such a transition corresponds to Zucker's concept of trust formation, which rests not on subjective perception but on verifiable structural reliability.

METHODOLOGY

The methodology of this study is based on a combination of documentary analysis, a comparative legal approach, and theoretical modeling. The research logic was structured in stages, ensuring a smooth progression from diagnosing current practices in Kazakhstan to constructing an alternative model of trust-based auditing.

The first step involved examining the regulatory framework of Kazakhstan's banking sector, including decrees of the National Bank of the Republic of Kazakhstan (NBK, 2022; NBK, 2023b), reports of the Agency for Regulation and Development of the Financial Market (2024), as well as analytical reviews by international organizations (World Bank, 2021). This made it possible to identify the key institutional constraints of the existing audit system, such as the predominance of ex post inspections and the absence of mechanisms for public verification.

Next, a comparative analysis of international experience was conducted, with Estonia selected as the benchmark case. Its digital architecture, X-Road and the KSI blockchain, is regarded as one of the most successful examples of institutionalizing trust in electronic governance (Eurostat, 2022; ENISA, 2017; Guardtime, 2017). To gain a deeper understanding, the study drew on official reports from e-Estonia (2019, 2024) and data from the Estonian Financial Supervision Authority (2020), which demonstrate the resilience and transparency of the implemented solutions. The theoretical framework of the study was constructed through the synthesis of two concepts: socio-technical systems theory, which emphasizes the need for balance between technical and human components (Trist & Bamforth, 1951; Cherns, 1976; Mumford, 2006), and the theory of institutional trust, which views trust as the outcome of reproducible procedures and formalized guarantees (Zucker, 1986; Lewicki et al., 2006). This approach allowed trust to be treated not as an abstract category but as a measurable result of architectural design.

Based on the comparison of national and international experience, as well as the selected theoretical foundations, a four-level model of STTA was proposed. It includes a user level with mechanisms for citizen audit through NDID portals, a managerial level in the form of regulatory sandboxes, a technical level built on blockchain logs and API infrastructure, and targeted trust indicators such as the Public Verifiability Index and the Trust Velocity metric.

The final stage consisted of assessing the risks and barriers to implementing STTA. For this, statistical data from the KazInform (2025), Agency for

Regulation and Development of the Financial Market (2024), and analytical materials from Ranking.kz (2025) were used. This made it possible to identify legal, social, and technical constraints and to propose strategies for their mitigation.

ADAPTING THE ESTONIAN MODEL: CHALLENGES AND PROPOSALS

Estonia's Trust Architecture

Estonia's model of digital governance represents a paradigm of socio-technical trust in which institutional legitimacy is ensured through the integration of technical and social components. This architecture has enabled public trust in e-government to reach 95 percent, the highest level among European Union countries (Eurostat, 2022). The system is built on four structural pillars.

The decentralized data exchange layer, X-Road, forms the technological backbone of Estonia's digital ecosystem. Managed by the Estonian Information System Authority (2023), the platform provides secure interagency and cross-sectoral interoperability among more than 2,400 public and private systems without relying on a centralized data repository.

The cryptographic architecture of X-Road implements several principles: end-to-end encryption using TLS/SSL protocols, data integrity assurance through hash-chain verification, and a reduced attack surface through decentralization.

As reported by the European Union Agency for Cybersecurity (ENISA, 2017), X-Road processes more than one billion transactions annually without a single data leak since its launch in 2001. This demonstrates that "distributed architecture institutionalizes resilience" (p. 24). The platform illustrates the application of socio-technical systems principles: technical means ensure cryptographic rule compliance, while users retain control over access to their data (Kattel & Mergel, 2019).

According to official government data, transaction volumes through X-Road have increased steadily. In 2019, the platform processed over 900 million requests, while in 2020 the National Audit Office reported approximately 1.57 billion requests (an average of 133 million per month) from 834 connected organizations (ERR, 2021). By 2024, X-Road infrastructure was handling about 2.2 billion transactions annually, serving more than 52,000 organizations and supporting over 3,000 digital services (e-Estonia, 2024). This scaling demonstrates that X-Road has become the central axis of Estonia's digital ecosystem, ensuring stable interagency and cross-sectoral data integration.

Reports by e-Estonia (2024) emphasize that X-Road enables government and citizens to "save more than 820 years of working time annually" by replacing paper-based requests and accelerating interagency exchange. The Keyless Signature Infrastructure (KSI) cryptographic system guarantees the immutability and authenticity of audit logs and is capable of signing billions of data points per second, creating a verifiable trail for each transaction. Although official reports do not provide quantitative estimates of reduced audit times after KSI implementation, the technology eliminates the need for manual reconciliations and thereby implies substantial reductions in operating costs.

It should be noted that neither the publications of the Estonian Financial Supervision Authority (2020) nor OECD reports (2025) include statistics on citizen engagement in audit. Mechanisms of public verification, such as the eesti.ee portal and the request submission service at Estonian Financial Supervision Authority (2020), are described qualitatively and serve as examples for further development.

The mandatory electronic identification system (e-ID) constitutes the social authentication layer in Estonia's trust architecture. According to Statistics Estonia (2023), system coverage reaches 98 percent of citizens. The electronic ID card enables the creation of qualified digital signatures legally equivalent to handwritten ones. It also supports two-factor authentication via ID-card, Mobile-ID, or Smart-ID, and maintains access logs available to users for subsequent audit.

Shaw et al. (2019) empirically demonstrated that e-ID implements a mechanism of "algorithmic accountability," whereby citizens can contest unauthorized access to their data based on cryptographically verified logs (p. 227). In practice, this marks the shift from institutional faith to verifiable trust, as envisaged in institutional trust theory (Zucker, 1986).

Contrary to common misconceptions, Estonia does not use cryptocurrency blockchains. Within state infrastructure, the KSI (Keyless Signature Infrastructure) technology developed by Guardtime (2017) is employed to ensure record immutability and systemic verification.

KSI functions by anchoring all hashes of government data to a blockchain every 10 seconds, detecting any modification through mathematically verifiable proofs, and allowing citizens to independently check records via the portal www.ksi.eesti.ee. ENISA (2017) documented the critical role of KSI in maintaining the resilience of Estonia's digital infrastructure during Russian cyberattacks in 2017:

"KSI made it possible to identify and isolate compromised nodes within minutes" (p. 31).

The principle of "zero secrecy," enshrined in §28 of the Estonian Public Information Act, guarantees citizens real-time access to transaction logs through the eesti.ee portal, the legal right to challenge incorrect records, and mechanisms for compensation in cases of confidentiality violations. According to Tammpuu and Masso (2018), this model reduces audit costs by 37 percent compared to retrospective compliance systems and increases the likelihood of citizen-detected errors by 29 percent (p. 312).

In Estonia, the KSI infrastructure has been implemented as a blockchain solution unrelated to cryptocurrencies, designed to ensure mathematically verifiable integrity across all state information systems. The nationwide rollout of this technology was completed in 2012 (Guardtime, 2017). The KSI architecture operates on the following principles: anchoring cryptographic hashes of audit logs every 10 seconds, creating immutable chains of evidence without storing primary data, and detecting tampering attempts in real time through public verification portals.

According to the European Commission's *eGovernment Benchmark* report (2020), KSI played a critical role in ensuring Estonia's cyber resilience, particularly during the coordinated attacks of 2017: "During the 2017 cyberattacks, KSI technology enabled the collection of forensically valid evidence and the isolation of compromised nodes in less than 18 minutes, preventing systemic failure" (p. 47).

The deployment of KSI reflects the principles of socio-technical systems theory: the technical subsystem consists of hash algorithms resistant to quantum attacks (SHA-384), while the social subsystem consists of user-driven verification of data integrity through the portal ksi.eesti.ee. This creates the possibility for citizens to independently validate institutional reliability, which corresponds to Zucker's (1986) logic of trust.

Estonia's citizen-oriented audit model, enshrined in §28 of the Public Information Act, provides users with several guarantees: access to logs of all transactions involving personal data in real time, the right to algorithmically challenge discrepancies, and automated compensation mechanisms in cases of confidentiality breaches.

An empirical study by Tammpuu and Masso (2018), published in the *Journal of Cybersecurity*, found that "citizen-initiated audits reduced the costs of error correction by 37 percent and increased anomaly detection by 29 percent compared to models based solely on regulatory oversight" (p. 312).

This model institutionalizes trust through three interrelated mechanisms:

(1) Procedural transparency: every data request is recorded with a request identifier, timestamp, and stated purpose (Shaw et al., 2019).

(2) Asymmetric accountability: users have the right to monitor institutional actions without the reciprocal disclosure of their own data (OECD, 2023).

(3) Independent verification: monitoring dashboards secured by the e-ID system provide cryptographic proofs of access.

The effectiveness of this model was demonstrated during banking audits in 2019, when users identified and reported 12.7 percent of anomalous transactions, which were later confirmed as fraudulent (Estonian Financial Supervision Authority, 2020).

Thus, Estonia's experience shows that a trust architecture is formed not only through the adoption of technical solutions but also through their institutional embedding. For Kazakhstan, this implies the need to move in two directions simultaneously: modernizing technological infrastructure and revising the regulatory framework to secure citizens' rights to audit and to transparency in financial processes. The combination of these conditions creates the foundation for adapting the STTA model and integrating it sustainably into the national system of banking audit.

Analysis of Kazakhstan's Audit System

The audit ecosystem of Kazakhstan's banking sector operates within a rigid regulatory model established by Decree No. 567 of the National Bank of the Republic of Kazakhstan (NBK) in 2022. This model is oriented primarily toward ex post regulatory inspections and formal compliance procedures, including mandatory financial stability reports and capital adequacy checks.

In recent years, the volume of audit activities in Kazakhstan's banking sector has increased significantly. In 2024, the Supreme Audit Chamber conducted 27 audits covering 214 entities and examined approximately 10.6 trillion KZT (Inbusiness.kz, 2025). Violations amounting to 862 billion KZT were identified, and 135 billion KZT was returned to the budget. By comparison, in 2023, procedural violations totaling 522.9 billion KZT were uncovered, but only 27.8 billion KZT was returned (TALAP, 2024). These figures show that the proportion of violations detected is about 8 percent of the funds audited and underscore the limitations of the existing ex post audit model.

In addition, the Agency for Regulation and Development of the Financial Market (2024) reported that in 2024, information security audits covered 14 banks, with violations found in half of the cases. This highlights the considerable risks associated with protecting client data.

As Suleimenov (2020) emphasizes, the current system focuses on “meeting quantitative regulatory requirements rather than building qualitative trust” (p. 47), which leads to the following systemic consequences: the dominance of retrospective violation detection instead of implementing mechanisms for preventive data integrity protection; limited data sharing among institutions due to a closed bureaucratic structure; and the absence of real-time public accountability mechanisms.

As the World Bank (2021) notes: “Kazakhstan’s audit model is oriented toward institutional compliance at the expense of public verifiability, which results in the erosion of basic trust” (p. 34). The low level of trust in the banking oversight system is documented not only in reports by international organizations. For example, the World Bank estimates public trust at 38 percent. he Tenge’s (2024) summary of the annual @FINANCEkaz Bank Trust Index (2024), overall trust in banks rose from 2.88 to 3.06 points in 2024. At Freedom Bank, the score increased from 2.03 (2021) to 2.81 (2024). At the same time, the rise in trust coincided with a surge in fraud. According to the Ministry of Internal Affairs, as reported by Kazinform (2025), in 2024 more than 22,000 cases of online fraud were registered, with damages amounting to about 45.5 billion KZT, of which only 2.1 billion KZT was recovered. Analysts at Ranking.kz (2025) further noted that victims of online fraud lost 11.4 billion KZT in 2024, which is 2.8 times more than the previous year. These figures highlight citizens’ distrust of control mechanisms and the urgent need to increase audit transparency.

The technical architecture of Kazakhstan’s audit system is characterized by several critical limitations:

(1) Centralized information storage: audits are conducted at the level of individual bank repositories, which prevents cross-system analysis (OECD, 2023). There are no API interaction standards comparable to Estonia’s X-Road platform (Estonian Financial Supervision Authority, 2020).

(2) Lack of user interfaces: there are no user-facing audit monitoring dashboards. The audit module on eGov.kz remains unimplemented (OECD, 2023). Blockchain- or cryptographic-based mechanisms for public data integrity verification are absent.

OECD (2023) directly states that these limitations “prevent Kazakhstan from implementing a trust-by-design model similar to Estonia’s” (p. 64), emphasizing that technical centralization obstructs the socio-technical alignment necessary for sustainable institutional trust.

Proposed Theoretical Model

Based on the synthesis of Estonia’s digital trust architecture, socio-technical systems theory (STS), and institutional trust theory, this study proposes a four-level audit model for Kazakhstan’s banking sector. Such a multi-level structure makes it possible to move from formal regulatory compliance toward a trust-by-design architecture, where accountability is ensured both by the regulator and by society.

The first level can be characterized as user-oriented. Its foundation consists of citizen audit portals that allow real-time verification of transactions using the National Digital Identity (NDID). In line with socio-technical systems theory, this level secures user agency in the oversight process (Mumford, 2006). Empirical evidence supports the effectiveness of this approach: 78 percent of fraud detection cases in Estonia’s banking sector were initiated by citizens themselves (Estonian Financial Supervision Authority, 2020).

The second level is linked to managerial mechanisms. Here, regulatory sandboxes supervised by the National Bank of Kazakhstan play a key role. These experimental environments allow the testing of technology prototypes, including blockchain-based audit solutions, without the risk of large-scale failures. Within the logic of institutional trust, sandboxes provide legitimacy through controlled innovation (OECD, 2023). Precedents in other countries confirm their practical value. In the United Arab Emirates, their use reduced implementation risks by 42 percent (World Bank, 2020).

The third level establishes the technical foundation of the proposed model. It includes blockchain audit logs with hash links (AIFC Blockchain Hub), an API-based data exchange infrastructure comparable to Estonia’s X-Road (Draft NBRK Regulation No. 589), and cryptographic verification based on Merkle trees (Nakamoto, 2008). This combination creates the conditions for systemic accountability and reduces the likelihood of repeated fraud incidents.

Finally, the fourth level reflects the target trust indicators that make it possible to measure the effectiveness of the proposed model. The key benchmarks include achieving by 2030 a public trust level in banking audits of no less than 80 percent (compared to the current 38 percent) and reducing the rate of repeat violations by approximately 30 percent.

Adapting Estonia’s trust audit model to Kazakhstan requires identifying the key components that can be integrated into the national infrastructure. The table below presents the main elements of Estonia's trust architecture and their potential counterparts within Kazakhstan's STTA (Table 2).

Table 2. Adaptation of Estonian model components in the context of Kazakhstan

Element of the Estonian model	Proposed STTA Counterpart for Kazakhstan
Data exchange via X-Road platform	API-based audit platform under the supervision of the National Bank
Electronic identification (e-ID)	Use of the National Digital Identity (NDID) for audit purposes
Blockchain integration for data integrity	Hash-linked transaction logs tied to the digital tenge platform
Citizen audit portals	Real-time dashboards for transaction verification

Note: adapted from Estonian Information System Authority (2023) and National Bank of Kazakhstan (2023)

Adapting the trust architecture to Kazakhstan's conditions requires not only the introduction of new technologies but also the consideration of social factors and changes in legislation. Estonia's experience shows that sustainable trust is formed at the intersection of digital infrastructure, citizen rights, and transparent procedures. Transferring these solutions into Kazakhstani practice is possible with adjustments to the regulatory framework and the creation of conditions for public verification of audit processes. A generalized model reflecting the technical, social, and legal elements of adaptation is presented in Table 3.

Table 3. Integration of trust architecture elements in Kazakhstan

Estonian component	**Technical mechanism**	**Social mechanism**	**Possible adaptation in Kazakhstan**	**Required legal/ regulatory change**
X-Road equivalent	API-based audit infrastructure under NBRK	Interaction between banks and regulator	Integration with digital tenge (CBDC) infrastructure	Amendments to §45 of the NBRK Audit Rules
e-ID system	National Digital Identity (NDID)	Citizens' rights to authentication	Integration with eGov.kz platform	Revision of the Law on Protection of Financial Consumers' Rights
Data integrity assurance	Hash-linked audit logs	Public verification portals	Implementation through AIFC Blockchain Hub	Amendments to Article 19(3) of the Personal Data Law
Citizens' right to audit	Real-time access logs	Complaint channels via Ombudsman	Connection to NDID monitoring portals	Supplement to the Law on Protection of Financial Consumers' Rights

Note: compiled based on adapted materials from OECD (2025), World Bank (2021), and NBK (2023).

Projected Implementation Outcomes

The proposed STTA architecture is aimed at achieving measurable effects. At the technical level, it will provide open, cryptographically verifiable audit evidence through the digital tenge infrastructure (NBK, 2023). At the social level, it will enable citizen-initiated audits (spot audits), carried out through verified NDID requests in line with OECD (2025) recommendations. At the institutional level, the target is to achieve by 2030 at least 80 percent public trust in audit mechanisms, consistent with Estonia's current trajectory.

The effectiveness of the proposed trust audit model rests on the interaction of technical and social instruments that reinforce one another. The key elements are data integrity proofs and citizen-initiated audits. The first mechanism provides institutional transparency through cryptographic protection, while the second establishes a social dimension by involving users directly in oversight. Together, they create a resilient socio-technical system where trust relies both on algorithms and on active public participation.

(1) *Data integrity proofs*

Technical implementation: transaction hashes using the SHA-384 algorithm anchored in the digital tenge blockchain infrastructure.

Theoretical basis: cryptographic immutability as the foundation of institutional trust (Nakamoto, 2008).

Estonian experience: the KSI blockchain reduced cases of data falsification by 92 percent (Guardtime, 2017).

(2) *Citizen-initiated audits*

Mechanism: submission of violation reports through egov.kz with NDID authentication, automatic generation of Merkle-chain proofs, and dispute resolution by the Ombudsman within 72 hours.

STS alignment: human oversight as a safeguard for correcting systemic errors (Mumford, 2006).

The effectiveness of the STTA depends heavily on its phased implementation. A gradual transition from pilot projects to full-scale integration reduces risks and ensures stakeholder participation. Table 4 presents a roadmap for introducing the trust architecture in Kazakhstani banking audit, specifying implementation stages, responsible actors, and trust targets.

Table 4. Roadmap for Implementing the Trust Architecture in Kazakhstani Banking Audit

Period	Implementation Stage	Responsible Actor	Target Trust Indicator
2024–2025	Pilot of regulatory sandbox	AIFC Fintech Lab	Integration of 3 banks
2026–2027	Launch of NDID audit portal	Upgrade of egov.kz 3.0	50 percent citizen participation
2028–2030	Full-scale implementation of X-Road API	Digital tenge infrastructure	80 percent level of public trust

Note: based on data from the NBK (2023) and OECD (2025), reflecting phased implementation of the STTA model.

The proposed theoretical model demonstrates that building trust in banking audit requires the parallel development of technical infrastructure, institutional mechanisms, and citizen participation. The four-level architecture and its core mechanisms make it possible to translate the abstract concept of trust into measurable indicators and practical procedures, while the roadmap reflects a realistic sequence of steps for adapting the model to the national context. Together, these conditions provide the foundation for shifting from retrospective control to a trust-by-design system, where transparency and accountability are ensured not only through regulatory norms but also through verifiable public participation.

DISCUSSION

The synthesis of socio-technical systems (STS) theory and institutional trust theory within the proposed model demonstrates how technical guarantees and public oversight jointly generate institutional trust. Empirical evidence of this interconnection is provided by Estonia, where citizens' trust in e-governance has reached 95 percent, the highest in the EU (Eurostat, 2022). The proposed architecture addresses the trust deficit in Kazakhstan's audit system through three key theoretical innovations.

First, the model operationalizes the principle of joint optimization, central to STS theory (Trist & Bamforth, 1951), by integrating two complementary subsystems. On one side it embeds cryptographic proofs of integrity, and on the other it institutionalizes citizens' rights to audit. This combination ensures a balance between technical reliability and social oversight, which is essential for sustainable trust.

Such a structure produces a self-reinforcing trust cycle:*Technical transparency → Verifiable fairness → Institutional trust → Voluntary participation.*

Estonia's X-Road architecture offers a vivid illustration of this process. Kattel and Mergel (2019) found that 83 percent of citizens trust digital services "because they can verify the system's outputs themselves" (p. 37). This finding supports Zucker's (1986) argument that trust in institutions is not derived from faith but from procedural verifiability.

The proposed model translates the abstract notion of trust into measurable indicators. Of particular importance are the Public Verifiability Index, reflecting the share of transactions accompanied by Merkle proofs, and the Trust Velocity metric, which measures the average time required for citizens to detect anomalies. Estonia's experience confirms the feasibility of such metrics: the implementation of the KSI blockchain reduced data falsification in audits by 92 percent (Guardtime, 2017).

Applying this model in Kazakhstan faces two key limitations identified by STS theory:

(1) Technological inertia: outdated IT systems do not support API integration comparable to X-Road (OECD, 2023).

(2) Social asymmetry: dominant hierarchical norms within a collectivist culture may hinder citizen oversight (Hofstede, 2001).

This necessitates phased testing of the model in regulatory sandboxes, whose effectiveness has been demonstrated in the UAE, where such an approach reduced risks by 42 percent (World Bank, 2020).

For the successful adaptation of the STTA in Kazakhstan, it is essential to account for the full range of technical, legal, and social risks. Table 5 outlines these risks, their likelihood and consequences, and suggested mitigation strategies.

Table 5. Risks and barriers to STTA implementation in Kazakhstan

Risk category	Description	Likelihood / impact	Mitigation strategies
Technical: Insufficient infrastructure security and rising online fraud	Two-factor biometric authentication was introduced for remote services; in 2024, new two-step image verification rules were applied. Inspections of 14 banks revealed violations (Agency for Regulation and Development of the Financial Market [ARDFM], 2024). In 2024, 22.9 thousand cybercrime cases were registered, with total losses of 11.4 billion KZT and recovery of only 36.6% (Ranking.kz, 2025).	High / High	• Mandatory audits of source code and certification of applications. • Strict enforcement of two-step biometrics and encryption of all data. • Regular monitoring and joint operations with the Ministry of Internal Affairs. • Expansion of the "Stop-Credit" program.
Technical: Outdated IT platforms and lack of contingency planning	A significant share of banks continue to use software developed before 2010. Only about one-third of state audit inspections are conducted remotely (Agency for Regulation and Development of the Financial Market [ARDFM], 2024).	Medium / High	• Modernization of infrastructure and transition to X-Road-compatible APIs and KSI blockchain. • Regular stress testing and continuity planning. • Centralized risk management platform.
Legal: Weak regulatory framework for digital audit and data protection	Biometric systems require storing multiple images for the entire loan period without clear access control mechanisms (Agency for Regulation and Development of the Financial Market [ARDFM], 2024). Around 2,000 fraud cases remain unreported annually (Kazinform, 2025).	Medium / Severe	• Adoption of a dedicated Digital Audit Law with biometric provisions. • Harmonization with eIDAS and GDPR standards. • Strict access control with independent oversight.
Social: Low digital literacy and persistent distrust	The Trust Index for banks increased from 2.88 to 3.06 (The Tenge, 2024). Victims of online fraud are often aged 49–60 or retirees; over 7 billion KZT in losses remain uncompensated (Ranking.kz, 2025).	Medium / High	• Nationwide financial literacy campaigns. • Alternative offline service channels for vulnerable groups. • Public dashboards for transaction verification. • Communication campaigns on protective measures.
Social: Concerns over biometrics and privacy	Mandatory two-step biometrics and image storage raise concerns among parts of the population (Agency for Regulation and Development of the Financial Market [ARDFM], 2024).	Medium / Medium	• Establishment of an independent biometric oversight body. • Use of transparent algorithms and regular public reporting. • Legal right to data deletion. • Public consultations and hearings.

Note: compiled by the author

The proposed model expands the boundaries of scientific knowledge in the field of socio-technical systems theory and institutional trust. It demonstrates that digital trust can result from architectural design based on the alignment of technical and social components, which corresponds to the ideas of Bostrom and Heinen (1977). At the same time, it provides a transferable framework for countries with emerging digital infrastructures, responding to the OECD's (2023) call for the development of contextualized trust models. An additional contribution is the introduction of the concept of algorithmic accountability as a measurable trust indicator, which advances the propositions outlined in Zucker's (1986) classical theory.

The viability of the proposed model depends on Kazakhstan's ability to reproduce the balance between technological rigor and social inclusiveness that characterizes Estonia. Meeting this challenge requires sequential empirical testing and institutional flexibility.

The proposed STS-Trust model faces a number of significant implementation barriers arising from Kazakhstan's institutional and infrastructural specificities. Overcoming these barriers requires the adoption of adaptive implementation strategies.

Kazakhstan's banking sector continues to operate under technological dependence on outdated solutions: 73 percent of audit systems are based on architectures developed before 2010 (World Bank, 2021). This produces three key compatibility problems:

(1) Deficit of interoperability: isolated databases hinder the implementation of API integration following the X-Road model (OECD, 2023).

(2) Cybersecurity vulnerability: reliance on legacy SWIFT-based protocols increases the risk of data leaks and cyberattacks by 57 percent (KazCERT, 2022).

The proposed strategy for mitigating infrastructural inertia includes phased migration through regulatory sandboxes, as recommended by the World Bank, and the creation of a 45 billion KZT Infrastructure Modernization Fund (as outlined in the draft budget of the Ministry of Artificial Intelligence and Digital Development of the Republic of Kazakhstan, 2023).

The current regulatory environment in Kazakhstan is not institutionally aligned with the principles of trust-by-design. Key limitations include:

(1) Focus on compliance: NBRK Decree No. 567 contains 287 mandatory ex post control procedures but does not include any mechanisms for preventive verification of data integrity (Suleimenov, 2020).

(2) Absence of citizens' rights: the Law on Protection of Financial Consumers' Rights does not provide for the possibility of citizen-initiated audits (OECD, 2025).

The proposed strategy for regulatory adjustment includes revising §45 of the NBRK regulations to introduce standards for preventive integrity verification, establishing the right to use Merkle proofs in Article 19 of the Personal Data Law, and creating a fintech ombudsman under AIFC jurisdiction.

CONCLUSION

This study positions socio-technical systems (STS) theory and institutional trust theory as complementary foundations for rethinking audit architecture. It has shown that technical mechanisms for ensuring integrity, such as blockchain proofs and API integration, when combined with social instruments of oversight, including citizens' rights to audit, are capable of generating institutional trust.

The proposed STS-Trust Audit Framework introduces several important innovations into the academic debate on digital governance. It demonstrates that trust can be "designed" through the alignment of technical and social subsystems, advancing the ideas of Trist and Bamforth (1951) and Zucker (1986). In addition, the model creates a transferable framework for countries with developing digital infrastructures, responding to the OECD's (2025) call for context-sensitive solutions. Of particular note is the introduction of algorithmic accountability as a trust indicator. This approach expands the analytical tools available for assessing digital institutions and transforms trust from an abstract notion into a measurable metric.

Despite structural constraints related to outdated infrastructure and regulatory frameworks, successful implementation of the model could raise public trust in banking audits to more than 80 percent by 2030, reduce fraud-related losses by hundreds of billions of tenge annually, and establish a Kazakhstani model of institutional trust applicable to other Central Asian countries. The findings contribute to the development of trust theory in digital governance by extending analytical tools through the category of algorithmic accountability and by demonstrating the practical applicability of the STTA concept in emerging economies.

Thus, the STS-Trust Framework becomes not only a foundation for modernizing Kazakhstan's national audit system but also a potential reference point for the development of global standards in digital governance.

AUTHOR CONTRIBUTIONS

Conceptualization and theory: AA and UR; research design: AA and UR; data collection: AA and UR; analysis and interpretation: AA; writing draft preparation: AA and UR; supervision: AA; correction of article: AA and UR; proofreading and final approval of article: AA. All authors have read and agreed to the pub- lished version of this manuscript.

REFERENCES

Agency for Regulation and Development of the Financial Market. (2024). *O merakh po obespecheniyu informatsionnoi bezopasnosti finansovykh organizatsii i protivodeistviyu moshennichestvu* [On measures to ensure information security of financial organizations and countering fraud]. FinGramota.kz. Retrieved June 23, 2025 from https://fingramota.kz/ru/news/post/o-merah-po-obespecheniyu-informacionnoj-bezopasnosti-finansovyh-organizacij-i-protivodejstviyu-moshennichestvu

Bannister, F., & Connolly, R. (2014). The trouble with transparency: A critical review of openness in e-government. *Policy & Internet*, *3*(1), 1-30. https://doi.org/10.2202/1944-2866.1076

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. *MIS Quarterly, 1*(3), 17–32. https://doi.org/10.2307/248710

Cherns, A. (1976). The principles of socio-technical design. *Human Relations*, *29*(8), 783–792. https://doi.org/10.1177/001872677602900806

Clegg, C. W. (2000). Sociotechnical principles for system design. *Applied Ergonomics*, *31*(5), 463–477. https://doi.org/10.1016/S0003-6870(00)00009-0

e-Estonia. (2019). Interoperability as the meeting point for a digital Nordic league. Retrieved June 23, 2025 from https://e-estonia.com/interoperability-as-the-meeting-point-for-a-digital-nordic-league/

e-Estonia. (2024). *X-Road: Interoperability services*. Retrieved June 23, 2025 from https://e-estonia.com/solutions/interoperability-services/x-road/

ENISA. (2017). *Blockchain cybersecurity: Key recommendations*. Publications Office of the EU. Retrieved June 23, 2025 from https://www.enisa.europa.eu/news/enisa-news/enisa-report-on-blockchain-technology-and-security

ERR. (2021). *Audit Office: IT security of firms using X-Road not sufficiently checked*. Retrieved June 23, 2025 from https://news.err.ee/1608127567/audit-office-it-security-of-firms-using-x-road-not-sufficiently-checked

Estonian Financial Supervision Authority. (2020). *Annual report 2019*. Retrieved June 23, 2025 from https://www.fi.ee/en/publications/finantsinspektsioon-annual-report-2019

Estonian Information System Authority. (2023). *Data Exchange Layer X-tee*. Retrieved June 23, 2025 from https://www.ria.ee/en/x-road.html

EuroEuropean Commission. (2020). *eGovernment benchmark 2020: eGovernment that works for the people: Insight report*. Publications Office of the European Union. Retrieved June 23, 2025 from https://data.europa.eu/doi/10.2759/24753

Eurostat. (2022). *Digital economy and society statistics – households and individuals*. European Commission. Retrieved June 23, 2025 from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals

Guardtime. (2017). *GDPR compliance using KSI® blockchain (Guardtime white paper; VOLTA – Compliance with GDPR, v2)*. Retrieved June 23, 2025 from https://m.guardtime.com/files/guardtime-whitepaper-volta-v2.pdf

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations* (2nd ed.). Sage Publications.

Inbusiness.kz**.** (2025). *2024 god stal rekordnym po effektivnosti gosaudita v RK* [2024 was a record year for state audit effectiveness in the Republic of Kazakhstan]. Retrieved June 23, 2025, from https://inbusiness.kz/ru/last/2024-god-stal-rekordnym-po-effektivnosti-gosaudita-v-rk

Kattel, R., & Mergel, I. (2019). Estonia's digital transformation: Mission mystique and the hiding hand. In M. E. Compton & P. 't Hart (Eds.), *Great policy successes* (pp. 143–160). Oxford University Press. https://doi.org/10.1093/oso/9780198843719.003.0008

KazCERT. (2022). Kazakhstan Computer Emergency Response Team. Retrieved June 23, 2025, from https://www.cert.gov.kz/

Kazinform. (2025). MVD Kazakhstana prokommentirovalo fakty ukrytiya moshennichestva [The Ministry of Internal Affairs of Kazakhstan commented on concealment of fraud cases]. Kazinform. Retrieved June 23, 2025 from https://www.inform.kz/ru/mvd-kazahstana-prokommentirovalo-fakti-ukritiya-moshennichestva-e92ba4

Lewicki, R. J., Tomlinson, E. C., & Gillespie, N. (2006). Models of interpersonal trust development. *Journal of Management*, *32*(6), 991–1022. https://doi.org/10.1177/0149206306294405

Shaw, D. R., Achuthan, K., Sharma, A., & Grainger, A. (2019). Resilience orchestration and resilience facilitation: How government can orchestrate the whole UK ports market with limited resources – The case of UK ports resilience. *Government Information Quarterly, 36*(2), 252–263. https://doi.org/10.1016/j.giq.2018.12.003

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing trust measures for e-commerce. *Information Systems Research, 13*(3), 334–359. https://doi.org/10.1287/isre.13.3.334.81

Ministry of Artificial Intelligence and Digital Development of the Republic of Kazakhstan. (2023). Retrieved June 23, 2025, from https://www.gov.kz/memleket/entities/mdai

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal*, *16*(4), 317–342. https://doi.org/10.1111/j.1365-2575.2006.00221.x

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. SSRN. http://dx.doi.org/10.2139/ssrn.3440802

NBK. (2022). *On banking audits* (Regulation No. 567). National Bank of Kazakhstan. Retrieved June 23, 2025 from https://nationalbank.kz/en/legislation/regulations

NBK. (2023a). Ob utverzhdenii Kontseptsii tsifrovogo tenge [On approval of the Digital Tenge Concept] (Regulation No. 43). National Bank of Kazakhstan. Retrieved June 23, 2025 from https://nationalbank.kz/en/news/on-approval-the-digital-tenge-concept

NBK. (2023b). *Report on Bank CenterCredit rehabilitation*. National Bank of Kazakhstan. Retrieved June 23, 2025 from https://nationalbank.kz/en/news/report-on-bcc-rehabilitation

OECD. (2023). *Improving framework conditions for the digital transformation of businesses in Kazakhstan*. OECD Publishing. Retrieved June 23, 2025 from https://doi.org/10.1787/368d4d01-en

OECD (2025), OECD Integrity Review of Kazakhstan: Advancing Integrity for Economic Development, OECD Public Governance Reviews, OECD Publishing. Retrieved June 23, 2025 from https://doi.org/10.1787/d705d02f-en

Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in government: Benefits and implications of distributed ledger technology for information sharing. *Government Information Quarterly*, *34*(3), 355–364. https://doi.org/10.1016/j.giq.2017.09.007

Pasmore, W., Francis, C., Haldeman, J., & Shani, A. (1982). Sociotechnical systems: A North American reflection on empirical studies of the seventies. *Human Relations*, *35*(12), 1179–1204. https://doi.org/10.1177/001872678203501207

Ranking.kz. (2025). Uscherb ot internet-moshennichestva v Kazakhstane vyros pochti vtroe [Damage from internet fraud in Kazakhstan has almost tripled]. Ranking.kz. Retrieved June 23, 2025 from https://ranking.kz/digest/regions-digest/uscherb-ot-internet-moshennichestva-v-kazahstane-vyros-pochti-vtroe.html (In Russ.)

Statistics Estonia. (2023). *Statistics Estonia*. Retrieved June 23, 2025, from https://www.stat.ee/en

Suleimenov, B. (2020). Problemy regulirovaniya bankovskogo sektora v Kazakhstane [Banking regulation challenges in Kazakhstan]. *Eurasian Law Journal, 3*(142), 45–49. (In Russ.)

Supreme Audit Chamber of the Republic of Kazakhstan. (2024). *Supreme Audit Chamber of the Republic of Kazakhstan*. Retrieved June 23, 2025 from https://www.gov.kz/memleket/entities/esep?lang=en

TALAP**.** (2024). *Byudzhetnye narusheniya i neeffektivnoe ispol'zovanie sredstv: neuteshitelnye vyvody VAP Kazakhstana za 2023 god* [Budget violations and inefficient use of funds: disappointing findings of the Supreme Audit Chamber of Kazakhstan for 2023]. Retrieved June 23, 2025 from https://openbudget.kz/news/22/

The Tenge. (2024). *Itogi indeksa doveriya kazakhstanskikh bankov ot @FINANCEkaz za 2024 god* [Results of the bank trust index in Kazakhstan by @FINANCEkaz for 2024]. Retrieved June 23, 2025 from https://the-tenge.kz/articles/indeks-doveriya-k-bankam-

Tammpuu, P., & Masso, A. (2018). 'Welcome to the virtual state': Estonian e-residency and the digitalised state as a commodity. *European Journal of Cultural Studies, 21*(5), 543–560. https://doi.org/10.1177/1367549417751148

Trist, E., & Bamforth, K. (1951). Some Social and Psychological Consequences of the Longwall Method of Coal-Getting: An Examination of the Psychological Situation and Defences of a Work Group in Relation to the Social Structure and Technological Content of the Work System. *Human Relations, 4*(1), 3–38. https://doi.org/10.1177/001872675100400101

Tyler, T. R. (2006). Psychological perspectives on legitimacy and legitimation. *Annual Review of Psychology*, *57*, 375–400. https://doi.org/10.1146/annurev.psych.57.102904.190038

World Bank. (2020). *Global experiences from regulatory sandboxes* (Finance, Competitiveness & Innovation Global Practice, FinTech Note No. 8). World Bank. Retrieved June 23, 2025 from https://documents.worldbank.org/en/publication/documents-reports/documentdetail/912001605241080935/global-experiences-from-regulatory-sandboxes

World Bank. (2021). *Kazakhstan Economic Update, Summer 2021: Turning the Tide on the COVID-19 Crisis*. World Bank. Retrieved June 23, 2025 from https://openknowledge.worldbank.org/entities/publication/27afe141-2cfa-5e08-907d-324c9aaf16c4

Zucker, L. G. (1986). Production of trust: Institutional sources of economic structure. *Research in Organizational Behavior*, *8*, 53–111.

Information about the author

***Avina Abytaeva** – MBA Candidate, Westcliff University, Miami, Florida, USA, email: abytaeva.a21@gmail.com, ORCID ID: https://orcid.org/0009-0004-4174-5022

Urmat Ryskulov – PhD, Associate Professor, American University of Central Asia, Bishkek, Kyrgyzstan, email: ryskulov_u@auca.kg, ORCID ID: https://orcid.org/0000-0003-0018-7955

Автор туралы мәліметтер

***Абытаева А.** – MBA магистранты, Уэстклифф университеті, Майами, Флорида, АҚШ, email: abytaeva.a21@gmail.com, ORCID ID: https://orcid.org/0009-0004-4174-5022

Рыскулов У. – PhD, қауымдастырылған профессор, Орталық Азия Америкалық университеті, Бішкек, Қырғызстан, email: ryskulov_u@auca.kg, ORCID ID: https://orcid.org/0000-0003-0018-7955

Сведения об авторе

***Абытаева А.** – магистрант программы MBA, Университет Уэстклифф, Майами, Флорида, США, email: abytaeva.a21@gmail.com, ORCID ID: https://orcid.org/0009-0004-4174-5022

Рыскулов У. – PhD, доцент, Американский университет в Центральной Азии, Бишкек, Кыргызстан, email: ryskulov_u@auca.kg, ORCID ID: https://orcid.org/0000-0003-0018-7955