# SOCIO-TECHNICAL SYSTEMS APPROACH TO FINANCIAL RISK MANAGEMENT AND FRAUD PREVENTION IN INTEGRATED LOGISTICS CHAINS

Ana-Maria GOLITA[1], Augustin SEMENESCU[2],
Ionut-Cristian SCURTU[3], Tanase TASENTE[4], Romeo BOSNEAGU[5,6]

[1] National University of Science and Technology Politehnica Bucharest, Bucharest, Romania,
ORCID No. 0009-0008-1607-5898, ana_maria.golita@stud.fiir.upb.ro
[2] National University of Science and Technology Politehnica Bucharest, Bucharest, Romania,
ORCID No. 0000-0001-6864-3297, asemenescu2002@yahoo.com
[3] National University of Science and Technology Politehnica Bucharest, Bucharest, Romania,
ORCID No. 0000-0003-3105-6384, scurtucristian@yahoo.com
[4] Ovidius University of Constanta, Constanta, Romania,
ORCID No. 0000-0002-3164-5894, tanase.tasente@365.univ-ovidius.ro
[5] Romanian Naval Academy "Mircea cel Bătrân", Constanta, Romania,
[6]. "Tomis" University Constanta, Romania
ORCID No. 0000-0002-6015-6512, e-mail address: romeo_bosneagu@yahoo.com

ABSTRACT: Integrated logistics chains are undergoing rapid digital transformation through the adoption of Enterprise Resource Planning (ERP) systems, artificial intelligence (AI), the Internet of Things (IoT), blockchain and cloud-based platforms. While these technologies improve visibility, speed and coordination across procurement, warehousing, transportation and distribution, they also expand the attack surface through which financial risks and fraud can materialize. Recent industry data illustrate the scale of the problem: the Association of Certified Fraud Examiners (ACFE, 2024) estimates that a typical organization loses approximately 5% of annual revenue to occupational fraud, equivalent to more than USD 3.1 billion in identified losses across the 1,921 cases examined in its 2024 study, while IBM (2024) reports that the global average cost of a data breach reached USD 4.88 million in 2024, with vendor- and supply-chain-related breaches among the costliest and slowest to contain. At the same time, Verizon's 2024 Data Breach Investigations Report attributes 68% of confirmed breaches to a non-malicious human element, underscoring that technology alone cannot resolve risks that are fundamentally socio-technical in nature. This paper develops a conceptual Socio-Technical Systems (STS) framework that integrates social, technical, organizational and process dimensions to strengthen financial risk management and fraud prevention in integrated logistics chains. Building on the foundational work of Trist and Emery on joint optimization, and on contemporary supply chain resilience and Industry 4.0 literature, the proposed framework maps human factors (leadership, ethics, training, awareness), technical controls (ERP, AI-based anomaly detection, IoT sensors, blockchain, cybersecurity architecture) and governance mechanisms (ISO 31000, COSO ERM) onto the core logistics processes of procurement, warehousing, transportation and distribution. The paper concludes with a discussion of theoretical and managerial implications and proposes a research agenda for the empirical validation of the framework through surveys, case studies and mixed-methods designs. The proposed framework provides a practical foundation for integrating socio-technical principles into financial risk governance and fraud prevention strategies within digitally enabled logistics ecosystems.

KEYWORDS**:** Socio-Technical Systems, integrated logistics chains, financial risk management, fraud prevention, enterprise risk management, supply chain resilience.

DOI 10.56082/annalsarscieco.2026.4.82
.

## 1. INTRODUCTION

Global supply chains have become deeply digitized ecosystems in which financial transactions, physical flows of goods and information flows are tightly interwoven. Enterprise Resource Planning (ERP) systems, artificial intelligence (AI) and machine learning, the Internet of Things (IoT), block chain - based traceability solutions and cloud computing platforms now underpin procurement, inventory management, transportation planning and distribution across most integrated logistics chains (Ivanov, 2021; Christopher, 2023). This digital transformation has delivered substantial efficiency gains, but it has simultaneously created new and more complex avenues for financial risk and fraud, because every additional interface, application programming interface (API), or connected device represents a potential point of compromise (IBM, 2024).

Despite rapid technological progress, many logistics organizations continue to experience significant financial losses caused by fraud, cyberattacks, and governance failures. Existing

research frequently investigates these challenges separately, while limited attention has been devoted to their interaction within an integrated socio-technical perspective.

The financial stakes are considerable. According to the Association of Certified Fraud Examiners' Occupational Fraud 2024: A Report to the Nations, the typical organization loses approximately 5% of its annual revenue to occupational fraud each year, and the 1,921 cases analyzed in the 13th edition of the study - drawn from 138 countries - produced more than USD 3.1 billion in identified losses, with a median loss per case of USD 145,000 and an average loss of roughly USD 1.7 million (ACFE, 2024). In parallel, IBM's Cost of a Data Breach Report 2024 found that the global average cost of a data breach rose 10% year-on-year to USD 4.88 million, the largest single - year increase since the COVID-19 pandemic, driven principally by business disruption and post-breach remediation costs (IBM, 2024). Critically for logistics chains, third-party and supply-chain-related compromises were identified among the most expensive and slowest-resolving breach categories, reportedly taking substantially longer than average to identify and contain because they exploit the trust relationships between vendors, carriers and customers (IBM, 2024, 2025).

A recurring finding across these industry studies is that financial and cyber risk in supply chains is not purely a technological problem. Verizon's 2024 Data Breach Investigations Report, which analyzed more than 30,000 security incidents and over 10,000 confirmed breaches across 94 countries, found that a non-malicious human element - an employee error, a successful phishing attempt, a misconfiguration, or a lapse in judgement - was present in 68% of confirmed breaches (Verizon, 2024). Similarly, the ACFE (2024) reports that more than half of occupational fraud cases were associated with a weak or overridden system of internal controls, a governance and organizational-culture failure rather than a purely technical one. These findings collectively suggest that effective financial risk management and fraud prevention in integrated logistics chains requires the joint optimization of social and technical subsystems — the central proposition of Socio-Technical Systems (STS) theory (Trist & Emery, 1960; Cherns, 1976).

This conceptual paper has three objectives. First, it reviews the literature on STS theory and its application to modern, digitally enabled supply chains. Second, it characterizes the principal categories of financial risk and fraud affecting integrated logistics chains, supported by recent public statistics from the ACFE, IBM and Verizon. Third, it proposes an integrative STS conceptual framework - linking social, technical, process and governance dimensions - intended to guide both future empirical research and practitioner efforts to strengthen resilience against financial risk and fraud in logistics operations.

This study contributes to the literature by proposing an integrated socio-technical framework for financial risk management and fraud prevention in digitally connected logistics chains. The framework combines technological safeguards, organizational governance, risk management practices, and human factors into a unified conceptual model that supports both theoretical development and managerial decision-making.

## 2. Literature Review

### 2.1 Foundations of Socio-Technical Systems Theory

Socio-Technical Systems (STS) theory originated in the work of Eric Trist and Fred Emery at the Tavistock Institute of Human Relations, based on their studies of coal-mining operations in the United Kingdom during the 1950s (Trist & Emery, 1960). The central insight of this research was that organizational performance is not determined by the technical subsystem (equipment, processes, technology) or the social subsystem (people, roles, relationships, culture) in isolation, but by the joint optimization of both. Organizations that optimize only the technical subsystem while neglecting the social subsystem - for example, by introducing new technology without adapting roles, training or incentives - tend to under-perform relative to their technical potential and to generate unintended human and organizational costs. Cherns (1976) later formalized this into a set of design principles, including compatibility between the design process and its objectives, minimal critical specification of tasks, and the co-location of variance control with the people who experience it.

### 2.2 Extensions to Digital Supply Chains and Industry 4.0

Contemporary supply chain and operations management scholarship has extended STS thinking to cyber-physical systems, Industry 4.0 and digital supply chain resilience. Ivanov (2021)

frames the modern supply chain as a network of cyber-physical systems in which digital twins, IoT sensors and AI-based decision support are embedded within - and dependent upon - human decision-making, particularly during disruptions. Christopher (2023) similarly argues that supply chain resilience depends jointly on technological visibility (real-time data on inventory, shipments and demand) and organizational agility (the capacity of people and processes to respond to that data). This body of work supports the proposition that fraud and financial - risk resilience in logistics chains cannot be achieved through technology deployment alone; it requires attention to organizational design, human factors and governance structures operating alongside the technical infrastructure.

### 2.3 Financial Risk, Fraud and Governance Frameworks

A parallel stream of literature addresses enterprise risk management (ERM) and fraud examination. The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management - Integrating with Strategy and Performance framework (COSO, 2017) positions risk management as embedded within governance, strategy-setting, performance and review processes, rather than as a standalone technical control function. ISO 31000:2018 provides complementary generic principles and a process (establishing context, risk identification, analysis, evaluation, treatment, monitoring and review) applicable across industries, including logistics. The ACFE's biennial Report to the Nations constitutes the largest publicly available empirical dataset on occupational fraud and consistently finds that internal-control weaknesses, rather than the absence of technology, are the dominant contributing factor in the majority of cases (ACFE, 2024). Taken together, these frameworks and findings converge with STS theory: financial risk management effectiveness depends on the alignment of governance, human behavior and technical controls.

### 2.4 Research Gap

Despite the conceptual convergence between STS theory, supply chain resilience literature and fraud-examination research, few studies explicitly integrate these three streams into a single framework tailored to the specific processes of integrated logistics chains - procurement, warehousing, transportation and distribution. This paper addresses that gap by proposing an STS-based conceptual model and by grounding its motivation in recent, publicly available quantitative evidence on the scale and nature of financial risk and fraud.

Overall, previous studies demonstrate that digital technologies substantially improve supply chain transparency and operational efficiency. Nevertheless, these technologies also introduce new financial vulnerabilities and governance challenges that remain insufficiently addressed by existing research.

The literature reviewed above confirms that financial risk management, fraud prevention, cybersecurity, and organizational governance are deeply interconnected within modern logistics ecosystems. However, existing studies rarely integrate these dimensions into a unified socio-technical framework. This gap provides the foundation for the conceptual model developed in the following sections.

## 3. Financial Risks and Fraud in Integrated Logistics Chains

Although previous research has significantly advanced the understanding of financial risks, cyber threats, and governance in logistics, most studies focus on isolated dimensions of these challenges. Comprehensive socio-technical models integrating organizational, technological, procedural, and human factors remain scarce.

Integrated logistics chains are exposed to a broad typology of financial risks, ranging from classic occupational fraud schemes (e.g., billing fraud, check tampering, procurement collusion) to cyber-enabled schemes that exploit digital interfaces between trading partners (e.g., business email compromise, invoice redirection, ransomware-driven extortion). Table 1 summarizes the principal categories of occupational fraud identified in the ACFE's 2024 global study, which - while not specific to logistics - provides the most comprehensive publicly available benchmark for the frequency and severity of internal fraud schemes relevant to procurement, warehousing and finance functions within supply chains. To facilitate a structured understanding of the financial risks affecting logistics chains, the principal categories identified in recent international reports are summarized below.

**Table 1.** Occupational Fraud Categories, Frequency and Median Loss (ACFE, 2024)

| Fraud Category | Share of Cases | Median Loss (USD) | Description |
|---|---|---|---|
| Asset misappropriation | 89% | $120,000 | Theft or misuse of cash, inventory or other organizational resources; most frequent but least costly category. |
| Corruption | 48% | $200,000 | Bribery, kickbacks, extortion and conflicts of interest, often involving vendors or procurement staff. |
| Financial statement fraud | 5% | $766,000 | Intentional misstatement or omission in financial reports; least frequent but most financially damaging category. |
| Overlap (2 or more categories) | 38% | n/a | Asset misappropriation combined with corruption is the most common overlap, occurring in 35% of all cases. |

Beyond internally generated occupational fraud, integrated logistics chains face a growing volume of externally enabled financial and cyber risk. IBM's Cost of a Data Breach Report 2024, based on an analysis of 604 breached organizations across 17 industries and 16 countries, found that the global average cost of a data breach reached USD 4.88 million, a 10% increase over the prior year (IBM, 2024). Table 2 summarizes cost benchmarks by breach type and vector most relevant to logistics and supply chain operations.

**Table 2.** Selected Data Breach Cost Benchmarks Relevant to Supply Chains (IBM, 2024, 2025)

| Breach Category / Vector | Average Cost (USD) | Notes |
|---|---|---|
| Global average, all breaches (2024) | $4.88 million | 10% increase year-on-year; largest jump since the pandemic. |
| Vendor / supply-chain / third-party breach | $4.91 million | Among the costliest attack vectors; longest average time to identify and contain (reported at over 260 days). |
| Breaches involving data across multiple environments | $5.00+ million | 40% of breaches involved data spread across public cloud, private cloud and on-premises systems. |
| Phishing-initiated breach | $4.80 million | Most common single initial attack vector across the 2025 study. |
| Healthcare sector (highest-cost industry) | $7.42–$9.77 million | Highest-cost industry for 14 consecutive years; figure varies by report year. |
| Cost reduction from extensive security AI/automation use | -$2.2 million | Largest single cost-mitigating factor identified across both the 2024 and 2025 reports. |

These figures indicate that supply-chain and vendor-related breaches are not only common but disproportionately expensive and slow to resolve relative to other attack vectors, precisely because they exploit inter - organizational trust rather than a single organization's perimeter defenses.

### 3.1 The Human Element in Financial and Cyber Risk

The human dimension of risk is further evidenced by Verizon's 2024 Data Breach Investigations Report (DBIR), which analyzed 30,458 security incidents and 10,626 confirmed data breaches across 94 countries between November 2022 and October 2023. The report found that a non-malicious human element - encompassing errors, misconfigurations and susceptibility to social engineering - was present in 68% of confirmed breaches (Verizon, 2024). In simulated phishing exercises referenced in the same report, the median time for a user to click a malicious link was approximately 21 seconds, and

the median time to submit sensitive data to a simulated phishing site was approximately 28 seconds, illustrating how quickly human behavior can convert a technical vulnerability into a financial loss event. Table 3 summarizes the trend in the human element's contribution to breaches across recent DBIR editions.

**Table 3.** Human Element in Confirmed Data Breaches, Verizon DBIR (2021–2024)

| Report Year | Human Element Share | Notes |
|---|---|---|
| 2021 | 85% | Includes malicious and non-malicious insider actions under the broader 'human element' category. |
| 2022 | 82% | Continued inclusion of malicious insider actions in the reported figure. |
| 2023 | 74% | Methodology consistent with prior years. |
| 2024 | 68% | Methodology changed to exclude malicious insider actions, isolating non-malicious human error and social engineering susceptibility specifically. |

Because logistics chains depend on coordinated action across procurement officers, warehouse staff, drivers, customs brokers, freight forwarders and finance teams — frequently spanning multiple organizations and jurisdictions — the number of individual human decision points exposed to error or manipulation is inherently larger than in a single-firm operating environment. This structural characteristic of logistics chains amplifies the relevance of the human element statistics reported above and reinforces the rationale for a socio-technical, rather than purely technical, approach to risk management.

### 3.2 Fraud Typology Specific to Logistics Operations

Building on the general categories above, financial risk and fraud in integrated logistics chains can be further disaggregated into operationally specific schemes, summarized in Table 4.

**Table 4.** Financial Risk and Fraud Typology in Integrated Logistics Chains

| Logistics Process | Representative Risk / Fraud Types | Primary STS Dimension Implicated |
|---|---|---|
| Procurement | Vendor collusion, bid rigging, fictitious suppliers, kickbacks, duplicate invoicing | Social / governance (ethics, segregation of duties, procurement controls) |
| Warehousing & Inventory | Inventory shrinkage, phantom stock, theft of noncash assets, manipulated cycle counts | Technical + Social (IoT/RFID tracking combined with staff accountability) |
| Transportation | Freight fraud (double brokering), fuel card abuse, fictitious mileage or delivery claims, cargo theft | Technical (telematics, GPS tracking) + Process controls |
| Distribution & Order-to-Cash | Business email compromise, invoice redirection fraud, payment diversion, chargeback abuse | Technical (email security, payment verification) + Social (staff verification protocols) |
| Cross-cutting / Financial Reporting | Financial statement manipulation, revenue recognition schemes, expense misclassification | Governance (internal controls, external audit, ERM) |

## 4. Proposed Socio-Technical Systems Framework

Drawing on the STS foundations reviewed in Section 2 and the risk typology developed in Section 3, this paper proposes an integrative conceptual framework comprising four interacting dimensions: (i) the social subsystem, (ii) the technical subsystem, (iii) core logistics processes, and (iv) risk governance activities. The framework's central proposition is that financial risk and fraud resilience in integrated logistics chains is a function of the alignment - the joint optimization, in Trist and Emery's original

terminology - of these four dimensions, rather than the strength of any single dimension in isolation.

### 4.1 The Social Subsystem

The social subsystem encompasses leadership commitment to ethical conduct, the design of incentive and accountability structures, fraud-awareness training, whistleblower and reporting mechanisms, and the broader organizational culture surrounding risk. Empirical support for the importance of this dimension is substantial: the ACFE (2024) reports that tips remain the single most common fraud-detection mechanism, accounting for 43% of case detections, and that organizations with anonymous reporting hotlines experience meaningfully lower losses and shorter detection times than those without. Employees supplied more than half of all fraud tips in the 2024 study, ahead of customers (21%) and vendors (11%) (ACFE, 2024). These findings indicate that a well-designed social subsystem - one that encourages reporting and embeds ethical expectations into daily practice - functions as a detection and prevention control in its own right, independent of any specific technology.

### 4.2 The Technical Subsystem

The technical subsystem comprises the digital infrastructure that enables integrated logistics operations and, simultaneously, must be secured against misuse: ERP platforms for financial and inventory control, AI and machine - learning models for anomaly and fraud detection, IoT sensors and RFID tagging for real-time asset tracking, block chain - based ledgers for provenance and transaction verification, and cybersecurity architecture (identity and access management, encryption, network segmentation, security operations). IBM (2024) found that organizations making extensive use of AI and automation in security prevention workflows incurred, on average, USD 2.2 million less in breach costs than organizations that did not - the single largest cost-mitigating factor identified in that year's study. This suggests that well-implemented technical controls yield measurable risk - reduction benefits, but the same report's finding that vendor and third-party breaches remain among the costliest and slowest to resolve indicates that technical controls implemented at a single node of the logistics chain cannot substitute for coordinated, chain-wide technical and organizational alignment (IBM, 2024, 2025).

### 4.3 Core Logistics Processes

The framework maps the social and technical dimensions onto four core logistics processes - procurement, warehousing, transportation and distribution - consistent with the operational typology developed in Table 4. Each process exhibits a distinct risk profile and therefore requires a distinct configuration of social and technical controls: procurement risk is disproportionately governance- and ethics-driven, warehousing risk benefits strongly from IoT - and RFID - based technical tracking combined with staff accountability, transportation risk benefits from telematics and route verification, and distribution/order-to-cash risk is increasingly dominated by cyber-enabled schemes such as business email compromise and invoice redirection fraud.

### 4.4 Risk Governance Activities

The fourth dimension embeds the framework within established enterprise risk management practice, consistent with ISO 31000:2018 and the COSO (2017) ERM framework. Four governance activities are proposed as continuous, cyclical processes operating across the social, technical and process dimensions: (1) risk identification - systematically cataloguing financial risk and fraud exposure across each logistics process; (2) risk assessment - evaluating likelihood and impact, informed by benchmarks such as those in Tables 1–4; (3) monitoring - continuous technical monitoring (e.g., AI-based anomaly detection, transaction monitoring) combined with social monitoring (e.g., internal audit, whistleblower channels); and (4) mitigation - the design and implementation of controls spanning both social interventions (training, segregation of duties, incentive redesign) and technical interventions (system controls, encryption, access management).

### 4.5 Summary of the Framework

Table 5 summarizes the proposed framework by cross-referencing its four dimensions with illustrative components and the supporting evidence base discussed in this paper.

**Table 5.** Summary of the Proposed STS Framework for Financial Risk Management in Integrated Logistics Chains

| Dimension | Illustrative Components | Supporting Evidence |
|---|---|---|
| Social subsystem | Leadership & tone at the top; ethics training; whistleblower hotlines; segregation of duties | 43% of fraud detected via tips; hotlines associated with lower losses (ACFE, 2024) |
| Technical subsystem | ERP; AI/ML anomaly detection; IoT/RFID; blockchain traceability; cybersecurity architecture | Extensive security AI use associated with $2.2M lower average breach cost (IBM, 2024) |
| Logistics processes | Procurement; warehousing; transportation; distribution/order-to-cash | Process-specific risk typology (Table 4) |
| Risk governance | Identification; assessment; monitoring; mitigation, aligned to ISO 31000 / COSO ERM | COSO (2017); ISO 31000:2018 |

## 5. Discussion

The primary contribution of this study is the development of an integrated socio-technical framework that combines governance mechanisms, technological controls, organizational processes, and human factors into a unified model for financial risk management and fraud prevention in integrated logistics chains.

The proposed framework advances the argument that financial risk management and fraud prevention in integrated logistics chains should be designed as a socio-technical problem from the outset, rather than treated as a technology-procurement exercise supplemented after the fact with compliance training. This position is consistent with, and extends, the original STS proposition of joint optimization (Trist & Emery, 1960) into a digital supply chain context characterized by inter-organizational dependency, high transaction velocity and an expanding attack surface (Ivanov, 2021).

Several implications follow. First, investment decisions regarding fraud - detection technology (e.g., AI-based transaction monitoring, blockchain provenance systems) should be evaluated not only on technical performance metrics but on their compatibility with existing organizational roles, incentive structures and reporting channels - a direct application of Cherns' (1976) STS design principles. A highly capable anomaly - detection system that generates alerts nobody is trained, incentivized or empowered to act upon will not reduce realized losses, regardless of its technical sophistication. Second, the finding that 68% of confirmed breaches involve a non - malicious human element (Verizon, 2024) suggests that technical controls should be designed with human-factors principles in mind - for example, reducing the cognitive burden of security decisions at the point of transaction - rather than assuming that awareness training alone will offset design weaknesses. Third, because vendor and third-party breaches are among the costliest and slowest to resolve (IBM, 2024, 2025), the framework implies that risk governance activities cannot be confined to a single organization's boundary; procurement contracts, vendor onboarding and shared monitoring arrangements become extensions of the technical and social subsystems across the entire chain.

The framework is also complementary to, rather than a replacement for, established governance standards. ISO 31000:2018 and the COSO (2017) ERM framework already provide generic risk-management processes; the contribution of the STS lens is to make explicit the joint, rather than sequential or additive, design of social and technical controls within those processes, and to anchor that design specifically in the process architecture of integrated logistics chains.

Unlike previous studies that primarily examine technological controls or governance mechanisms independently, this study proposes an integrated socio-technical framework that simultaneously incorporates organizational, technological, procedural, and governance dimensions.

### 5.1 Managerial Implications

- Fraud-detection technology investments should be paired with role redesign, training and incentive alignment at the point of implementation, not as a subsequent phase.
- Whistleblower and tip-based reporting channels should be maintained and promoted as a primary control, given their demonstrated detection effectiveness (ACFE, 2024).
- Vendor and third-party risk management should be treated as a joint social-technical extension of the organization's own control environment, reflecting the elevated cost and duration of third-party breaches (IBM, 2024).

- Security and fraud-awareness training should specifically address the speed at which human error can be exploited, given evidence of sub-30-second phishing susceptibility windows (Verizon, 2024).

### 5.2 Limitations

As a conceptual paper, this study has not empirically tested the proposed framework against primary data from logistics organizations; the framework is grounded in secondary industry data (ACFE, IBM, Verizon) and established theory rather than original fieldwork. The industry statistics cited are also not logistics - specific in all cases - the ACFE, IBM and Verizon studies span multiple industries - and should be interpreted as indicative benchmarks rather than sector-precise estimates. Future empirical work, discussed in Section 7, is required to validate the framework's constructs and relationships within logistics settings specifically.

## 6. Illustrative Application to Integrated Logistics Chain Operations

To illustrate the practical application of the framework, consider a stylized integrated logistics chain spanning procurement of raw materials, third-party warehousing, multimodal transportation and distribution to retail or industrial customers. At the procurement stage, the social subsystem would be operationalized through documented conflict-of-interest disclosures, rotation of procurement staff across supplier relationships, and mandatory two-person authorization above a defined transaction threshold, while the technical subsystem would be operationalized through ERP - embedded three-way matching (purchase order, goods receipt, invoice) and AI-based duplicate - invoice detection. Given that the ACFE (2024) identifies corruption as present in 48% of all occupational fraud cases and billing schemes as among the highest-risk asset-misappropriation sub-schemes, this combination directly targets the process stage and risk category with the greatest empirical exposure.

At the warehousing stage, IoT - enabled RFID tagging and automated cycle counting constitute the technical subsystem response to inventory shrinkage and phantom-stock risk, while the social subsystem response includes segregation between staff who record inventory movements and staff who have physical custody of goods - a classic internal-control principle reinforced by the ACFE's (2024) finding that weak or overridden internal controls were associated with more than half of all occupational fraud cases. At the transportation stage, telematics and GPS-based route verification address freight fraud and fictitious delivery claims technically, while carrier vetting, background checks and fuel-card policy enforcement address the same risks socially. At the distribution and order-to-cash stage - where business email compromise and invoice-redirection fraud have grown into a leading cyber-enabled financial risk - the technical subsystem includes email authentication protocols (e.g., DMARC, SPF, DKIM) and payment-verification systems, while the social subsystem includes mandatory callback verification of any changed banking details, directly addressing the type of scheme implicated in the elevated cost of phishing - initiated breaches reported by IBM (2024, 2025).

This illustrative application demonstrates that the proposed framework is operational rather than purely abstract: each logistics process stage can be mapped to a specific, evidence-grounded pairing of social and technical controls, embedded within the continuous risk - governance cycle of identification, assessment, monitoring and mitigation described in Section 4.4.

## 7. Limitations and Future Research Agenda

This paper is conceptual in nature and is subject to the limitations inherent to that method: the framework synthesizes theory and secondary industry data rather than primary empirical evidence collected from integrated logistics chain organizations. Several avenues for future empirical research follow directly from this limitation.

- Survey-based validation: Large-sample surveys of logistics and supply chain risk, finance and compliance professionals could test the relative explanatory power of social-subsystem, technical - subsystem and governance variables in predicting realized fraud losses or breach costs, using constructs derived from the framework in Table 5.
- Comparative case studies: In - depth case studies of logistics organizations that have experienced significant fraud or breach events, contrasted with matched organizations that have not, could examine whether the joint alignment of social and technical controls (rather than the presence of either alone) differentiates outcomes.
- Longitudinal analysis: Given that median fraud losses increased 24% between the ACFE's 2022 and 2024 studies despite a stable average detection time of approximately 12 months (ACFE, 2024),

- Sector - and process-specific studies: Because the statistics used in this paper are drawn from multi-industry studies, future research should develop logistics - and process-specific benchmarks (e.g., freight fraud incidence, warehousing shrinkage rates) to refine the risk typology presented in Table 4.
- Cross-organizational governance mechanisms: Given the elevated cost and duration of vendor and third-party breaches (IBM, 2024, 2025)

Mixed-methods designs combining quantitative survey data with qualitative case analysis are likely to be particularly well suited to testing a framework whose central claim - that joint optimization outperforms either social or technical optimization alone - is inherently interactional and difficult to capture through purely quantitative or purely qualitative methods in isolation.

## 8. Conclusions

This paper has argued that financial risk management and fraud prevention in integrated logistics chains should be approached through the lens of Socio-Technical Systems theory, integrating social, technical, process and governance dimensions rather than relying on technology deployment alone. The evidence reviewed - a typical revenue loss to occupational fraud of approximately 5% (ACFE, 2024), a global average data breach cost of USD 4.88 million with vendor and third - party breaches among the costliest and slowest-resolving categories (IBM, 2024, 2025), and a non-malicious human element present in 68% of confirmed data breaches (Verizon, 2024) - collectively supports the proposition that resilience against financial risk and fraud in modern, digitally enabled logistics chains depends on the joint optimization of people, technology, process and governance.

The proposed STS conceptual framework offers logistics and supply chain organizations a structured basis for aligning fraud-detection technology investment with organizational design, training and incentive structures, and offers researchers a set of testable constructs for future empirical validation. As integrated logistics chains continue to digitize and as the financial stakes of fraud and cyber risk continue to rise, an explicitly socio-technical approach - rather than a purely technical or purely organizational one - is likely to represent a more durable basis for resilience.

The proposed framework extends the existing literature by integrating financial risk management, fraud prevention, organizational governance, and socio-technical systems theory into a unified conceptual model applicable to digitally connected logistics environments.

From a practical perspective, the proposed framework can assist logistics organizations in designing integrated governance systems capable of reducing fraud exposure while improving organizational resilience in increasingly digital supply chain environments.

Future empirical validation across different logistics sectors will further assess the applicability and robustness of the proposed framework.

## References


[1] Association of Certified Fraud Examiners (ACFE). (2024). Occupational Fraud 2024: A Report to the Nations (13th ed.). Austin, TX: ACFE.

[2] Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. Interacting with Computers, 23(1), 4–17.

[3] Cherns, A. (1976). The principles of sociotechnical design. Human Relations, 29(8), 783–792.

[4] Christopher, M. (2023). Logistics & Supply Chain Management (6th ed.). Harlow: Pearson Education.

[5] Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2017). Enterprise Risk Management — Integrating with Strategy and Performance.

[6] IBM Security. (2024). Cost of a Data Breach Report 2024. Armonk, NY: IBM Corporation, in partnership with the Ponemon Institute.

[7] IBM Security. (2025). Cost of a Data Breach Report 2025. Armonk, NY: IBM Corporation, in partnership with the Ponemon Institute.

[8] International Organization for Standardization (ISO). (2018). ISO 31000:2018 Risk Management — Guidelines. Geneva: ISO.

[9] Ivanov, D. (2021). Digital Supply Chain Management and Technology to Improve Resilience by Building and Using End-to-End Visibility During the COVID-19 Pandemic. IEEE Transactions on Engineering Management.

[10] Trist, E. L., & Emery, F. E. (1960). Socio-Technical Systems. In Management Science, Models and Techniques (Vol. 2). London: Tavistock Institute of Human Relations.

[11] Verizon. (2024). 2024 Data Breach Investigations Report. Basking Ridge, NJ: Verizon Business.