Journal of Finance - Marketing Research; Special Issue 1; 2026
e-ISSN: 3030-430X
DOI: https://doi.org/10.52932/jfmr.v17i1enes

Journal of Finance - Marketing Research
http://jfm.edu.vn

CYBERSECURITY RISK GOVERNANCE AND FRAUD MANAGEMENT IN INVOICE-TAX DATA SHARING FOR CREDIT SCORING: A TRIPARTITE FRAMEWORK FOR VIET NAM

Truong Thanh Cong[1*], Vu Thi Thanh Huong[1], Nguyen Van Phong[1], Le Cong Thanh[2]

[1]University of Finance - Marketing, Vietnam

[2]Saigon Bank for Industry and Trade, Viet Nam

ARTICLE INFO

DOI:
10.52932/jfmr.v17i1enes.1522

Received:
February 26, 2026
Accepted:
April 09, 2026
Published:
August 08, 2026

Keywords:
Credit scoring,
Cybersecurity governance,
Invoice fraud,
Tax data sharing,
Third-Party risk management

Article classification:
Conceptual paper

JEL Codes:
G32, G38, K24, L86, O38

ABSTRACT

Purpose – Decree 70/2025 and Decree 94/2025 in Vietnam established a tripartite data pipeline that shares real-time e-invoices from the General Department of Taxation (GDT) to credit institutions for enterprise credit scoring. Prevailing Third-Party Risk Management (TPRM) frameworks, including DORA, NIST CSF 2.0, the FSB TPRM Toolkit, and BIS BCBS d577, address private-sector relationships and do not cover risks specific to government-as-data-provider architectures, such as non-terminability, monopoly provision, and accountability fragmentation. No existing TPRM standard accounts for a government agency serving as the sole, non-terminable data source in private-sector credit scoring, leaving this configuration in a governance vacuum.

Method – Using Design Science Research (DSR) methodology, we conducted a comparative regulatory analysis of Decree 94/2025 and constructed a threat taxonomy. Building on this taxonomy, we designed the Tripartite Governance Framework for Vietnam (TGF-VN v1.0) through analogical transfer from HIPAA, Singapore's MyInfo, and the SWIFT Customer Security Controls Framework.

Findings – Our analysis identifies 10 regulatory gaps in areas including API security, accountability, and breach notification, and 16 threat vectors across API, transmission, and invoice-fraud layers. TGF-VN v1.0 comprises 12 integrated controls that address these exposures

*Corresponding author:
Email: ttcong@ufm.edu.vn

and provide the structural basis for the State Bank of Vietnam's (SBV) implementing circulars.

Originality – The framework also yields a replicable governance template for similar government-data-sharing initiatives across ASEAN and emerging markets.

1. Introduction

In mid-2025, two Vietnamese decrees created a data pipeline with no precedent in the country's financial regulatory history. Decree 70/2025/NĐ-CP (effective 1 June 2025) mandated real-time e-invoice connectivity between all enterprises with annual revenue exceeding VND 1 billion and the General Department of Taxation central system. Decree 94/2025/NĐ-CP (effective 1 July 2025) authorized credit institutions and fintech companies to use alternative data (including GDT invoice-tax records) within a regulatory sandbox for credit scoring. Together, the two decrees established a tripartite pipeline: GDT supplies invoice data via API, financial institutions (FIs) and fintechs consume it for credit assessment, and borrowing enterprises are scored on the basis of their tax transaction history.

The economic rationale is compelling. Vietnam's SME sector accounts for more than 97% of enterprises. Access to finance remains a major business constraint for SMEs; the World Bank–IFC estimate Vietnam's MSME financing gap at USD 48.6 billion; the gap across Southeast Asia is substantial, with Indonesia alone accounting for about USD 234.7 billion (IFC & SME Finance Forum, 2025). A real-time, government-authenticated invoice dataset, if made accessible to credit decision-makers, could substantially reduce information asymmetry and extend credit to firms currently excluded from the formal financial system.

The pipeline operates in a risk governance vacuum. Four existing international frameworks share a common structural assumption: the Digital Operational Resilience Act (DORA, EU Regulation 2022/2554), the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 (2024), the Financial Stability Board TPRM Toolkit (2023), and the Basel Committee's Principles for Third-Party Risk (BIS BCBS d577, 2023) all presuppose that the third-party providing data or services is a private entity. The FSB Toolkit (2023, p. 4) defines its scope as "arrangements between a financial institution and a third-party service provider (private entity)" and explicitly excludes government bodies from its coverage.

This gap has operational consequences. When GDT occupies the role of central data provider to dozens of participating institutions simultaneously, attack surface concentrates in a way that private-sector TPRM does not anticipate: a successful compromise of the GDT API disrupts all downstream FIs simultaneously, a systemic dependency analogous in mechanism to the SolarWinds supply-chain attack (Peisert et al., 2021). Invoice data that directly influences credit decisions also creates new fraud incentives (invoice inflation, ghost invoices, and temporal manipulation) for which no detection taxonomy has been systematically developed. A search of Scopus, Web of Science, and IEEE Xplore in April 2026 returned no peer-reviewed paper constructing a risk taxonomy or governance framework for this configuration.

This paper addresses the governance vacuum through three contributions.

First, it delivers a compliance matrix comparing Decree 94/2025 against four international frameworks across 12 pre-specified control criteria, using a codebook with operational definitions and inter-rater reliability of Cohen's Kappa >= 0.70.

Second, it synthesizes a threat taxonomy for the tripartite pipeline covering at least 15 discrete threat vectors from at least 20 sources, organized into four clusters: API layer attacks, data integrity threats, invoice fraud in credit scoring, and governance accountability gaps.

Third, it proposes TGF-VN v1.0, a three-layer governance artifact constructed through a DSR-informed design process using analogical transfer from HIPAA, Singapore's MyInfo platform, and the SWIFT Customer Security Controls Framework. TGF-VN v1.0 contains 12 specific controls and is the first framework designed for the government-as-data-provider configuration in a financial credit scoring context.

The findings carry immediate policy relevance. Vietnam's FIs and fintechs are currently designing system architectures for Decree 94/2025 compliance; governance structures decided in this window are costly to retrofit.

2. Background and research context

2.1. Third-Party risk management in financial services

Third-party risk management (TPRM) for financial institutions has been codified in a set of authoritative documents produced between 2023 and 2025. The FSB Final Report (2023) provides the most comprehensive toolkit, covering vendor due diligence, contractual requirements, concentration risk, and exit planning. BIS BCBS d577 (2023) articulates ten principles for sound third-party risk management, emphasizing board-level oversight and operational continuity. The OCC/FDIC/Federal Reserve Interagency Guidance (2023) adds granular implementation requirements for the US context. The Digital Operational Resilience Act (DORA, EU Regulation 2022/2554), applicable since January 2025, extends TPRM requirements to ICT third-party dependencies and mandates resilience testing across the EU financial sector.

Despite the breadth of these frameworks, all share a definitional boundary that excludes the present study's context. Each framework presupposes that the third party is a private entity whose relationship with the financial institution is governed by commercial contract. The FSB Toolkit (2023, p. 4) states this explicitly. This boundary has two practical consequences when a government agency is the data provider: financial institutions cannot terminate the relationship when risk materialises, and liability allocation follows public law rather than commercial contract. Neither condition is addressed by existing TPRM frameworks.

2.2. API security in open banking

Research on API security in financial services accelerated after the introduction of Payment Services Directive 2 (PSD2) (EU) and the UK Open Banking Standard. Ojehomon et al. (2026) combine System Dynamics, Agent-Based Modelling, and Monte Carlo simulation to model API-enabled financial crime in open banking, finding that rate-limit controls and anomaly detection reduce operational tail losses by 20–30%. A formal security analysis of open banking API protocols (Modesti et al., 2025) identifies structural vulnerabilities in token management and OAuth 2.0 authorization flows that persist despite API versioning. The Open Web Application Security Project (OWASP) API Security Top 10 (2023) catalogs the most prevalent API attack vectors (broken object-level authorization, excessive data exposure, and injection) across financial and non-financial contexts.

All published API security research in financial services assumes a bank-to-bank or bank-to-third-party bilateral structure. No study addresses the centralized government-to-many-FI configuration created by Decree 94/2025, in which a single government API simultaneously serves dozens of financial institutions. This architectural difference matters: bilateral API security analysis focuses on pairwise protocol vulnerabilities, whereas one-to-many government API creates systemic concentration risk that bilateral models do not capture.

2.3. Fraud invoice in credit scoring contexts

Fraud detection research in financial services has grown considerably since 2019. A systematic review covering 57 studies published between 2019 and 2024 found that deep learning models (CNNs, LSTMs, transformers) are applied across credit card transactions, insurance claims, and financial statement audits, but no established taxonomy includes invoice manipulation fraud in a credit scoring context as a distinct category (Chen et al., 2025). A parallel synthesis in *Humanities and Social Sciences Communications* (Hernandez Aros et al., 2024) confirms this gap across 104 studies: credit card fraud detection and behavioral fraud dominate, while invoice fraud in credit scoring is absent.

The Decree 94/2025 pipeline merges two previously separate research domains: invoice records generated for tax compliance purposes now directly influence credit access, creating fraud incentives and attack vectors that neither research tradition has examined.

2.4. Analogical Governance Cases

Three governance systems from adjacent domains share structural features with the GDT–FI tripartite pipeline: a government or quasi-government entity serves as the primary data source; at least three parties hold defined roles; the data is sensitive; and participants cannot unilaterally exit the arrangement.

HIPAA's Business Associate Agreement (BAA) framework governs the tripartite relationship between covered healthcare entities, business associates, and patients. The BAA imposes explicit data-use limitations on downstream handlers and establishes contractual accountability allocation that follows data across organizational boundaries. Singapore's MyInfo platform enables government-authenticated personal data to flow to licensed financial institutions via a consent-based pull mechanism, with mandatory audit trails logged at the government API layer. The SWIFT Customer Security Controls Framework (CSCF) establishes mandatory baseline security controls and self-attestation requirements for all participants in the SWIFT messaging network – participants cannot exit the network without ceasing operations, a structural analogue to the non-terminability of the GDT–FI relationship.

These cases have been used as sources for analogical transfer in DSR-based governance research (Peffers et al., 2007). The structural (rather than superficial) similarities justify extracting design principles that can be translated to the Vietnam context.

2.5. The Vietnamese regulatory context

Decree 70/2025: E-Invoice infrastructure

Decree 70/2025/NĐ-CP, effective 1 June 2025, completed Vietnam's transition to mandatory real-time e-invoice connectivity. All business households and individuals with annual revenue exceeding VND 1 billion, alongside enterprises selling directly to consumers (retail, hospitality, entertainment), must issue e-invoices generated from cash registers connected directly to the tax authorities.

By mid-2025, the GDT platform collected invoice records from approximately 900,000 registered enterprises. Invoice data includes counterparty identification, transaction amount, date, commodity classification,

and tax category, a data profile rich enough to reconstruct enterprise cash flow, trade relationships, and seasonal revenue patterns.

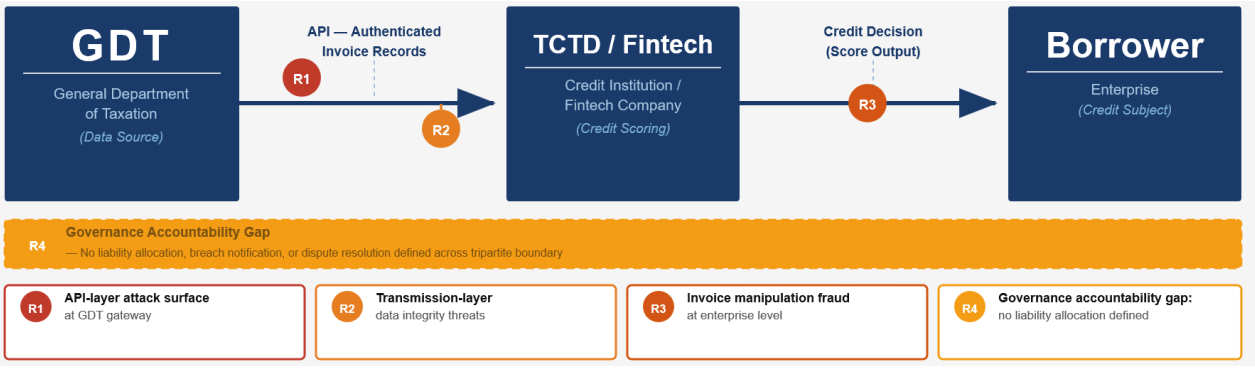
Decree 94/2025: Fintech credit scoring sandbox

Decree 94/2025/NĐ-CP, effective 1 July 2025, established Vietnam's controlled regulatory sandbox for fintech activities, prioritizing credit scoring as a primary use case. Through this mechanism, participating credit institutions and fintech companies are permitted to pilot credit assessment models using alternative data inputs, including GDT invoice-tax data (subject to enterprise consent).

While the State Bank of Vietnam recently issued Circular 19/2026/TT-NHNN (May 2026) to decentralize administrative supervision of sandbox participants, a comprehensive technical framework specifying security controls and data standardization for these high-risk integrations remains absent, a critical regulatory gap this paper addresses

Tripartite risk topology

The two decrees together define a three-node pipeline with four risk exposure points, illustrated in Figure 1.



Notes: *R1: API-layer attack surface at the GDT gateway; R2: transmission-layer data integrity threats; R3: invoice fraud at enterprise level prior to credit scoring; R4: governance accountability gap across the three parties.*

Figure 1. GDT–FI–Borrower tripartite pipeline and four-point risk topology (R1–R4)

Risk point R1 represents the concentrated attack surface at the GDT API. Risk point R2 covers data integrity threats during transit. Risk point R3 covers invoice manipulation fraud at the enterprise level. Risk point R4 represents the structural accountability gap: no regulation currently specifies liability allocation, breach notification obligations, or dispute resolution when a breach or fraud event spans the tripartite boundary.

2.6. Research gap synthesis

Table 1 maps existing research streams against the characteristics of the present study's problem. No existing work covers the combination of government data provider, tripartite relationship, credit scoring purpose, and emerging market regulatory context.

Table 1. Research gap matrix

Characteristic	TPRM frameworks (FSB/BIS/DORA)	API security (Ojehomon 2026; OWASP)	Invoice fraud detection	Credit scoring (Alt data)	This study
Government as data provider	✗	✗	Partial	✗	✓
Tripartite relationship	✗	✗	✗	✗	✓
Credit scoring purpose	✗	✗	✗	✓	✓
Emerging market context	✗	✗	✗	Partial	✓
Governance framework artifact	✓ (private sector)	✗	✗	✗	✓ (government provider)
Threat taxonomy	Partial	Partial	✗	✗	✓

The gap is structural, not incremental. Existing TPRM frameworks cannot be extended to cover the government-as-data-provider configuration by adding a module, because the foundational assumptions, commercial relationship, contractual exit, private-sector accountability, do not transfer. A purpose-built framework is required.

3. Methodology

3.1. Research Design: DSR-Informed conceptual framework approach

This study adopts a Design Science Research informed approach as its overarching paradigm, combined with Comparative Regulatory Analysis and focused literature synthesis as the data collection methods. DSR was established within the Information Systems discipline to generate prescriptive knowledge through the creation and evaluation of artifacts (frameworks, models, or constructs) that address problems where adequate solutions do not yet exist (Hevner et al., 2004). The paradigm differs from behavioral science in that its primary contribution is a purposefully designed artifact, not an empirically tested hypothesis.

Three characteristics of the current problem justify this choice. The GDT–FI pipeline created by Decree 94/2025 began operating in mid-2025; transaction-level security logs from the government API are non-public, ruling out empirical data collection. The research objective is explicitly prescriptive: because existing TPRM frameworks do not address the government-as-data-provider configuration, the task is to design a viable solution. DSR is also well-established in information security governance research (Peffers et al., 2007).

The study executes the Problem Identification and Design stages of the DSR cycle described by Hevner et al. (2004). Problem Identification is addressed through regulatory analysis (Section 3.2) and threat synthesis (Section 3.3). Design is executed through analogical transfer (Section 3.4). The Demonstration and Evaluation stages are contingent on access to fintech sandbox participants under Decree 94/2025 and are deferred to subsequent work; the present paper is accordingly framed as a DSR-informed conceptual framework proposal rather than a complete DSR study.

3.2. Phase 1: Comparative regulatory analysis

The first phase constructs a compliance matrix mapping Decree 94/2025 against four international frameworks: DORA (EU Regulation 2022/2554), NIST CSF 2.0, the FSB TPRM Toolkit (2023), and BIS BCBS d577 (2023). These four frameworks represent the most authoritative current standards for operational risk governance in financial services.

The analysis uses a codebook of 12 control criteria, each defined operationally before coding begins. Operational definitions specify observable indicators for three score levels: full compliance (2), partial compliance (1), and absence (0). Pre-specifying indicators reduces post-hoc judgment and supports independent replication.

Two coders apply the codebook to all five documents independently. The second coder, an independent researcher with expertise in financial regulation and information security governance from a separate institution, coded all 12 criteria without prior knowledge of the lead author's scores; no supervisory or collaborative relationship existed between the coders, and no conflicts of interest were declared. Inter-rater reliability is measured using Cohen's Kappa, with $\kappa \geq 0.70$ established a priori as the minimum acceptable agreement threshold. Disagreements are resolved through structured discussion. A criterion is flagged as a regulatory gap when Decree 94/2025 scores lower than at least two of the four international frameworks on the same criterion.

3.3. Phase 2: Threat synthesis

The second phase produces a threat taxonomy through a focused literature review and thematic synthesis. A focused review is appropriate because the objective is conceptual synthesis across disciplinary boundaries, not a census of all studies on a given topic (Snyder, 2019).

The search covers three databases: IEEE Xplore, ScienceDirect, and ENISA threat landscape reports. Sources meet inclusion criteria if they (a) address API security, data pipeline integrity, or fraud in a financial services context; (b) were published between 2019 and 2026; and (c) contain threat descriptions applicable to a government-to-financial-institution data model. Studies addressing general cybersecurity without reference to financial data pipelines are excluded.

Thematic synthesis groups identified threats by attack vector and target pipeline layer. The taxonomy documents at least 15 discrete threat vectors from at least 20 sources, organized into four clusters. Severity ratings follow ENISA classification conventions. Note that Cluster C3 (invoice fraud in credit scoring) draws on a preprint systematic review (Chen et al., 2025) and one practitioner typology report (EPC, 2023); peer-reviewed empirical validation of these specific vectors in credit scoring contexts is a priority for future work, and C3 confidence levels should be interpreted accordingly.

3.4. Phase 3: Framework design via analogical transfer

The third phase produces the governance framework artifact through analogical transfer (Gentner, 1983). Three source domains are selected on the basis of structural similarity across four dimensions: a government or heavily regulated entity serves as the data source; the relationship involves at least three parties; the data exchanged is sensitive; and participants cannot unilaterally exit the arrangement. Table 1 presents the formal basis mapping for each domain.

HIPAA's Business Associate Agreement contributes to the principle of explicit data-use limitation and contractual accountability allocation for downstream data handlers. Singapore's MyInfo platform contributes

consent-based data pull with mandatory audit trails at the government API layer. The SWIFT CSCF contributes mandatory baseline controls and self-attestation requirements for participants who cannot exit the network.

The design process follows three steps: design principles are extracted from each source domain as abstract statements independent of domain-specific language; each principle is translated into a concrete governance control for the Vietnam context; and controls are organized into a three-layer architecture (Governance, Control, Operational). The resulting artifact is TGF-VN v1.0.

4. Results

4.1. Compliance Matrix: Decree 94/2025 versus international frameworks

Table 3 presents the compliance matrix. Scores reflect mean ratings across two independent coders (Cohen's Kappa = 0.74, exceeding the pre-specified threshold of 0.70). A criterion is flagged as a regulatory gap (G) when Decree 94/2025 scores lower than at least two of the four international frameworks on the same criterion. *(see Appendix 1 online)*

Decree 94/2025 scores 5 out of a possible 24 points. Ten of 12 criteria are flagged as regulatory gaps. The largest deficits fall on API Security (score 0), Accountability (score 0), Monitoring (score 0), Breach Notification (score 0), and Independent Assessment (score 0). Two criteria are not flagged: Data Retention (aligned via reference to Decree 13/2023) and Consent Management (partially addressed but without a specified technical consent architecture).

4.2. Threat taxonomy for the tripartite pipeline

The focused literature review identified 23 relevant sources meeting all inclusion criteria. Thematic synthesis produced 16 discrete threat vectors in four clusters. *(see Appendix 2 online).* C3 vectors are drawn from a review (Chen et al., 2025) and a practitioner typology (EPC, 2023). Peer-reviewed empirical validation of these vectors in credit scoring contexts is a research priority.

Cluster C3 (Invoice Fraud) is the most novel contribution of the taxonomy: no prior taxonomy catalogues these vectors in a credit scoring context. Clusters C1 and C2 extend established API and transmission security taxonomies to government-to-many-FI architecture. Cluster C4 reflects findings from the compliance matrix: because Decree 94/2025 scores zero on Accountability and Breach Notification, the pipeline currently has no defined response chain when a governance event occurs.

4.3. TGF-VN v1.0: The tripartite governance framework

TGF-VN v1.0 organizes 12 specific controls across three layers, designed to close the ten regulatory gaps identified in Table 3 while addressing all 16 threat vectors. TGF-VN v1.0 three-layer governance architecture with 12 controls distributed across Governance, Control, and Operational layers *(see Appendix 3 online).* Control labels align with Appendix 4 *(see Appendix 4 online)*. The three Governance controls draw primarily from HIPAA's Business Associate Agreement model. The API and Data Integrity controls adapt Singapore's MyInfo technical architecture to the GDT context. Compliance controls adopt SWIFT CSCF's mandatory self-attestation model.

4.4. Discussion

Why TPRM fails for government-as-data-providers

The compliance matrix result (Decree 94/2025 scoring 5 out of 24 against an average of 19.5 for the four international frameworks) reflects a genuine structural absence rather than regulatory immaturity. Three structural

characteristics of the government-as-data-provider relationship fall outside the boundary conditions of existing TPRM frameworks.

The first is non-terminability. TPRM frameworks are built on the assumption that a financial institution can exit a third-party relationship when risk exceeds tolerance. The FSB Toolkit (2023) devotes an entire section to exit planning and run-off provisions. For a fintech participating in the Decree 94/2025 sandbox, exit from the GDT data relationship means ceasing the credit scoring business entirely; no alternative government-authenticated invoice source exists.

The second is the absence of competitive alternatives. Private-sector TPRM assumes that a financial institution can replace a problematic vendor with a competing supplier. GDT has no competitor. Standard contract negotiation tools, performance penalties, service level agreements with exit clauses, multi-vendor diversification, cannot be applied.

The third is accountability fragmentation across public and private law. When a breach occurs in a commercial third-party relationship, liability allocation follows contract law. When the data source is a government agency, liability spans public administrative law (governing GDT), banking regulation (governing FIs), and private consumer protection law (governing borrower data rights). No single legal instrument currently coordinates these three regimes in Vietnam, which explains why Accountability and Breach Notification both score zero in the compliance matrix.

Generalisable design principles from analogical transfer

Each analogical domain contributes one design principle that maps to one structural characteristic. Together, the three principles provide coverage across all three failure modes, and the controls they generate do not overlap.

HIPAA's Business Associate Agreement addresses non-terminability by shifting governance logic from exit rights to data-use limitation. Financial institutions cannot reverse their dependence on GDT data once integration begins; governance therefore focuses on constraining downstream use rather than enabling exit. This principle generates the accountability clause template (G-3) and the data retention and deletion control (C-6).

Singapore's MyInfo addresses the monopoly-provider problem by placing the primary technical control at the government API layer rather than at the consuming institution. Three controls follow from this principle: mTLS authentication (C-1), digital signature at GDT origin (C-4), and immutable API-layer audit trail (C-5).

SWIFT CSCF addresses accountability fragmentation through mandatory self-attestation for all network participants, independent of jurisdiction or legal form. Controls C-10, C-11, and C-12 adopt this approach, specifying reporting timelines and assessment requirements that apply regardless of which legal regime governs each party. The three principles are architecturally independent: each targets a distinct failure mode, and none of their controls overlap.

5. Conclusion and implications

5.1. Conclusion

We examined the risk governance problem that arises when a government agency, rather than a private vendor, occupies the data-provider role in a multi-party financial data pipeline. Decrees 70/2025 and 94/2025, which established a GDT–FI–Borrower tripartite pipeline for invoice-tax credit scoring in Vietnam, ground three contributions that build sequentially: from gap identification to threat documentation, to governance design.

The compliance matrix shows that Decree 94/2025 addresses only 5 of 24 control points relative to four international frameworks, leaving 10 criteria as regulatory gaps. API Security, Accountability, and Breach Notification each score zero, confirming that sandbox authorization has not been accompanied by the technical security specification required to operate it safely.

These gaps motivate the threat taxonomy, which documents 16 vectors across four clusters. Cluster C3 (Invoice Fraud in Credit Scoring) constitutes the first systematic documentation of fraud vectors specific to the government-invoice-to-credit-scoring pipeline. C3 vectors derive from practitioner and preprint sources and require peer-reviewed empirical validation.

TGF-VN v1.0 is the first governance framework designed for the government-as-data-provider configuration. Its 12 controls derive from structural analogies in healthcare data governance, government identity infrastructure, and financial messaging network security. Three structural characteristics (non-terminability, monopoly provision, and cross-law accountability fragmentation) are the determinants of TPRM failure in this configuration. These findings carry immediate implications for both financial institutions designing GDT integrations and regulators drafting the sandbox's implementing circular.

5.2. Practical significance

TGF-VN v1.0 and the compliance matrix address two audiences: financial institutions making architecture decisions now, and SBV drafting the implementing circular for Decree 94/2025.

Institutions and fintechs entering the sandbox are making architecture decisions that will determine the security posture of their GDT integrations for years. TGF-VN v1.0 provides a control checklist these institutions can apply during system design.

For SBV, the compliance matrix offers a gap analysis against which the implementing circular can be written. The four provisions in Section 5.3 are regulatory measures that close the largest gaps.

The three structural characteristics identified as TPRM failure determinants are not unique to Vietnam. Government open-data initiatives in comparable ASEAN and emerging-market contexts face structurally similar configurations. Design principles extracted from HIPAA, MyInfo, and SWIFT CSCF apply to any jurisdiction implementing a government-data-to-financial-institution pipeline, and TGF-VN v1.0 can be adapted to those regulatory contexts.

5.3. Policy Implications for Vietnam

Four provisions in TGF-VN v1.0 require regulatory action by SBV:

First, the implementing circular for Decree 94/2025 should specify API security standards as a mandatory condition of sandbox participation, covering mTLS authentication, OAuth 2.0 with PKCE, and per-institution rate limits (controls C-1 and C-2).

Second, SBV should establish a tripartite accountability template governing the GDT–FI relationship for all sandbox participants, specifying liability allocation and a mandatory breach notification chain (controls G-1, G-2, G-3).

Third, GDT should implement origin-signing of invoice records at the API gateway, making record tampering detectable at the FI ingestion point (control C-4).

Fourth, SBV should require annual self-attestation and biennial independent assessment including resilience testing exercises, creating a governance feedback loop independent of breach events (control C-12).

5.4. Limitations and future research

This study delivers the Problem Identification and Design stages of the DSR cycle. Demonstration (deploying TGF-VN v1.0 in a participating fintech) and Evaluation (measuring control effectiveness against actual threat data) are deferred to subsequent research. The threat taxonomy is constructed from published sources and ENISA reports; Cluster C3 vectors should be treated as practitioner-evidenced hypotheses pending peer-reviewed empirical validation. The compliance matrix reflects the text of Decree 94/2025 as published; any implementing circular issued by SBV after the research window could modify several gap scores. Future work should apply TGF-VN v1.0 across ASEAN jurisdictions with comparable government data-sharing initiatives and develop a machine-learning detection model for the invoice fraud vectors in Cluster C3.

Funding Acknowledgment

This research was funded by the University of Finance - Marketing.

Data Availability

Data available upon reasonable request (contact corresponding author).

AI Usage Statement

This paper used ChatGPT to support grammar correction and structural editing. All idea development, literature review, data collection, analysis, and interpretation were carried out entirely by the authors, who take full responsibility for the study.

References

Bank for International Settlements (2023). *Principles for the sound management of third-party risk* (BCBS d577). BIS. https://www.bis.org/bcbs/publ/d577.pdf

Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review. *arXiv*, 2502.00201. https://doi.org/10.48550/arXiv.2502.00201

European Parliament (2025). *Digital Operational Resilience Act (DORA)*, EU Regulation 2022/2554. https://www.digital-operational-resilience-act.com/

European Payments Council (2023). *2023 payments threats and fraud trends report*. EPC.

Financial Stability Board (2023). *Final report: Enhancing third-party risk management and oversight — A toolkit for financial institutions and financial authorities*. FSB. https://www.fsb.org/2023/12/

Gentner, D. (1983). Structure-mapping: A theoretical framework for analogy. *Cognitive Science*, *7*(2), 155–170. https://doi.org/10.1207/s15516709cog0702_3

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., Moreno Hernandez, J. J., & Rodríguez Barrero, M. S. (2024). Financial fraud detection through the application of machine learning techniques: A literature review. *Humanities and Social Sciences Communications*, *11*(1), 1–22. https://doi.org/10.1057/s41599-024-03606-0

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105. https://dl.acm.org/doi/10.5555/2017212.2017217

IFC & SME Finance Forum (2025). *MSME Finance Gap: An Updated Estimation and Evolution of the MSME Finance Gap in Emerging Markets and Developing Economies.* https://www.smefinanceforum.org/data-sites/msme-finance-gap

Modesti, P., Freitas, L., Shotomiwa, Q., & Almehrej, A. (2025). Security analysis of the open banking account and transaction API protocol. *Cyber Security and Applications*. https://doi.org/10.1016/j.csa.2025.100097

NIST (2024). *Cybersecurity framework 2.0* (NIST.CSWP.29). https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

OCC/FDIC/Federal Reserve (2023). *Interagency guidance on third-party relationships: Risk management.* https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html

OWASP (2023). *API security top 10*. Open Web Application Security Project.

Ojehomon, O. G., Cichorska, J., & Michnik, J. (2026). Cyber Risk Management of API-Enabled Financial Crime in Open Banking Services. *Entropy, 28*(2), 163. https://doi.org/10.3390/e28020163

Peisert, S., Schneier, B., Okhravi, H., Massacci, F., Benzel, T., Landwehr, C., Mannan, M., Mirkovic, J., Prakash, A., & Michael, J. B. (2021). Perspectives on the SolarWinds incident. *IEEE Security & Privacy, 19*(2), 7–13. https://doi.org/10.1109/MSEC.2021.3051235

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039