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, Viet Nam

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

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

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

DOI: 10.52932/jfmr.v17i1enes.1522

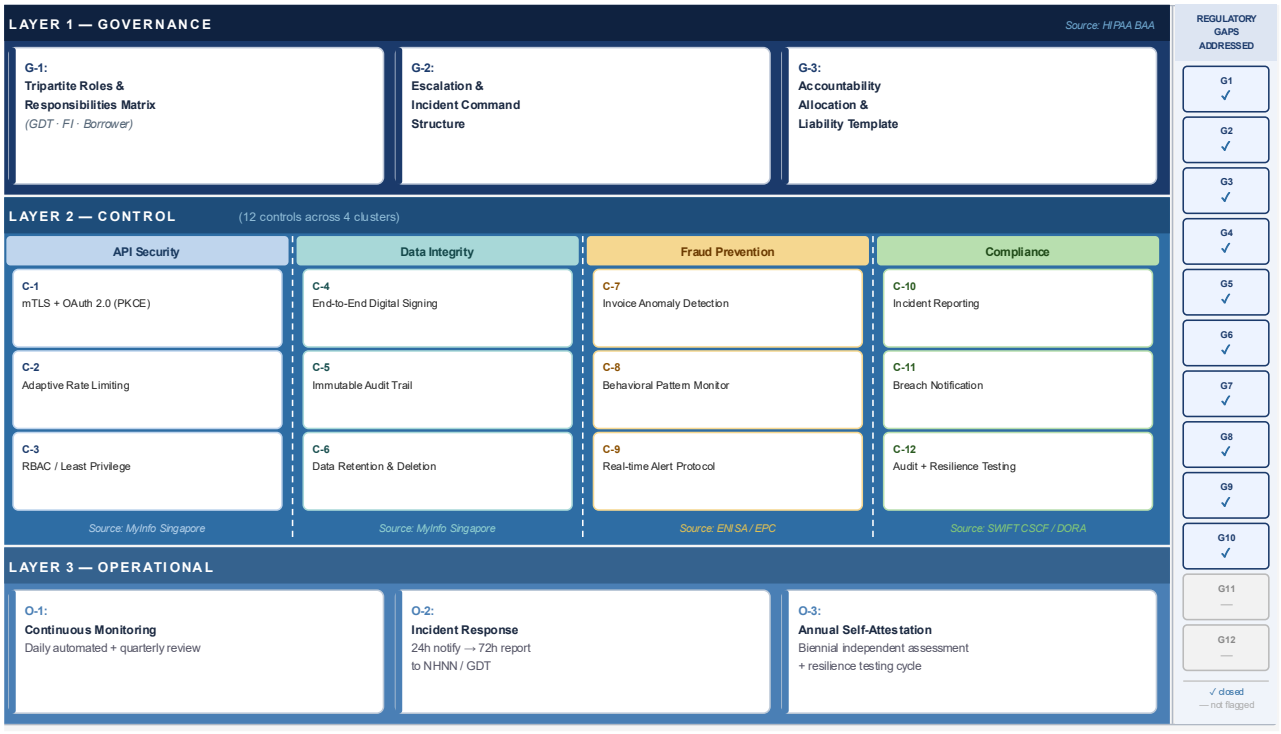
Appendix 1. Compliance matrix Decree 94/2025 vs. international frameworks (0–2 scale)

#	Control Criterion	DORA	NIST CSF 2.0	FSB Toolkit	BIS d577	Decree 94/2025	Gap?
1	API Security	2	2	1	1	0	**G**
2	Data Integrity	2	2	2	2	1	**G**
3	Incident Reporting	2	2	2	2	1	**G**
4	Third-party Audit	2	1	2	2	0	**G**
5	Resilience Testing	2	2	1	1	0	**G**
6	Data Retention	1	1	2	1	1	—
7	Accountability	2	1	2	2	0	**G**
8	Consent Management	1	1	0	0	1	—
9	Access Control	2	2	2	2	1	**G**
10	Monitoring	2	2	2	1	0	**G**
11	Breach Notification	2	1	2	2	0	**G**
12	Independent Assessment	2	1	2	2	0	**G**

Appendix 2. Threat taxonomy: GDT–FI–Borrower pipeline

Cluster	#	Threat Vector	Risk Node	Severity	Primary Source(s)
C1: API layer attacks	1	Broken object-level authorization (API data leakage)	R1	High	OWASP (2023)
	2	API credential theft / token replay	R1	High	Modesti et al. (2025)
	3	Excessive data exposure via unfiltered API responses	R1	High	OWASP (2023)
	4	Rate-limit bypass leading to bulk data extraction	R1	High	Ojehomon et al. (2026)
	5	Injection attacks on API query parameters	R1	Medium	OWASP (2023)
C2: Data integrity threats	6	Man-in-the-middle interception during transmission	R2	High	Modesti et al. (2025)
	7	Replay attack using captured invoice records	R2	High	ENISA (2024)
	8	Hash/checksum bypass — undetected payload modification	R2	Medium	ENISA (2024)
	9	Metadata manipulation (timestamp, counterparty ID)	R2	Medium	ENISA (2024)
C3: Invoice fraud in credit scoring †	10	Invoice value inflation prior to credit application	R3	High	Chen et al. (2025); EPC (2023)
	11	Ghost invoice fabrication (non-existent transactions)	R3	High	Chen et al. (2025)
	12	Circular invoicing to inflate apparent revenue	R3	High	EPC (2023)
	13	Temporal manipulation (concentrate invoices pre-application)	R3	Medium	Chen et al. (2025)
	14	Counterparty collusion (coordinated invoice inflation)	R3	High	EPC (2023)
C4: Governance accountability gaps	15	Unresolved liability when breach spans GDT–FI boundary	R4	High	FSB (2023); BIS d577
	16	Absence of breach notification chain for tripartite pipeline	R4	High	DORA (2025); FSB (2023)

Appendix 3. TGF-VN v1.0 three-layer governance architecture



Appendix 4. TGF-VN v1.0 controls — DSR design principles, sources, and gap coverage

Control	Description	DSR design principle	Analogical source	Gaps addressed
G-1	Tripartite roles matrix: GDT (data custodian), FI (data processor), Borrower (data subject) with defined obligations	Data-use limitation as substitute for exit rights	HIPAA BAA	Gap 7 (Accountability)
G-2	Escalation structure: incident command chain with primary contacts at GDT, SBV, and each participating FI	Mandatory cross-party notification above jurisdictional law	SWIFT CSCF	Gap 11 (Breach Notification)
G-3	Liability clause template for GDT–FI data processing agreements	Data-use limitation as substitute for exit rights	HIPAA BAA	Gap 7 (Accountability)
C-1	Mutual TLS authentication and OAuth 2.0 with PKCE for all GDT API connections	Government-layer technical control for monopoly providers	MyInfo Singapore	Gap 1 (API Security)
C-2	Adaptive rate limiting: per-institution quotas, burst detection, automatic throttling	Government-layer technical control for monopoly providers	Ozoemena et al. (2026)	Gap 1 (API Security)
C-3	Role-based access control at GDT API gateway: least-privilege data scoping per institution	Government-layer technical control for monopoly providers	NIST CSF 2.0	Gap 9 (Access Control)
C-4	Digital signature on all invoice records at GDT origin; signature verification required at FI ingestion	Government-layer technical control for monopoly providers	MyInfo Singapore	Gap 2 (Data Integrity)
C-5	Immutable audit trail at GDT API layer logging all data access events with institution ID, timestamp, and data scope	Government-layer technical control for monopoly providers	MyInfo Singapore	Gap 10 (Monitoring)
C-6	Data retention and secure deletion: FI-held invoice data for credit scoring retained maximum 5 years, then certified deletion	Data-use limitation as substitute for exit rights	HIPAA / DORA	Gap 6 (Data Retention)
C-7	Invoice anomaly detection: statistical threshold model flagging outlier invoice patterns (value, frequency, counterparty concentration)	Government-layer technical control for monopoly providers	Chen et al. (2025)	Gap 10 (Monitoring); C3 threats
C-8	Behavioral pattern monitoring: cross-institution detection of circular invoicing and coordinated inflation patterns	Government-layer technical control for monopoly providers	EPC (2023)	C3 threats

Control	Description	DSR design principle	Analogical source	Gaps addressed
C-9	Real-time alert protocol: anomalies above defined thresholds trigger mandatory review within 48 hours	Mandatory attestation above jurisdictional law	SWIFT CSCF	Gap 10 (Monitoring)
C-10	Incident reporting: internal report to institution Chief Information Security Officer (CISO) within 4 hours; report to SBV within 24 hours	Mandatory attestation above jurisdictional law	DORA	Gap 3 (Incident Reporting)
C-11	Breach notification: affected borrowers notified within 72 hours of confirmed breach; GDT and SBV notified simultaneously	Mandatory attestation above jurisdictional law	DORA / GDPR	Gap 11 (Breach Notification)
C-12	Independent assessment: annual self-attestation against published control checklist; biennial external audit; biennial resilience testing exercise against simulated API disruption scenarios	Mandatory attestation above jurisdictional law	SWIFT CSCF	Gap 4 (Third-party Audit); Gap 5 (Resilience Testing); Gap 12 (Independent Assessment)

Note on Gap 5 coverage: C-12 incorporates resilience testing as an explicit component of the biennial independent assessment cycle. Sandbox participants are required to conduct and document simulated disruption exercises targeting the GDT API dependency (e.g., GDT API unavailability, mass credential revocation), with results submitted to SBV alongside the audit report. This addresses Gap 5 (Resilience Testing) without requiring a separate control.