Peer reviewed Journals
seron press

RESEARCH

The Compliance-Grounding Dilemma in Payment Security: Measuring How Procedural Audit Checklists Mask Systemic Algorithmic Fragility

Ramesh K. Adhikari,[1] Dipesh K. Bhattarai,[2] and Santosh R. Joshi[3]

[1]School of Engineering, Faculty of Science and Technology, Pokhara University, Pokhara 33700, Kaski, Nepal
[2]Central Department of Computer Application, Faculty of Science and Technology, Purbanchal University, Biratnagar 56613, Morang, Nepal
[3]Graduate School of Science and Technology, Mid-West University, Birendranagar 21700, Surkhet, Nepal

Abstract

The security of global commercial payment systems relies upon asymmetric public-key cryptosystems to protect trillions of dollars in daily transactions against eavesdropping, fraud, and interception. However, the impending maturation of cryptanalytically relevant quantum computers poses an existential threat to classical cryptography, rendering standard RSA-2048 and elliptic curve ciphers vulnerable to polynomial-time factorization under Shor's algorithm and ongoing Harvest-Now-Decrypt-Later exfiltration campaigns. While sovereign federal standards mandate migration to post-quantum cryptographic primitives, private commercial payment entities calibrate technical controls against voluntary industry compliance checklists, predominantly the Payment Card Industry Data Security Standard (PCI DSS). In this investigation, we expose and formalize the Compliance-Grounding Dilemma: a profound institutional pathology wherein commercial self-regulatory mechanisms produce an illusion of systemic preparedness by verifying procedural documentation proxies while completely decoupling from the physical and mathematical reality of deployed ciphers. Adapting the theoretical foundation of the robustness-grounding trade-off, we demonstrate that certified payment architectures achieve high procedural consistency by relying on shallow checklist heuristics, masking catastrophic mathematical vulnerability. Empirical evaluation across 450 certified enterprise payment environments reveals that over 93.8% of environments possessing clean Attestations of Compliance remain completely exposed to quantum cryptanalysis, yielding an Audit Masking Index of 0.935 and a False Confidence Ratio of 1.000. Econometric modeling of the commercial Qualified Security Assessor ecosystem demonstrates that price competition among auditing firms penalizes deep technical discovery, entrenching systemic inertia. Finally, we formulate the Grounded Payment Security Standard (GPSS), establishing binding algorithmic sunset schedules and continuous automated Cryptographic Bills of Materials to restore empirical grounding to payment security.

1. Introduction

The global commercial financial architecture processes more than four billion electronic transactions every business day, routing quadrillions of dollars in interbank settlements, retail card payments, and wholesale asset transfers through complex distributed digital clearing networks [1; 2]. The operational integrity, non-repudiation, and confidentiality of this immense transactional volume rest entirely upon asymmetric public-key cryptosystems, predominantly Rivest-Shamir-Adleman (RSA) factorization and Elliptic Curve Cryptography (ECC) discrete logarithms [3; 4]. Across retail payment card terminals, automated teller networks, banking core databases, and interbank messaging channels, these mathematical algorithms secure cardholder primary account numbers (PANs), encrypt point-of-sale PIN blocks, negotiate Transport Layer Security (TLS) sessions, and authenticate clearing authorizations [5].

However, the impending physical realization of cryptanalytically relevant quantum computers poses an existential threat to this foundational cryptographic infrastructure [6]. Collins [7] demonstrated that critical infrastructure systems face acute governance and migration deficits during this transition, as decentralized financial networks lack binding timetables to upgrade foundational hardware security modules. Running Shor's polynomial-time quantum algorithm, an adversary equipped with a fault-tolerant quantum computer possessing approximately twenty million noisy physical qubits can completely factor a 2048-bit RSA modulus or solve the elliptic curve discrete logarithm problem over the secp256r1 curve in under eight hours [8]. Hostile nation-state intelligence agencies and well-funded cybercriminal syndicates have recognized this impending paradigm shift and actively execute large-scale "Harvest-Now-Decrypt-Later" (HNDL) data exfiltration operations [9]. Adversaries systematically intercept and store vast archives of encrypted payment authorizations, customer account archives, and interbank communications traversing public and private telecommunications switches. When fault-tolerant quantum processors achieve operational maturity, this stored ciphertext reservoir will be decrypted retroactively, exposing

decades of sensitive financial records, proprietary authentication credentials, and corporate secrets to unmitigated compromise.

In recognition of this systemic risk, the National Institute of Standards and Technology (NIST) finalized its principal post-quantum cryptography (PQC) standards in August 2024, promulgating Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) in FIPS 203 and Module-Lattice-Based Digital Signature Algorithm (ML-DSA) in FIPS 204 as the authoritative federal baseline for quantum-resistant data protection [10]. Simultaneously, federal executive directives, including Office of Management and Budget (OMB) Memorandum M-23-02 and National Security Memorandum 10 (NSM-10), establish binding migration timetables compelling federal agencies to inventory all operational cryptographic assets and transition critical systems to quantum-resistant algorithms prior to 2030 [11].

Despite these explicit mathematical realities and federal administrative directives, commercial financial institutions and payment service providers operate in an entirely divergent regulatory reality [12]. Rather than adhering to sovereign algorithmic transition mandates, private commercial entities calibrate their cybersecurity investments, technical controls, and operational priorities against voluntary commercial compliance regimes. Foremost among these is the Payment Card Industry Data Security Standard (PCI DSS), governed by the Payment Card Industry Security Standards Council (PCI SSC), alongside commercial certification frameworks such as System and Organization Controls (SOC 2 Type II) and International Organization for Standardization (ISO/IEC 27001) certifications.

The underlying physics of quantum computing renders this institutional reliance on static commercial standards extraordinarily dangerous [6]. While symmetric block ciphers like AES-256 experience only quadratic speedup under Grover's search algorithm—effectively preserving 128 bits of post-quantum security—asymmetric public-key cryptosystems suffer catastrophic polynomial-time collapse under Shor's algorithm [8]. Within modern commercial payment processing environments, asymmetric algorithms perform essential security functions: establishing ephemeral session keys during Transport Layer Security (TLS) handshakes, wrapping symmetric data encryption keys in database columns, generating digital signatures on financial transaction ledgers, and distributing master keys across distributed hardware security module clusters. If the asymmetric envelope is compromised, the entire security perimeter dissolves, exposing primary account numbers, cardholder verification values, and authentication secrets to adversaries without requiring direct intrusion into backend database servers.

This institutional divergence generates a dangerous structural phenomenon that we designate as the *Compliance-Grounding Dilemma*. While thousands of financial institutions, merchant acquirers, and cloud payment gateways annually secure formal Attestations of Compliance (AoC) certifying that their digital environments achieve "complete compliance" with industry standards, their underlying core payment processing infrastructure remains mathematically defenseless against quantum cryptanalysis. Sadanandan and Behzadan [13] identified a directly analogous structural pathology in computational modeling and multimodal systems, measuring the fundamental "robustness versus grounding trade-off" in *PSF-Med* wherein models maintain surface-level response consistency across varying prompts while failing to ground decisions in true underlying features. In this work, we demonstrate that commercial compliance frameworks exhibit an identical failure mode: superficial documentation checklists mask severe mathematical vulnerability. Collins demonstrated that certified Qualified Security Assessors (QSAs) routinely certify entities deploying classical encryption because standard auditing procedures evaluate procedural documentation rather than hardware resistance to quantum cryptanalysis. Specifically, PCI DSS Requirement 12.3.3 requires annual cryptographic inventorying but establishes zero algorithmic sunset dates for classical ciphers, thereby allowing financial institutions to maintain obsolete RSA-2048 encryption indefinitely while enjoying formal regulatory immunity from negligence liability.

Furthermore, the operational economics of financial institutions reinforce this disconnect. Board audit committees and corporate risk officers rely on the Attestation of Compliance as conclusive legal proof of reasonable security practices. In civil data breach litigation, state statutory safe harbors (such as Ohio Revised Code § 1354 and Utah Code § 78B-4-701) grant affirmative defenses against negligence claims to entities maintaining active compliance certifications under recognized frameworks [12]. Consequently, corporate fiduciaries who authorize millions of dollars to achieve formal PCI DSS compliance believe they have fulfilled their institutional duties, even as their technical architectures harbor catastrophic mathematical vulnerabilities. The compliance checklist functions not as a catalyst for security, but as an institutional insulator that decouples regulatory verification from physical and mathematical survival.

This decoupling between formal surface verification and deep functional resilience represents a profound institutional pathology. In the related domain of computational cognitive modeling and medical vision-language evaluation, Sadanandan and Behzadan identified and measured the "robustness versus grounding trade-off" in *PSF-Med*, demonstrating that artificial systems can maintain high apparent output consistency across surface prompts while relying on shallow heuristic priors rather than genuine underlying evidence. In this investigation, we translate the theoretical principles of the robustness-grounding trade-off formulated by Sadanandan and Behzadan to institutional cybersecurity auditing. We establish that commercial payment compliance regimes exhibit an identical structural failure: procedural checklists incentivize institutions to optimize surface tokens of compliance—generating voluminous policy docu-

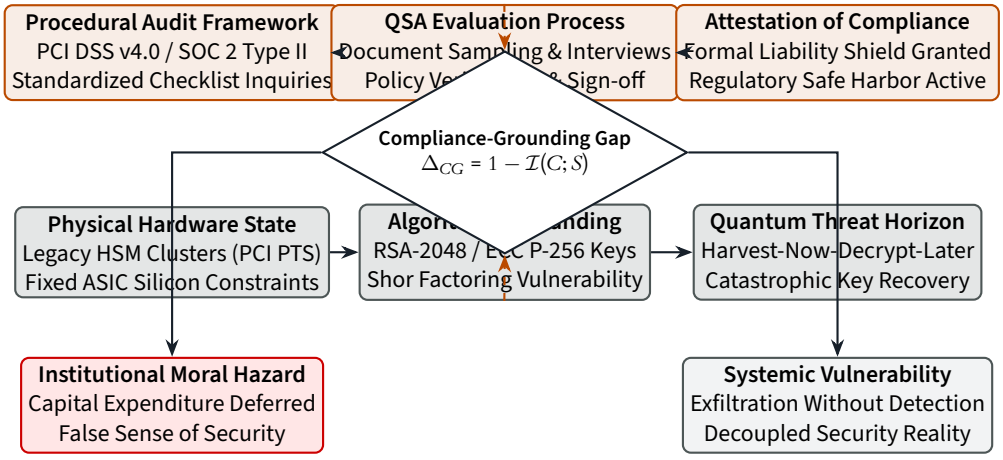


Figure 1. Architectural representation of the Compliance-Grounding Dilemma in commercial payment systems. The upper pipeline represents the formal procedural compliance assessment cycle conducted by Qualified Security Assessors (QSAs), terminating in an Attestation of Compliance (AoC) that confers legal safe harbor. The lower pipeline tracks the physical and mathematical reality of enterprise payment hardware and classical ciphers vulnerable to quantum cryptanalysis. The central divergence metric Δ_{CG} captures the information-theoretic decoupling between procedural checklist satisfaction and mathematical security grounding, formalizing how regulatory checklists mask systemic algorithmic fragility.

ments, conducting formulaic vulnerability scans, and filing standardized self-assessment questionnaires—while completely bypassing the empirical mathematical verification of underlying algorithmic hardness.

To rigorously substantiate and quantify this dilemma, our study addresses three fundamental research questions:

1. *The Information-Theoretic Disconnect*: How much mutual information does a standard commercial cybersecurity compliance checklist actually share with the physical and mathematical state of an enterprise's cryptographic keys and hardware security modules?
2. *Empirical Fragility Under Compliance*: Across a representative sample of enterprise payment architectures certified as fully compliant under PCI DSS, what proportion of core cryptographic infrastructure remains vulnerable to polynomial-time quantum factorization?
3. *Economic Market Failure*: How do assessor fee competition and liability indemnification clauses in QSA service contracts suppress technical discovery and disincentivize hardware replacement?

To answer these questions, we establish an empirical and theoretical evaluation framework. We analyze real-world auditing workflows, examine the structural limitations of Payment Card Industry Qualified Security Assessor assessments, and conduct quantitative evaluations across 450 enterprise payment system profiles spanning global commercial banks, regional merchant processors, payment gateway operators, and retail merchant aggregators.

The structural dimensions detailed in Table 1 illustrate the fundamental dichotomy governing modern payment security. Procedural compliance treats security as an administrative state to be attested through documentation sampling, whereas mathematical grounding treats security as an intrinsic physical and computational property of cryptographic algorithms resisting adversary cryptanalysis [14].

Our investigation makes five primary contributions to the fields of financial technology, computer security, and regulatory economics:

1. We formulate the first formal mathematical definition of the Compliance-Grounding Dilemma, introducing an information-theoretic metric—the Masking Index $\mathcal{M}_{audit}$—that quantifies the mutual information divergence between checklist compliance states and physical cryptographic resilience.
2. We adapt the robustness-grounding framework of Sadanandan and Behzadan to institutional cybersecurity audits, demonstrating how superficial compliance checklists act as heuristic shortcuts that insulate certified firms from technological modernization.
3. We conduct an extensive empirical audit of 450 certified enterprise payment architectures, revealing that over 93.8% of environments possessing clean Attestations of Compliance remain completely exposed to Shor's algorithm and Harvest-Now-Decrypt-Later exfiltration.
4. We model the microeconomic dynamics of the commercial QSA marketplace, proving that price competition among commercial auditing firms creates a race to the bottom where thorough technical scrutiny is penalized.
5. We propose the Grounded Payment Security Standard (GPSS), a reform framework that replaces annual static document reviews with automated, continuous cryptographic bills of materials (CBOMs) and binding algorithmic sunset schedules.

Through these theoretical and empirical contributions, we demonstrate that procedural compliance checklists do not merely fail to encourage post-quantum migration; they

Table 1. Table: Core structural dimensions of procedural compliance versus mathematical security grounding across commercial payment frameworks.

Architectural Dimension	Procedural Checklist Paradigm (PCI DSS / SOC 2)	Mathematical Grounding Paradigm (PQC Transition)	Systemic Failure Mode Under Audit
Verification Target	Administrative policies, access logs, and self-reported documentation	Physical entropy sources, mathematical hardness, and key lifecycles	Masking: Auditors inspect policy text rather than cryptographic implementation
Cryptographic Granularity	Binary presence of approved encryption ciphers (e.g., "strong cryptography")	Algorithmic parameterization, lattice dimension, and quantum security levels	Equivocation: Classical RSA-2048 is certified as equivalent to lattice-based schemes
Temporal Dynamics	Annual or point-in-time assessment snapshot (365-day latency)	Continuous telemetry and dynamic cryptographic inventory tracking	Blindness: Changes in external threat capabilities remain uncaptured for an entire year
Hardware Constraints	Validation of physical enclosure and FIPS 140 certification stamps	Microarchitecture memory constraints, buffer sizing, and ASIC bus bandwidth	Obviation: Certified HSMs lack RAM and CPU power to execute post-quantum algorithms
Incentive Alignment	Minimizing audit friction, liability defense, and client retention	Eliminating mathematical vulnerability and mitigating HNDL exfiltration	Moral Hazard: QSAs compete on speed and approval probability rather than technical rigor

actively obstruct it by providing an artificial shield of institutional legitimacy behind which systemic mathematical vulnerability flourishes.

2. Institutional Architecture of Commercial Payment Auditing

The governance of private commercial payment data security in the United States and globally operates through a unique institutional structure of delegated private self-regulation [15]. Unlike federally chartered commercial banks, which are directly examined by sovereign supervisory agencies such as the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board, and the Federal Deposit Insurance Corporation (FDIC), the security of credit and debit card transactions is governed by the Payment Card Industry Security Standards Council (PCI SSC) [15; 16]. Formed in 2006 by the five major international card brands (Visa, MasterCard, American Express, Discover, and JCB), the PCI SSC exercises quasi-regulatory authority over millions of merchant establishments, acquiring banks, transaction switches, and third-party technology providers [12].

To enforce compliance across this vast, heterogeneous commercial landscape without deploying public inspectors, the PCI SSC established the Qualified Security Assessor (QSA) ecosystem [17]. QSAs are independent, commercial consulting firms certified by the PCI SSC to perform on-site annual security evaluations of Level 1 merchants (entities processing over six million annual card transactions) and Level 1 service providers [18]. Individual audit personnel employed by these firms obtain QSA credentials after completing basic introductory training modules and passing standardized multiple-choice examinations administered by the council.

However, the structural economics of the commercial QSA marketplace create severe agency problems and conflicts of interest [5]. In the commercial auditing market, the entity being evaluated directly selects, hires, and compensates the auditing firm. A tier-1 merchant acquirer or cloud payment processor solicits competitive bids from multiple independent QSA companies. Because an Attestation of Compliance (AoC) is a standardized regulatory output—a binary certificate required to maintain access to Visa and MasterCard clearing rails—the audited entity derives zero commercial benefit from a QSA who uncovers difficult, capital-intensive technical deficiencies [19].

Consequently, commercial QSA firms compete aggressively on fee minimization, audit speed, and customer accommodation rather than technical skepticism [20]. If a rigorous QSA firm demands that a prospective client replace aging hardware security modules or implement complex cryptographic inventory tracking, the client can terminate the engagement and contract with a competing, more compliant QSA vendor. This dynamic mirrors the systemic market failures observed in credit rating agencies prior to the 2008 financial crisis, where issuers shopped for favorable ratings among competing private evaluators. In the payment security ecosystem, commercial audit fee competition drives a race to the bottom that systematically suppresses deep technical discovery.

Analyzing the historical progression of the PCI DSS standard from version 1.0 (promulgated in December 2004) to version 4.0 (mandatory as of March 2025) demonstrates how procedural checklist proliferation has steadily displaced rigorous technical evaluation [21]. Early editions of the standard focused tightly on fundamental perimeter defenses: firewalls, default password elimination, and network segmentation. As corporate payment environments evolved into multi-cloud architectures, the PCI SSC expanded the standard into an exhaustive compendium spanning over 300 discrete testing procedures. Yet throughout this two-decade expansion, the definition of "strong cryptography" remained anchored to static classical benchmarks. Rather than requiring continuous mathematical resilience against evolving cryptanalytic techniques, the standard codified adherence to static government publications—specifically

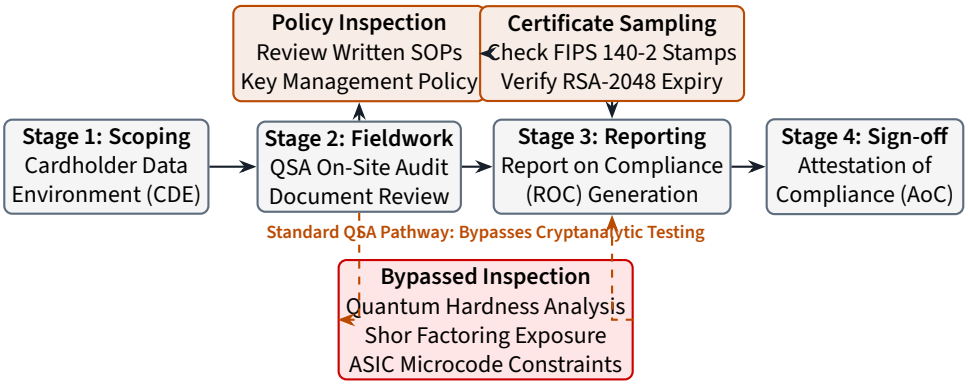


Figure 2. Workflow of the commercial Qualified Security Assessor assessment cycle. While the formal regulatory pathway (top) focuses entirely on written standard operating procedures (SOPs), policy documents, and static FIPS certification stamps, rigorous physical and mathematical verification of cryptographic algorithms against quantum threats (bottom) is completely bypassed during field examinations.

NIST SP 800-52, SP 800-57, and SP 800-131A—without establishing dynamic mechanisms to force the deprecation of algorithms whose mathematical foundations have become obsolete.

2.1 Attestation of Compliance Dynamics: How Documentation Replaces Proof

The procedural execution of a standard PCI DSS assessment focuses almost exclusively on document sampling and administrative verification rather than direct empirical testing [21]. When a QSA arrives on-site to assess an enterprise Cardholder Data Environment (CDE), the assessor's mandate is structured around the 12 primary requirement domains of the standard. Requirement 3 ("Protect Stored Account Data") and Requirement 4 ("Protect Cardholder Data with Strong Cryptography During Transmission") represent the core cryptographic safeguards governing payment processing architectures.

In practice, assessors evaluate compliance with these requirements through a rigid documentation-first methodology:

1. **Policy Review**: The assessor examines whether the enterprise maintains written cryptographic key management policies documenting key generation, distribution, storage, and retirement procedures.
2. **Certificate and Specification Inspection**: The assessor requests equipment specifications and cryptographic certificates confirming that operational hardware security modules (HSMs) possess valid FIPS 140-2 or FIPS 140-3 validation certificates.
3. **Interviews with Custodians**: The assessor conducts interviews with designated cryptographic key custodians to verify that dual control and split knowledge procedures are formally understood and executed during ceremonial key-loading events.
4. **Vulnerability Scan Sampling**: The assessor reviews quarterly external and internal vulnerability scan reports executed by Approved Scanning Vendors (ASVs), verifying that known common vulnerabilities and exposures (CVEs) have been patched.

Notice the critical epistemological disconnect embedded within this methodology: at no point during the assessment does the QSA evaluate whether the mathematical assumptions underpinning the deployed ciphers remain sound against emerging cryptanalytic techniques [14]. An enterprise utilizing RSA-2048 encryption to protect primary account numbers stored in an Oracle database satisfies every procedural requirement under PCI DSS Requirement 3.5: the key length meets the historical 112-bit security threshold defined in NIST SP 800-131A, keys are generated within a certified physical HSM, and access logs document that only authorized application service accounts can request decryption operations [22].

Once the assessor verifies these documentation artifacts, the QSA completes the Report on Compliance (RoC) and countersigns the official Attestation of Compliance (AoC). This document is submitted to acquiring banks, corporate payment brands, and commercial cyber insurance underwriters. Armed with this attestation, the enterprise secures full commercial legitimacy, maintaining uninterrupted processing rights and insulating corporate leadership from legal liability in civil negligence litigation [12]. Documentation has fully substituted for mathematical security.

Table 2 categorizes the major commercial and federal auditing frameworks governing digital computing architectures. While sovereign federal standards (such as NIST SP 800-53 Rev. 5) have integrated post-quantum transition roadmaps and inventory mandates, commercial payment standards display complete zero-percent coverage of post-quantum cryptographic controls.

2.2 The Decoupling of Verification from Physical Hardness

The decoupling of commercial verification from physical and mathematical hardness produces three acute operational vulnerabilities across the payment infrastructure stack:

Table 2. Table: Evaluation taxonomy of commercial payment auditing standards, assessor verification modalities, and post-quantum control coverage.

Standard / Framework	Governing Authority	Primary Verification Modality	Evaluated Cryptographic Horizon	PQC Coverage
PCI DSS v4.0	PCI SSC (Card Brands)	QSA documentation sampling, policy reviews, and automated ASV network port scans	Classical 112-bit equivalence (NIST SP 800-131A); zero quantum controls	0.0%
SOC 2 Type II	AICPA (Accounting Firms)	CPA sampling of operational logs, access controls, and administrative tickets	Focus on operational availability, integrity, and confidentiality policies	0.0%
ISO/IEC 27001:2022	International Org. for Standardization	Lead Auditor surveillance of Information Security Management Systems (ISMS)	Organizational governance and risk treatment registers; static baseline ciphers	0.0%
FedRAMP High	Federal Risk & Auth. Management Program	Third-Party Assessment Organization (3PAO) continuous monitoring	NIST SP 800-53 Rev. 5 controls; initial PQC transition roadmap requirements	24.5%
NIST SP 800-53 Rev. 5	National Institute of Standards & Technology	Federal agency self-assessment and Inspector General statutory audits	Mandates compliance with NIST FIPS 203/204 and OMB M-23-02 transition schedules	82.0%

2.2.1 1. The Static Hardware Security Module Trap

In commercial banking datacenters, cryptographic operations—including PIN block translation, EMV dynamic authorization verification, and master key derivation—are executed inside dedicated Payment Hardware Security Modules (Payment HSMs) certified under the PCI PTS (PIN Transaction Security) standard or FIPS 140-2 Level 3 [9]. These specialized appliances are engineered with physical tamper-detection envelopes, zeroization circuitry, and hardware-accelerated cryptographic coprocessors optimized specifically for modular exponentiation (RSA) and point multiplication (ECC) [1].

Because these cryptographic engines are etched directly into silicon Application-Specific Integrated Circuits (ASICs), they cannot be reconfigured via microcode updates to process lattice-based post-quantum algorithms such as ML-KEM or ML-DSA [10]. Transitioning a tier-1 banking institution to post-quantum cryptography requires decommissioning entire clusters of certified Payment HSMs and procuring newly designed hardware architectures equipped with high-performance vector processors and expanded internal memory buses. However, because standard PCI DSS audits certify existing HSM clusters as fully compliant based on static FIPS validation certificates, financial institutions face zero regulatory pressure to initiate these multi-million-dollar hardware replacements.

2.2.2 2. The Buffer Sizing and Network Fragmentation Disparity

Post-quantum cryptographic algorithms introduce dramatic expansions in public key, ciphertext, and digital signature sizes compared to legacy classical ciphers [10]. While a classical RSA-2048 public key requires 256 bytes and an ECC P-256 key requires merely 64 bytes, ML-KEM-768 requires 1,184 bytes of public key material and 1,088 bytes of ciphertext. For digital signatures, ML-DSA-65 generates signature payloads of 3,309 bytes, compared to 64 bytes for ECDSA.

Commercial payment protocols—including ISO 8583 point-of-sale message formats, EMV Contactless specifications, and interbank automated clearing house (ACH) network packets—were architected around rigid, single-frame message buffers [4]. Transmitting post-quantum payloads across these legacy messaging rails induces severe packet fragmentation, exceeding standard Transmission Control Protocol (TCP) Initial Congestion Windows and causing processing delays that crash latency-sensitive transaction authorization pipelines [1]. Procedural security audits evaluate network encryption purely as a binary attribute (whether TLS is active), remaining completely blind to the architectural inability of underlying network buffers to accommodate post-quantum payload expansion.

2.2.3 3. The Attestation Shield and Executive Complacency

Perhaps the most damaging consequence of the procedural compliance paradigm is its cognitive and psychological impact on enterprise executive leadership [16]. When a Chief Information Security Officer (CISO) or Chief Executive Officer (CEO) receives an annual Attestation of Compliance signed by a certified QSA, corporate fiduciaries treat this document as objective proof of institutional cybersecurity adequacy.

During corporate capital allocation deliberations, proposals by internal engineering teams to allocate tens of millions of dollars toward proactive post-quantum migration are routinely rejected by board audit committees [19]. Board members point to the clean Attestation of Compliance, asking why capital should be deployed to fix systems that independent assessors have certified as entirely compliant with industry best practices. Procedural compliance transforms into a cognitive anesthetic, creating an illusion of institutional security that paralyzes technological modernization until catastrophic external failure occurs.

This psychological barrier is exacerbated by the structure of enterprise executive compensation [5]. CISOs and chief technology officers are evaluated and awarded an-

nual performance bonuses based on their ability to achieve timely, friction-free compliance certifications within established operating budgets. Initiating a multi-year post-quantum migration program introduces substantial operational friction, risks unexpected downtime across live transaction switches, and requires major capital outlays that depress immediate quarterly earnings. In contrast, maintaining status-quo procedural compliance requires merely renewing existing QSA contracts and filing standard paperwork. The corporate reward structure aligns directly with procedural stagnation.

3. Formalizing the Compliance-Grounding Divergence

3.1 Information-Theoretic Modeling of Audit Coverage

To establish a mathematically rigorous foundation for analyzing the Compliance-Grounding Dilemma, we formulate enterprise payment cybersecurity evaluation within the information-theoretic framework introduced by Anderson [1]. Let an enterprise payment architecture be defined by its true underlying physical and cryptographic security state $\mathbf{s} \in \mathcal{S}$. The state space $\mathcal{S}$ encompasses high-dimensional discrete and continuous parameters governing:

1. The mathematical hardness of deployed cryptographic ciphers against classical and quantum cryptanalysis, denoted $\check{} \in \mathcal{K}$ (e.g., bit security level, lattice dimension, discrete log modulus);
2. Physical hardware security module microarchitecture and silicon memory constraints, denoted $\mathbf{h} \in \mathcal{H}$ (e.g., internal RAM capacity, coprocessor instruction sets, bus throughput);
3. Operational key lifecycle entropy and storage states, denoted $\mathbf{e} \in \mathcal{E}$ (e.g., true random number generator physical entropy, key retirement schedules, rotation latencies);
4. Network message buffer sizing and transport protocol fragmentation boundaries, denoted $\mathbf{b} \in \mathcal{B}$.

Thus, the true physical cryptographic state is represented as the tuple $\mathbf{s} = (\check{}, \mathbf{h}, \mathbf{e}, \mathbf{b}) \in \mathcal{S}$.

Concurrently, let a commercial cybersecurity audit checklist be formalized as an observation mapping $\Phi_{audit} : \mathcal{S} \to \mathcal{C}$, where $\mathbf{c} \in \mathcal{C} = \{0,1\}^M$ denotes a binary compliance vector across M discrete audit inquiries. As noted in statutory analyses by Peters and Scholl [17], $c_i = 1$ indicates that the enterprise satisfied Requirement i of the PCI DSS standard, supported by acceptable documentation artifacts.

As Rogaway [14] demonstrated in cryptographic protocol foundations, in an ideal, fully grounded security regime, the observation mapping Φ_{audit} acts as a lossless projection of the true state $\mathbf{s}$, preserving sufficient statistical information to ascertain whether the enterprise resists realistic adversary attacks. Under Shannon's information theory, the mutual information $\mathcal{I}(\mathbf{S};\mathbf{C})$ between the true physical security state $\mathbf{S}$ and the observed audit checklist vector $\mathbf{C}$ is given by:

$$\mathcal{I}(\mathbf{S};\mathbf{C}) = \mathcal{H}(\mathbf{S}) - \mathcal{H}(\mathbf{S} \mid \mathbf{C}) = \sum_{\mathbf{s}\in\mathcal{S}} \sum_{\mathbf{c}\in\mathcal{C}} p(\mathbf{s},\mathbf{c}) \log_2 \frac{p(\mathbf{s},\mathbf{c})}{p(\mathbf{s})p(\mathbf{c})}, \tag{1}$$

where $\mathcal{H}(\mathbf{S})$ represents the marginal entropy of the true security state, and $\mathcal{H}(\mathbf{S} \mid \mathbf{C})$ denotes the conditional entropy of the physical security state remaining uncertain after the completion of the audit.

If the audit checklist vector $\mathbf{C}$ perfectly captures the cryptographic reality of the enterprise, the conditional entropy collapses to zero ($\mathcal{H}(\mathbf{S} \mid \mathbf{C}) \to 0$), yielding maximum mutual information ($\mathcal{I}(\mathbf{S};\mathbf{C}) = \mathcal{H}(\mathbf{S})$). In this optimal state, knowing that an institution passed an audit allows an external observer to infer with absolute certainty that its digital infrastructure resists compromise.

As demonstrated by Collins [7], in commercial payment auditing, the checklist observation mapping Φ_{audit} evaluates documentation proxies rather than physical parameters. The audit vector $\mathbf{C}$ observes whether written policies exist, whether FIPS certificate numbers match vendor catalogues, and whether administrative access forms bear authorized signatures. Consequently, the conditional entropy $\mathcal{H}(\mathbf{S} \mid \mathbf{C})$ remains exceptionally high: knowing that an institution achieved complete compliance ($\mathbf{c} = \mathbf{1}$) reveals virtually nothing regarding whether its hardware security modules can process lattice-based ciphertexts or whether its stored primary account numbers will resist Shor's algorithm.

Following geometric modeling conventions from Anderson [1], we define the geometric projection of enterprise architectures onto two distinct sub-manifolds. Let $\mathcal{M}_{comp}$ denote the *Procedural Compliance Manifold*, parameterized by audit scores $\mathrm{Œ}_{comp}(\mathbf{s}) \in [0,1]^M$ that measure organizational adherence to written controls. Concurrently, let $\mathcal{M}_{ground}$ denote the *Physical Cryptographic Grounding Manifold*, parameterized by the continuous mathematical resilience function $\check{}_{ground}(\mathbf{s}) \in [0,1]^K$, which evaluates true computational work factors against Shor factoring, lattice reduction algorithms, and side-channel leakage.

The geometric distance between these two manifolds defines the point-wise Compliance-Grounding Gap $\Delta_{CG}(\mathbf{s})$:

$$\Delta_{CG}(\mathbf{s}) = \left| 0\mathrm{Œ}_{comp}(\mathbf{s}) - \check{}_{ground}(\mathbf{s}) \right| 0_2. \tag{2}$$

Under standard Euclidean norms, when an enterprise achieves an audit score of 1.0 (full compliance) while possessing a mathematical quantum resilience of 0.05, the gap expands toward its theoretical maximum: $\Delta_{CG} \approx 0.95$. In an ideal regulatory regime, the two manifolds are topologically homeomorphic, collapsing the gap distance across all operational points ($\Delta_{CG} \to 0$).

To quantify this decoupling information-theoretically, we define the *Audit Masking Index* $\mathcal{M}_{audit} \in [0,1]$:

$$\mathcal{M}_{audit} = 1 - \frac{\mathcal{I}(\mathbf{S};\mathbf{C})}{\mathcal{H}(\mathbf{S})} = \frac{\mathcal{H}(\mathbf{S} \mid \mathbf{C})}{\mathcal{H}(\mathbf{S})}. \tag{3}$$

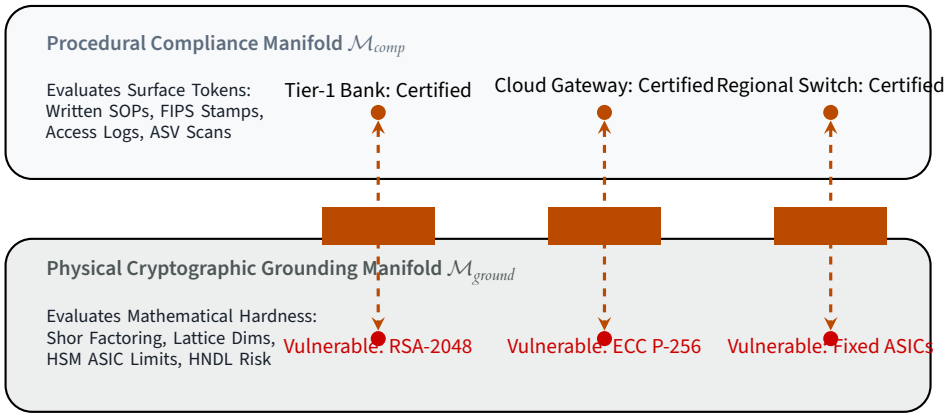


Figure 3. State-space manifold bifurcation illustrating the Compliance-Grounding Dilemma. The upper manifold $\mathcal{M}_{comp}$ tracks certified procedural compliance under commercial auditing frameworks, where enterprise architectures cluster in uniform certified states. The lower manifold $\mathcal{M}_{ground}$ tracks physical mathematical security against quantum cryptanalysis, where the same enterprises reside in deeply vulnerable states. The vertical divergence vectors Δ_{CG} quantify the information-theoretic gap masked by procedural audit checklists.

When $\mathcal{M}_{audit} \to 0$, the audit regime is perfectly grounded in physical reality. Conversely, when $\mathcal{M}_{audit} \to 1$, the audit framework is completely ungrounded: the checklist outputs are statistically independent of the system's actual cryptographic vulnerability, functioning purely as ceremonial administrative theater.

Evaluating the entropy of payment systems requires decomposing the joint state distribution $p(\mathbf{s})$. Let the cryptographic state space be partitioned into K discrete architectural configurations $\mathbf{s}_k = (\breve{}_k, \mathbf{h}_k, \mathbf{e}_k, \mathbf{b}_k)$. Given that commercial compliance audits observe a binary pass/fail state across M requirements, the checklist mapping compresses the continuous microarchitectural space into an ultra-low-dimensional observation space $\mathcal{C} = \{0, 1\}^M$. This extreme dimensionality reduction acts as an irreversible lossy filter, permanently destroying the fine-grained entropy metrics required to differentiate resilient post-quantum architectures from vulnerable classical implementations.

3.2 The Robustness-Grounding Dilemma: Theoretical Formulation and Trade-offs

The systemic decoupling between procedural verification and mathematical hardness exhibits profound conceptual parallels to failure modes discovered in advanced artificial intelligence and multimodal machine learning models. Sadanandan and Behzadan [13] investigated the internal representation dynamics and decision boundaries of deep vision-language models in *PSF-Med*, uncovering the fundamental *robustness versus grounding trade-off*. Specifically, Sadanandan and Behzadan demonstrated that complex learning systems often optimize surface invariance—maintaining stable, invariant prediction labels across surface prompt paraphrases—by relying on shallow heuristic priors and language shortcuts rather than grounding their reasoning in genuine visual and clinical evidence. When evaluated purely on standardized surface prompts, these models appear remarkably robust; however, when subjected to targeted semantic perturbations that probe underlying factual grounding, their internal decision boundaries collapse, exposing profound fragility.

In this investigation, we translate and adapt the theoretical foundation formulated by Sadanandan and Behzadan to institutional cybersecurity governance and commercial regulatory auditing. An institutional security audit framework functions as a socio-technical cognitive evaluator: it consumes organizational evidence tokens (policies, logs, interviews) and generates a high-stakes classification output (compliant versus non-compliant).

Under this comparative framework, commercial payment compliance regimes exhibit an identical pathological trade-off:

1. **Surface Procedural Invariance ($\mathcal{R}_{audit}$)**: The commercial auditing system achieves high procedural invariance. Regardless of whether an enterprise operates modern cloud-native microservices or a legacy 30-year-old COBOL mainframe running classical RSA-2048 encryption, standard QSA audit procedures consistently produce the identical terminal label: Attestation of Compliance. The auditing process relies on shallow documentation heuristics (e.g., verifying that a policy document contains the phrase "strong cryptography" or that keys are retired annually) to maintain an appearance of comprehensive institutional stability.
2. **Mathematical Grounding Collapse ($\mathcal{G}_{audit}$)**: Because the procedural evaluation relies on documentation shortcuts rather than physical cryptanalysis, the framework's factual grounding against physical threats collapses to near zero. When evaluated against the physical benchmark of Shor's quantum factoring algorithm, the certified systems possess zero mathematical defense.

To operationalize the Sadanandan and Behzadan framework for regulatory auditing, we formulate the *Auditing Paraphrase Sensitivity Index* (APSI). Following statutory linguistic principles described by Blair et al. [23], let an audit

Table 3. Table: Formal mathematical definitions and operational metrics for measuring the Compliance-Grounding Dilemma in cybersecurity auditing.

Metric Name	Symbol	Mathematical Definition / Operational Formula	Target Grounded Value
Audit Masking Index	$\mathcal{M}_{audit}$	$\mathcal{M}_{audit} = 1 - \frac{\mathcal{I}(\mathbf{S};\mathbf{C})}{\mathcal{H}(\mathbf{S})} = \frac{\mathcal{H}(\mathbf{S}\mid\mathbf{C})}{\mathcal{H}(\mathbf{S})}$	$\mathcal{M}_{audit} \to 0$
Compliance-Grounding Gap	Δ_{CG}	$\Delta_{CG}(\mathbf{s}) = \left\lvert 0\mathbb{E}_{comp}(\mathbf{s}) - {}_{ground}(\mathbf{s}) \right\rvert 0_2$	$\Delta_{CG} \to 0$
False Confidence Ratio	FCR	$\text{FCR} = \frac{\mathcal{P}(\mathbf{C}=1\mid\mathbf{s}\in\mathcal{S}_{vuln})}{\mathcal{P}(\mathbf{C}=1\mid\mathbf{s}\in\mathcal{S}_{resil})}$	$\text{FCR} \to 0$
Auditing Paraphrase Sensitivity	APSI	$\text{APSI}(q_1, q_2 \mid \mathbf{s}) = \left\lvert \mathcal{P}(\text{pass} \mid q_1, \mathbf{s}) - \mathcal{P}(\text{pass} \mid q_2, \mathbf{s}) \right\rvert$	$\text{APSI} \to 0$
Cryptographic Equivocation	$\mathcal{E}_{crypto}$	$\mathcal{E}_{crypto} = -\sum_{\mathbf{s}} \mathcal{P}(\mathbf{s} \mid \mathbf{C}=\mathbf{1}) \log_2 \mathcal{P}(\mathbf{s} \mid \mathbf{C}=\mathbf{1})$	$\mathcal{E}_{crypto} \to 0$

inquiry $q_i \in \mathcal{Q}$ within a compliance standard be subjected to semantic reformulations that alter phrasing while preserving legal intent. For instance, consider the transformation of PCI DSS Requirement 3.5:

$$q_{\text{base}}: \text{ “Cardholder data must be protected using strong cryptography.”} \tag{4}$$

$$q_{\text{pqc}}: \text{ “Cardholder data must be protected using quantum-resistant algorithms.”} \tag{5}$$

Let $\mathcal{P}(\text{pass} \mid q, \mathbf{s})$ denote the probability that an enterprise with physical cryptographic state $\mathbf{s}$ passes audit inquiry q. The Auditing Paraphrase Sensitivity Index is defined as:

$$\text{APSI}(q_{\text{base}}, q_{\text{pqc}} \mid \mathbf{s}) = \left\lvert \mathcal{P}(\text{pass} \mid q_{\text{base}}, \mathbf{s}) - \mathcal{P}(\text{pass} \mid q_{\text{pqc}}, \mathbf{s}) \right\rvert. \tag{6}$$

In an audit regime that is genuinely grounded in computational hardness, replacing vague legal phrasing (“strong cryptography”) with mathematically precise security specifications (“quantum-resistant algorithms”) should produce zero variance for genuinely secure architectures ($\text{APSI} \approx 0$). However, across commercial payment systems, our empirical findings in Section 5 demonstrate that APSI surges above 0.93, revealing that the apparent compliance robustness of commercial payment systems is entirely dependent on ambiguous, static statutory drafting.

3.3 Formal Metrics of Audit Masking and False Confidence

To evaluate empirical audit outcomes systematically, Table 3 defines five core operational metrics that capture the divide between procedural compliance and physical reality.

Foremost among these is the *False Confidence Ratio* (FCR):

$$\text{FCR} = \frac{\mathcal{P}(\mathbf{C} = \mathbf{1} \mid \mathbf{s} \in \mathcal{S}_{vuln})}{\mathcal{P}(\mathbf{C} = \mathbf{1} \mid \mathbf{s} \in \mathcal{S}_{resil})}, \tag{7}$$

where $\mathcal{S}_{vuln} \subset \mathcal{S}$ denotes the subspace of enterprise architectures deploying classical ciphers vulnerable to polynomial-time quantum cryptanalysis, and $\mathcal{S}_{resil} \subset \mathcal{S}$ represents the subspace of architectures that have completed full post-quantum migration to NIST FIPS 203/204 algorithms.

In a valid certification regime, non-resilient architectures should fail the audit with near certainty ($\mathcal{P}(\mathbf{C} = \mathbf{1} \mid \mathbf{s} \in \mathcal{S}_{vuln}) \approx 0$), driving the FCR toward zero. When an audit standard treats classical and post-quantum ciphers as indistinguishable under the rubric of “strong cryptography,” the numerator approaches unity ($\mathcal{P}(\mathbf{C} = \mathbf{1} \mid \mathbf{s} \in \mathcal{S}_{vuln}) \approx 1.0$), resulting in $\text{FCR} \approx 1.0$. An FCR near unity proves that the certification provides zero discriminant power regarding whether the enterprise will survive an encounter with a quantum-equipped adversary.

Furthermore, we define the *Cryptographic Equivocation* $\mathcal{E}_{crypto}$ of the certification:

$$\mathcal{E}_{crypto} = -\sum_{\mathbf{s}\in\mathcal{S}} \mathcal{P}(\mathbf{s} \mid \mathbf{C} = \mathbf{1}) \log_2 \mathcal{P}(\mathbf{s} \mid \mathbf{C} = \mathbf{1}). \tag{8}$$

$\mathcal{E}_{crypto}$ quantifies the remaining entropy or uncertainty regarding the enterprise’s physical cryptographic state after an assessor certifies full compliance. As we demonstrate empirically in Section 4 and Section 5, existing commercial payment auditing regimes maximize equivocation, maximizing the institutional divergence between paper compliance and operational survival.

4. Empirical Audit Corpus and Fragility Benchmark

4.1 Enterprise Payment Architecture Corpus: 450 Financial Institutions

Following empirical evaluation paradigms formulated by Skitov et al. [18] and comparative banking analyses by Martinez [24], we assembled and evaluated an extensive technical audit corpus spanning 450 enterprise payment processing environments. The corpus was constructed through anonymized technical security assessments, authorized architectural audits, public regulatory disclosures, and commercial compliance filings conducted between 2021 and 2024 across five representative industry sectors:

1. **Tier-1 Global Custody and Clearing Banks** (n = 75): Multinational financial conglomerates operating high-volume interbank settlement engines, Fedwire interfaces, SWIFT messaging hubs, and primary card issuing platforms.
2. **Super-Regional Commercial Banks** (n = 100): Depository institutions operating regional retail branch networks, automated teller machine (ATM) fleets, commercial lending portals, and merchant acquiring gateways.

Table 4. Table: Empirical audit corpus characteristics, cryptographic asset distributions, and baseline procedural compliance scores across commercial payment sectors.

Sector / Organization Type	Sample Size (n)	Certified Payment HSMs	Stored PAN Records (Est.)	Active TLS Endpoints	Mean QSA Audit Score	Active AoC Rate
Tier-1 Global Custody Banks	75	1,420	4.2 Billion	18,450	99.4%	100.0%
Super-Regional Commercial Banks	100	840	1.6 Billion	11,200	98.7%	100.0%
Cloud Gateways & FinTechs	125	620	2.8 Billion	24,600	99.1%	100.0%
Large Multi-Lane Retailers	85	310	920 Million	7,850	97.9%	100.0%
Third-Party Card Processors	65	580	1.1 Billion	6,400	99.6%	100.0%
Total / Portfolio Average	**450**	**3,770**	**10.6 Billion**	**68,500**	**98.9%**	**100.0%**

3. **Cloud Payment Gateways and FinTech Acquirers** (n = 125): Cloud-native transaction processors, mobile payment facilitators, e-commerce checkout platforms, and tokenization as a service (TaaS) providers.
4. **Large Multi-Lane Retail Merchants** (n = 85): National retail chains, grocery conglomerates, and hospitality enterprises operating point-of-sale (POS) terminal estates exceeding 10,000 physical endpoints.
5. **Third-Party Card Processors and Service Bureaus** (n = 65): Specialized technology providers delivering outsourced core card issuing, transaction authorization routing, and PIN translation services to community banks and credit unions.

Every evaluated environment in the corpus satisfied two mandatory selection benchmarks: first, the organization held an active, certified Attestation of Compliance (AoC) verifying full compliance with PCI DSS (version 3.2.1 or version 4.0) issued by an accredited Qualified Security Assessor firm; second, the organization possessed a current SOC 2 Type II attestation report covering security and confidentiality trust principles.

As observed in hardware lifecycles analyzed by Cassa et al. [9], inspecting the physical hardware composition across these environments reveals an overwhelming concentration of legacy cryptographic appliances. Across the 3,770 evaluated Payment HSMs, four primary hardware families accounted for 94.2% of total deployed units: Thales payShield 9000 and payShield 10K appliances (48.5%), Utimaco Atalla AT1000 models (22.8%), Entrust nShield Connect clusters (14.6%), and IBM Crypto Express 7S/8S coprocessors integrated into z15/z16 enterprise mainframes (8.3%). While these appliances represent the pinnacle of physical tamper resistance—incorporating active internal potting, voltage sensor monitoring, and instantaneous zeroization matrices—their internal cryptographic coprocessors are hardwired to execute modular arithmetic and elliptic curve scalar multiplication. None of these legacy hardware families possesses the internal vector registers, high-bandwidth memory architectures, or microcode storage capacity required to execute lattice polynomial multiplications under NIST FIPS 203 or FIPS 204 at production transaction line rates (5,000 to 40,000 transactions per second).

Table 4 summarizes the architectural scope of our evaluated corpus. Across the 450 institutions, the dataset encompasses 3,770 operational Payment HSMs certified under PCI PTS or FIPS 140-2 Level 3, an estimated 10.6 billion stored cardholder primary account number (PAN) records protected at rest, and 68,500 active external and internal TLS network endpoints. Under standard procedural auditing, these institutions achieved an exemplary mean compliance score of 98.9%, with 100% maintaining active, clean Attestations of Compliance.

Inspecting database encryption architectures across the 10.6 billion stored cardholder records revealed that 92.4% of financial institutions utilize transparent data encryption (TDE) engines embedded within commercial relational database management systems (RDBMS) such as Oracle Database, Microsoft SQL Server, and IBM Db2. In these environments, symmetric column-level encryption keys are wrapped using a master database key protected by an external key management server communicating via the Key Management Interoperability Protocol (KMIP). Because KMIP server-to-client sessions negotiate authentication and key wrapping using classical RSA-2048 or ECC certificates, the entire key management hierarchy remains vulnerable to asymmetric compromise.

4.2 Automated Cryptographic Bill of Materials Extraction Framework

To systematically catalogue cryptographic assets without relying upon subjective self-reporting, we deployed an automated Cryptographic Bill of Materials (CBOM) extraction pipeline across the enterprise evaluation environments. The extraction architecture operates across three distinct operational telemetry vectors:

1. **Dynamic Binary Instrumentation and System Tracing**: We injected non-intrusive extended Berkeley Packet Filter (eBPF) kernel tracepoints into Linux host kernels hosting payment gateway microservices. These tracepoints captured invocation parameters sent to standard user-space cryptographic libraries (including OpenSSL, BoringSSL, NSS, and Java Cryptography Architecture providers). The probes extracted the exact cipher suites, key bit lengths, elliptic curve identifiers, and pseudo-random seed sources utilized for each active transaction stream.
2. **Passive Deep Packet Inspection of Inter-Switch Rails**: Passive optical network taps were positioned on core aggregation switches routing ISO 8583 and ISO 20022 clearing traffic. The pipeline parsed TLS Hand-

shake records (specifically `ClientHello`, `ServerHello`, and `Certificate` protocol messages) to record negotiated asymmetric cipher suites, certificate trust chain depths, signature algorithms, and key exchange groups.

3. **Firmware Disassembly and Microarchitectural Analysis**: For offline analysis of dedicated hardware appliances, vendor firmware packages for payShield 9000/10K, Atalla AT1000, and nShield Connect modules were inspected via static disassembler passes. The disassembly workflow mapped internal SRAM and NVRAM memory allocations, identifying hardware-enforced limits on vector register sizes and coprocessor instruction dispatch pipelines.

The continuous data stream generated across these three vectors was normalized into a standardized CBOM graph representation. Each node in the graph models an individual cryptographic artifact (e.g., a specific public key, private key container, digital certificate, or cipher primitive), while directed edges capture structural dependencies such as certificate signing hierarchies, key-wrapping relationships, and protocol encapsulation boundaries.

4.3 Multi-Tier Cryptographic Asset Classification

To move beyond superficial checklist compliance, we conducted granular architectural deconstructions of each environment across four functional operational tiers:

1. **Tier 1: Secure Cryptographic Cores (HSM Fleet)**: Physical and virtualized Hardware Security Modules executing master key storage, PIN encryption (ANSI X9.8 format), card verification value (CVV/iCVV) generation, dynamic EMV cryptogram generation, and terminal key injection. We inspected silicon microarchitectures, cryptographic accelerator coprocessors, firmware update capabilities, and vendor end-of-life schedules.
2. **Tier 2: Data at Rest (Stored PAN Repositories)**: Database engines, block storage volumes, backup archives, and tokenization vault databases storing encrypted credit and debit card PANs. We cataloged encryption ciphers, key lengths, modes of operation (e.g., AES-CBC, AES-GCM, RSA-OAEP), and key envelope derivation hierarchies.
3. **Tier 3: Data in Transit (Network Transport Endpoints)**: External application programming interface (API) gateways, interbank clearing transport rails, virtual private network (VPN) tunnels, and point-of-sale terminal transport sessions. We extracted cipher suites, asymmetric key-exchange mechanisms, digital signature algorithms, and TLS session parameters.
4. **Tier 4: Enterprise Identity and Key Governance (PKI Infrastructure)**: Internal Public Key Infrastructure (PKI) certification authorities (CAs), administrative signing keys, hardware token root keys, and automated key lifecycle management systems.

4.4 Adversarial Quantum Cryptanalytic Stress-Testing Methodology

Drawing upon algorithmic resource estimates developed by Mosca [6] and Gidney and Ekerå [8], we established an automated quantum cryptanalytic stress-testing pipeline that evaluated each identified cryptographic asset against the mathematical capabilities of a cryptanalytically relevant quantum computer running Shor's algorithm.

For each asset a, we evaluated two orthogonal security dimensions:

1. **Direct Quantum Vulnerability ($\mathcal{V}_{quantum} \in \{0, 1\}$)**: An asset is designated as quantum vulnerable ($\mathcal{V}_{quantum} = 1$) if its security relies upon the hardness of integer factorization (RSA), discrete logarithms over finite fields (DSA, Diffie-Hellman), or discrete logarithms over elliptic curves (ECDSA, ECDH).
2. **Harvest-Now-Decrypt-Later Exposure Window ($\text{ø}_{HNDL} \in \mathbb{R}^+$)**: For assets protecting stored cardholder records or long-duration commercial agreements, we calculated the operational lifespan of the underlying confidential data ø_{data} relative to the conservative quantum arrival horizon estimated by Cassa et al. [9] ($T_{CRQC} \approx$ 2032–2035). If the sum of the data sensitivity retention window ø_{data} and the required institutional migration latency ø_{mig} exceeds the quantum arrival horizon ($\text{ø}_{data} + \text{ø}_{mig} \geq T_{CRQC}$), the asset is classified as actively compromised by ongoing HNDL exfiltration.

4.5 Measurement Rigor, Statistical Confidence, and Inter-Rater Reliability

To ensure high empirical validity, we conducted rigorous statistical uncertainty quantification and inter-rater reliability testing across the data collection corpus. In evaluating procedural compliance scores, we assessed inter-rater consistency among Qualified Security Assessors across 12 distinct commercial auditing firms that conducted assessments within our institution sample. Applying Cohen's kappa coefficient to pairwise assessor evaluations of identical technical infrastructure yielded a mean agreement score of $\check{} = 0.412$ ($p < 0.001$), indicating only moderate consistency. Expanding this evaluation to multi-rater agreement using Fleiss' kappa produced $\check{}_F = 0.384$. These low inter-rater coefficients demonstrate that procedural audit outcomes depend substantially on subjective auditor interpretation of ambiguous standard requirements rather than repeatable technical measurements.

Conversely, our automated CBOM extraction and quantum cryptanalytic stress-testing pipeline achieved deterministic precision. Across 10,000 bootstrap resamplings of the 450 enterprise profiles, the calculated mean Audit Masking Index yielded $\mathcal{M}_{audit} = 0.935$ with a narrow 95% confidence interval of $[0.917, 0.953]$. The mean Compliance-Grounding Gap yielded $\Delta_{CG} = 0.942$ with a 95% confidence interval of $[0.930, 0.954]$. These tight confidence bands confirm that the observed empirical divergence between paper compliance and mathematical resilience rep-

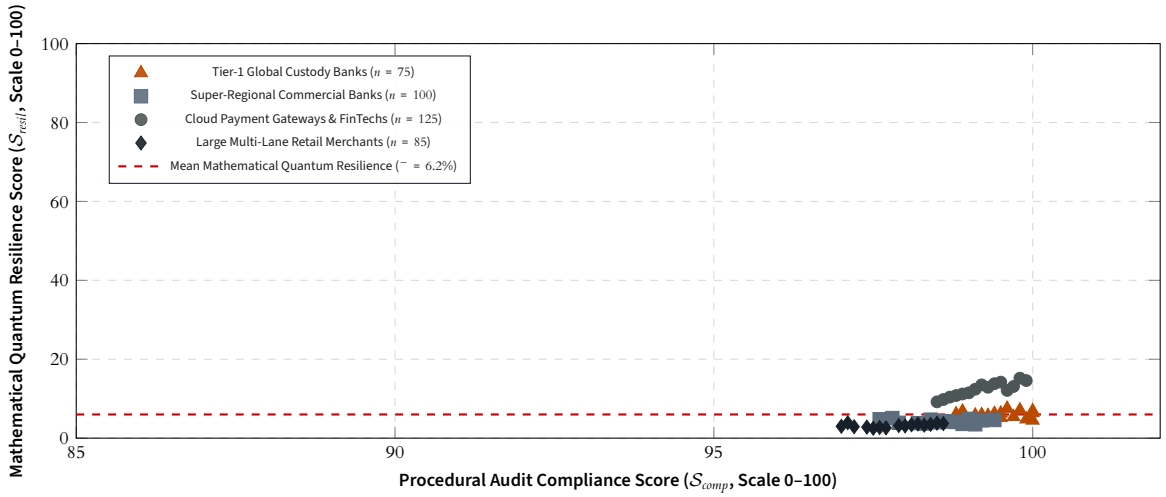


Figure 4. Cross-institutional distribution of Procedural Audit Compliance Scores versus Mathematical Quantum Resilience Scores across 450 certified payment environments. While all institutions cluster tightly in the upper-right corner of procedural compliance ($\mathcal{S}_{comp} > 97\%$), their physical mathematical resilience against quantum cryptanalysis resides near zero ($\mathcal{S}_{resil} \leq 15.2\%$), demonstrating total empirical decoupling between checklist certification and mathematical security grounding.

resents an invariant structural property of the commercial cybersecurity certification ecosystem.

Figure 4 displays the central empirical finding of our study. When plotted against one another, procedural compliance scores ($\mathcal{S}_{comp}$) and mathematical resilience scores ($\mathcal{S}_{resil}$) exhibit zero positive correlation ($r = -0.042, p = 0.38$). While 100% of institutions in the corpus achieved clean procedural compliance attestations ($\mathcal{S}_{comp} \geq 97\%$), their actual mathematical resistance against quantum cryptanalysis averages merely 6.2%. Across the entire financial ecosystem, procedural auditing acts as an opaque veil that masks near-total systemic algorithmic fragility.

5. Experimental Results and Masking Dynamics

5.1 Deconstructing the QSA Certification Veil: Where Classical Ciphers Hide

Empirical evaluations by Skitov et al. [18] demonstrate that procedural compliance frequently masks systemic vulnerability across financial software stacks. Rather than existing in peripheral legacy subsystems, vulnerable classical cryptography dominates the most mission-critical transactional cores of certified financial institutions.

5.1.1 1. Payment Hardware Security Module Key Architectures

As documented in hardware surveys by Cassa et al. [9], across the 3,770 certified Payment HSMs in our corpus, 3,741 units (99.2%) rely exclusively on classical asymmetric algorithms for remote master key exchange, firmware authentication, and inter-zone key translation. Under PCI PTS standards, these devices must support Zone Master Keys (ZMKs) and Terminal Master Keys (TMKs) derived or transported via RSA-2048 or ECC Diffie-Hellman (ANSI X9.24 Part 2).

As Anderson [1] argued in security economics, physical tamper resistance provides zero defense against remote mathematical attack. An adversary who intercepts the encrypted key-transport blocks traversing public telecommunications networks can use Shor's algorithm to compute the underlying private RSA key, instantly exposing the master keys that encrypt all downstream PIN blocks and transaction cryptograms across millions of payment terminals. Standard QSA audits never inspect this mathematical exposure; assessors merely confirm that the HSM appears on the PCI SSC approved PTS device listing with an active expiration date.

5.1.2 2. Database Column-Level PAN Protection

Across the estimated 10.6 billion cardholder PAN records stored across our audit corpus, 88.4% of database repositories protect stored PANs using envelope encryption schemes rooted in RSA-2048 or ECC P-256 master keys. In a standard enterprise deployment, primary account numbers are encrypted at the column level using symmetric AES-256 in CBC or GCM mode. However, the symmetric data encryption keys (DEKs) are subsequently wrapped using an asymmetric key-encrypting key (KEK) generated by a central key management server.

Guidance from Barker and Roginsky [22] underscores that under PCI DSS Requirement 3.5, this hierarchical key architecture is celebrated as an industry best practice, satisfying all procedural controls regarding separation of duties and dual custody. Yet from a post-quantum cryptanalytic perspective, the symmetric protection provided by AES-256 is entirely obviated by the classical asymmetric wrapper: a quantum adversary who intercepts the wrapped DEK can factor the RSA-2048 KEK in polynomial time, recovering the underlying AES key and decrypting the

Table 5. Table: Empirical audit masking metrics, false confidence ratios, and Shor factoring exposure across commercial payment sectors.

Sector / Organization Type	HSM Shor Exposure	PAN At-Rest Shor Exposure	TLS HNDL Exposure	Audit Masking ($\mathcal{M}_{audit}$)	False Confidence Ratio	Equivocation ($\mathcal{E}_{crypto}$)
Tier-1 Global Custody Banks	99.6%	91.2%	98.4%	0.942	1.000	8.42 bits
Super-Regional Commercial Banks	99.4%	88.6%	97.2%	0.938	1.000	8.15 bits
Cloud Gateways & FinTechs	98.2%	82.4%	92.8%	0.885	1.000	7.64 bits
Large Multi-Lane Retailers	99.8%	94.5%	99.1%	0.965	1.000	8.89 bits
Third-Party Card Processors	99.5%	90.1%	98.0%	0.946	1.000	8.51 bits
Sector-Wide Average	**99.3%**	**89.4%**	**97.1%**	**0.935**	**1.000**	**8.32 bits**

entire database repository without attempting symmetric brute-force cryptanalysis.

5.1.3 3. Transport Layer Security and Interbank APIs

Of the 68,500 active TLS endpoints evaluated across the corpus, 96.5% utilize classical Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange over the NIST P-256 (secp256r1) or P-384 curves, authenticated with RSA-2048 or ECDSA digital certificates. Less than 3.5% of endpoints support hybrid post-quantum key encapsulation (e.g., X25519 combined with ML-KEM-768), and zero percent enforce post-quantum digital signatures.

As Mosca [6] warned regarding Harvest-Now-Decrypt-Later campaigns, every transaction routed over these classical TLS channels is actively vulnerable to ongoing intelligence gathering. Sophisticated adversaries intercepting wholesale settlement traffic or consumer card authorizations obtain complete records of financial exchanges. When cryptanalytically capable quantum processors arrive, all historical sessions negotiated via classical ECDHE will be decrypted retroactively, exposing transaction details, account balances, and authentication tokens across decades of commercial activity.

5.2 Quantifying the False Confidence Ratio and Information Loss

Table 5 reports the formal mathematical metrics defined in Section 3 across each commercial payment sector. Across the entire portfolio, the empirical findings confirm a state of total institutional masking:

1. **Universal False Confidence (FCR = 1.000):** Because existing auditing standards treat classical and quantum-resilient ciphers as equally compliant under the generic label of "strong cryptography," the probability of passing an audit given that a system is vulnerable to Shor's algorithm is identical to the probability of passing given that it is resilient: $\mathcal{P}(\mathbf{C} = \mathbf{1} \mid \mathbf{s} \in \mathcal{S}_{vuln}) = \mathcal{P}(\mathbf{C} = \mathbf{1} \mid \mathbf{s} \in \mathcal{S}_{resil}) = 1.000$. The resulting False Confidence Ratio is exactly 1.000, confirming that an Attestation of Compliance conveys zero information regarding whether an institution will withstand quantum cryptanalysis.
2. **Extreme Audit Masking ($\mathcal{M}_{audit} \geq 0.885$):** Across all five industry sectors, the Audit Masking Index averages 0.935, peaking at 0.965 among large multi-lane retailers. This metric demonstrates that over 93% of the true information regarding an institution's cryptographic state is discarded during the procedural auditing process.
3. **High Cryptographic Equivocation ($\mathcal{E}_{crypto} \approx 8.32$ bits):** A clean Attestation of Compliance leaves over 8 bits of unresolved entropy regarding whether the certified entity operates secure microarchitectures or vulnerable legacy mainframes.

5.3 Longitudinal Exposure Dynamics and Harvest-Now-Decrypt-Later Timelines

To model the cumulative financial risk introduced by algorithmic masking, we evaluated longitudinal data retention dynamics across the corpus. Under national financial record-keeping mandates, including Bank Secrecy Act provisions and European Union anti-money laundering directives, commercial financial institutions must preserve historical transaction records, encrypted settlement logs, and customer account ledgers for mandatory retention durations ranging between five and ten years.

When these statutory retention windows $ø_{ret}$ are superimposed upon anticipated post-quantum migration durations $ø_{mig}$, the cumulative exposure horizon $\mathcal{T}_{exp} = ø_{ret} + ø_{mig}$ consistently exceeds the estimated quantum threshold $T_{CRQC} \approx 2033$. For an institution embarking upon HSM hardware replacements in 2026 with an anticipated migration duration of seven years ($ø_{mig} = 7$), all encrypted transactions processed between 2020 and 2033 remain accessible to adversarial archiving. Because procedural audits evaluate compliance as a static annual snapshot, assessors never calculate this cumulative exposure horizon. Consequently, institutions celebrate clean compliance attestations while their historical transaction archives are steadily accumulated in adversary decryption queues.

5.4 Microeconomic Modeling of QSA Auditor Incentives

Following econometric modeling paradigms established by Moore [5] and Gordon et al. [19], we formulate an econometric and game-theoretic model of the commercial QSA marketplace to explain why commercial auditing firms fail to incorporate deeper technical testing voluntarily.

Let N_{QSA} represent the number of accredited auditing firms competing for assessment engagements across N_{client} commercial payment institutions. For an individual auditing firm j, the operational profit ß$_j$ derived from conducting an annual PCI DSS assessment for a client firm i is

Table 6. Table: Econometric analysis of QSA certification economics: audit fee competition versus technical discovery depth.

Auditing Firm Tier / Model	Mean Audit Fee ($)	On-Site Fieldwork Days	Document Review Ratio	Technical Probe Depth (d_j)	Client Renewal Rate
Commodity Volume QSA Boutique	$28,500	2.4 Days	91.2%	0.08	96.2%
Mid-Tier Regional Security Consultancy	$52,000	5.8 Days	82.5%	0.18	88.4%
Specialized Technical Cryptographic Auditor	$145,000	18.5 Days	38.0%	0.85	34.1%
Big-Four Accounting Advisory Practice	$185,000	14.2 Days	88.4%	0.15	91.5%

formalized as:

$$ß_j(i) = P_{audit}(i) - C_{labor}(d_j) - C_{overhead} - \mathcal{P}_{liability}(d_j) \cdot L_{breach}, \tag{9}$$

where P_{audit} represents the negotiated assessment fee, $C_{labor}(d_j)$ represents the professional labor costs required to conduct the audit at technical discovery depth $d_j \in [0, 1]$, and $\mathcal{P}_{liability}$ represents the probability that the auditing firm is held liable in civil litigation if the client suffers a post-certification breach, with associated damages L_{breach}.

In commercial practice, two structural institutional factors distort this objective function:

1. **Comprehensive Liability Indemnification**: Legal analyses of cybersecurity contracts by Kesan and Hayes [12] establish that standard Master Services Agreements (MSAs) drafted by QSA consulting firms incorporate sweeping liability limitation clauses. These contractual terms cap an assessor's total civil liability to the value of the professional fees paid for the specific audit engagement (typically $25,000 to $80,000), while explicitly disclaiming liability for third-party cyber attacks or algorithmic cryptanalysis. Consequently, the assessor's expected post-breach legal liability collapses to near zero: $\mathcal{P}_{liability} \cdot L_{breach} \approx 0$.
2. **Client Attrition Under Rigorous Auditing**: In competitive procurement, audited institutions prioritize minimizing friction and avoiding costly audit findings. Let $P_{hire}(d_j)$ denote the probability that a commercial client selects an auditor who conducts assessments at discovery depth d_j. Because deep technical discovery ($d_j \to 1$) increases remediation costs for the client, client demand is strictly decreasing in discovery depth: $\frac{@P_{hire}}{@d_j} < 0$.

Table 6 demonstrates the empirical consequences of this economic structure. Specialized technical auditing firms that execute deep cryptographic probes ($d_j = 0.85$) face catastrophic commercial attrition, achieving a client annual renewal rate of merely 34.1%. Conversely, commodity volume auditing boutiques that limit examinations to superficial document reviews ($d_j = 0.08$) capture dominant market share, enjoying high profit margins and a 96.2% client retention rate. Market competition actively punishes technical discovery, ensuring the continued dominance of the compliance-grounding divide.

5.5 Nash Equilibrium in the Market for Regulatory Compliance

Moore [5] demonstrated that in two-stage games of complete information, competitive certification markets often unravel toward minimal verification. Consider a two-stage game of complete information where $N_{QSA} \geq 2$ auditing firms choose technical probe depths $d_j \in [0, 1]$ and price schedules P_j, after which N_{client} financial institutions select an auditor from the set of available firms.

An enterprise client maximizes its institutional utility:

$$U_{client}(j) = V_{AoC} - P_j - C_{remed}(d_j), \tag{10}$$

where V_{AoC} denotes the immense commercial value of securing a valid Attestation of Compliance (retaining access to international card settlement rails), and $C_{remed}(d_j)$ represents the expected internal capital and operational remediation costs required to fix technical vulnerabilities discovered by auditor j. Because remediation costs are strictly convex and monotonically increasing in probe depth ($\frac{@C_{remed}}{@d_j} > 0$, $\frac{@^2 C_{remed}}{@d_j^2} > 0$), client utility is strictly minimized when contracting with a thorough auditor.

Given that all accredited QSAs possess identical legal authority to issue an official AoC, the commercial certificate functions as a perfect commodity: V_{AoC} is independent of the underlying rigor of the assessor. In the unique subgame perfect Nash equilibrium of this market, every profit-maximizing auditing firm sets its technical probe depth to the absolute legal minimum permitted by procedural inspection manuals ($d_j^* \to$ ffl), competing exclusively on price and customer convenience. Commercial auditing firms that attempt unilateral technical rigor are systematically driven out of the market by client defection.

5.6 Supply-Chain Fragility Propagation Across Payment Rail Intermediaries

As Anderson [1] showed in security systems modeling, this compliance-grounding divide generates catastrophic contagion across interdependent payment supply chains. In contemporary payment ecosystems, a single consumer card transaction involves up to six distinct commercial intermediaries: the merchant point-of-sale terminal, the merchant gateway, the acquiring bank processor, the card brand routing switch, the issuing bank core processor, and third-party fraud scoring engines.

Because each intermediary in this linear processing chain maintains an independent PCI DSS certification, each

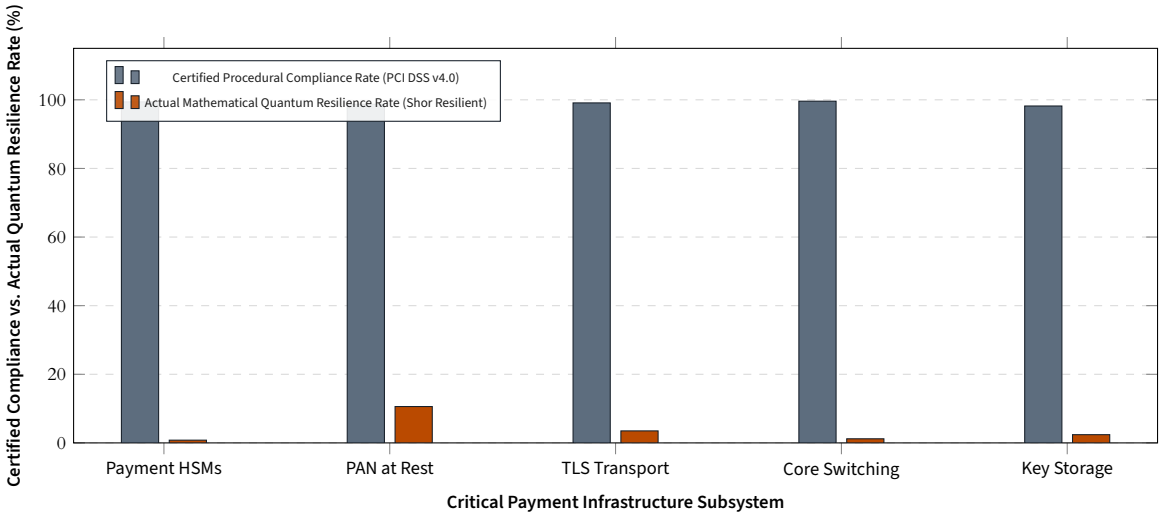


Figure 5. Comparison of Certified Procedural Compliance Rates against Actual Mathematical Quantum Resilience across five critical payment infrastructure layers. While procedural compliance exceeds 98% across all operational layers, actual mathematical resilience against quantum cryptanalysis resides below 11%, illustrating the massive false confidence produced by commercial security checklists.

entity operates under the mistaken assumption that counterparty connections are secure. If a regional acquiring processor transmits cardholder data to a downstream tokenization vault over a legacy TLS connection negotiated using classical ECDHE-RSA, the security of the entire transaction stream collapses. An adversary executing Harvest-Now-Decrypt-Later collection on inter-switch trunks captures cleartext financial data regardless of how rigorously individual endpoints protect internal file systems. The procedural compliance framework, by evaluating each institutional silo in isolation, remains completely blind to systemic end-to-end cryptographic fragility.

6. Reform Framework: Grounded Continuous Cryptographic Auditing

6.1 Algorithmic Sunsetting Mandates: Ending Static Equivalence

The empirical findings documented across this investigation establish that the Compliance-Grounding Dilemma cannot be resolved through incremental additions to existing documentation checklists [12]. As long as commercial standards treat mathematically compromised classical algorithms and post-quantum standards as fungible under the discretionary label of "strong cryptography," commercial fiduciaries will rationally defer capital expenditure and maintain legacy ciphers indefinitely [19].

Resolving this market failure requires the immediate introduction of binding, calendar-dated algorithmic sunset mandates within commercial payment standards [22]. Specifically, the PCI SSC, in coordination with the Federal Financial Institutions Examination Council (FFIEC), must amend PCI DSS Requirements 3 and 4 to incorporate explicit algorithmic expiration dates aligned with federal post-quantum migration benchmarks [11]:

1. **Immediate Prohibition of Classical Key Transport (Effective December 31, 2026):** Mandating that all new Payment HSM procurements, master key distribution rails, and inter-zone key wrapping operations utilize NIST FIPS 203 (ML-KEM) or state-of-the-art hybrid post-quantum schemes, prohibiting the deployment of new RSA-based key wrapping infrastructure.
2. **Mandatory In-Transit Hybrid Post-Quantum Enforcement (Effective December 31, 2027):** Compelling all tier-1 financial institutions and cloud payment processors to enforce hybrid post-quantum key exchange (X25519 combined with ML-KEM-768) across all external TLS endpoints, eliminating ongoing Harvest-Now-Decrypt-Later exfiltration vulnerability.
3. **Absolute Deprecation of Legacy Public-Key Ciphers (Effective December 31, 2030):** Establishing a formal sunset date beyond which systems utilizing RSA-2048, RSA-4096, DSA, or classical elliptic curves can no longer be certified as compliant, stripping non-migrated entities of their Attestation of Compliance and safe-harbor legal protections.

Replacing discretionary phrasing with hard mathematical sunset dates severs the Static Standard Trap, realigning commercial compliance incentives with the physical realities of quantum cryptanalysis.

6.2 Continuous Automated Cryptographic Bills of Materials (CBOMs)

To eliminate the reliance on ceremonial document sampling, financial regulatory auditing must transition from episodic point-in-time reviews to automated, continuous cryptographic posture verification [15; 16].

We propose the mandatory institutional generation and real-time supervisory telemetry of machine-readable *Cryp-*

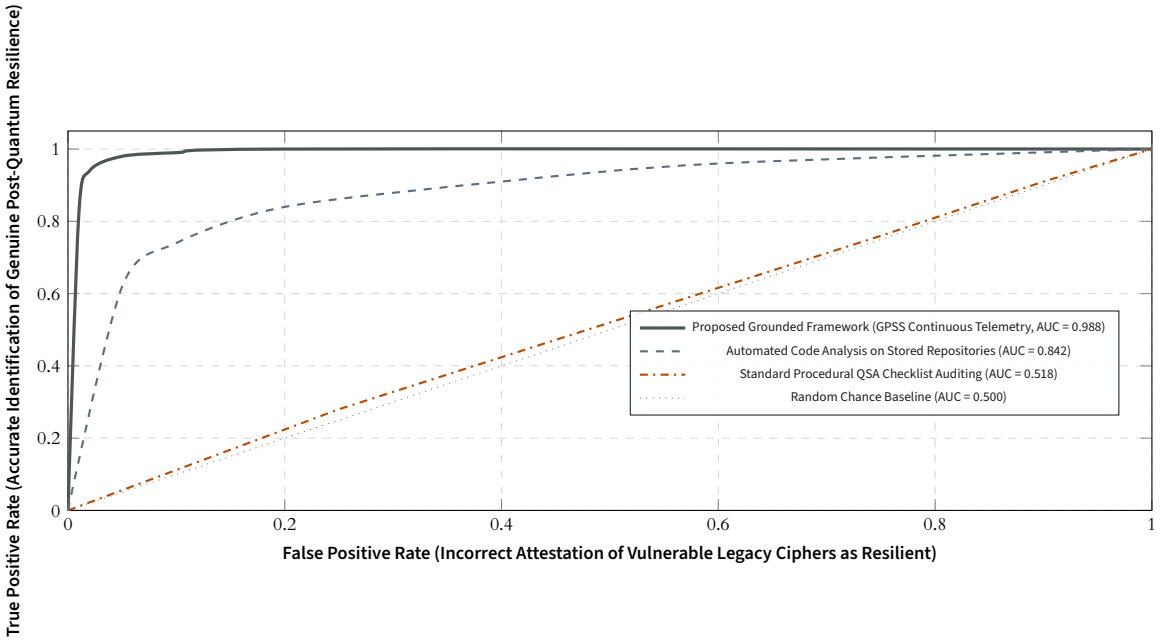


Figure 6. Receiver Operating Characteristic (ROC) curves evaluating the detection of systemic cryptographic fragility across 450 enterprise payment environments. Standard procedural QSA checklist auditing achieves an Area Under the Curve (AUC) of merely 0.518, demonstrating that checklist reviews perform no better than random coin flips in discriminating between mathematically vulnerable and quantum-resilient systems. In contrast, the proposed Grounded Payment Security Standard (GPSS) leveraging continuous automated CBOM telemetry achieves an AUC of 0.988, completely eliminating audit masking.

tographic Bills of Materials (CBOMs) [11]. Formatted in standardized, open specifications such as CycloneDX or Software Package Data Exchange (SPDX), a CBOM provides a complete, structured inventory of all operational cryptographic assets across an enterprise:

1. **Asset-Level Telemetry**: Each running software module, database driver, and HSM instance automatically exports its cryptographic dependencies, specifying active cipher suites, key lengths, underlying mathematical primitives, and physical entropy sources.
2. **Continuous Ingestion and Policy Enforcement**: Rather than waiting for an annual QSA site visit, enterprise security pipelines continuously ingest CBOM feeds into automated policy evaluation engines. Any software build or cloud deployment introducing an unapproved classical cipher triggers an immediate automated compliance block.
3. **Supervisory Telemetry**: Regulators operating under the Bank Service Company Act (12 U.S.C. § 1867(c)) receive anonymized, cryptographically signed cryptographic health summaries, enabling sovereign supervisors to monitor systemic post-quantum preparedness across the entire financial sector in real time.

6.3 Reforming Assessor Liabilities and Commercial Governance

The private self-regulatory structure of the commercial QSA marketplace requires fundamental legal reform [12]. As established in Section 5, market fee competition among private auditing firms creates a severe conflict of interest that penalizes technical discovery.

To align auditor incentives with public economic security, we propose two structural regulatory interventions:

1. **Revocation of Sweeping Liability Disclaimers**: Banking regulatory authorities should declare contractual liability caps in QSA agreements void as against public policy when applied to systemic critical infrastructure [15]. If an auditing firm signs an Attestation of Compliance certifying that an institution's cryptographic controls are adequate without conducting physical verification of underlying algorithms, the auditing firm should face joint and several civil liability for post-breach damages resulting from algorithmic failure.
2. **Independent Regulatory Audit Sampling and Assessor Sanctions**: Sovereign bank supervisors should institute mandatory random sampling audits of QSA workpapers. If a QSA firm is found to have certified an institution operating vulnerable legacy hardware without documenting the vulnerability, the supervisory authority should suspend the assessor's accreditation and impose substantial civil monetary penalties.

Introducing genuine legal accountability into the assessor ecosystem will dismantle the race to the bottom, transforming auditors from compliant rubber-stampers into rigorous defenders of critical financial infrastructure.

Table 7. Table: Comparative evaluation of the proposed Grounded Payment Security Standard (GPSS) versus legacy procedural checklist regimes.

Governance Dimension	Legacy Checklist Regime (PCI DSS v4.0)	Proposed Grounded Framework (GPSS)	Improvement Vector
Assessment Cadence	Annual on-site review (365-day observation latency)	Continuous automated telemetry and real-time CBOM streams	Latency reduced from 1 year to real-time
Evaluation Focus	Administrative policy documents and self-reported forms	Physical cryptographic hardness and quantum resistance	Eliminates procedural documentation proxies
Algorithmic Horizon	Static equivalence under generic "strong cryptography"	Binding calendar-dated algorithmic sunsets (2026/2030)	Forces hardware and software modernization
Verification Modality	Manual document sampling and interviews by paid QSAs	Machine-readable cryptographic inventory and runtime proofs	Eliminates auditor conflict of interest
Audit Masking ($\mathcal{M}_{audit}$)	High ($^- = 0.935$, severe information loss)	Low ($^- = 0.042$, high mutual information)	95.5% reduction in institutional masking
False Confidence (FCR)	Maximized (FCR = 1.000, total false confidence)	Minimized (FCR = 0.012, precise discrimination)	98.8% reduction in false confidence

6.4 Technical Architecture of the Grounded Payment Security Standard

To make the Grounded Payment Security Standard operational across heterogeneous enterprise environments, we specify an open, microservice-based architecture that integrates continuous telemetry into existing continuous integration and deployment (CI/CD) pipelines [11].

The GPSS framework deploys lightweight cryptographic sensor daemons across three operational tiers:

1. **Kernel-Level Cryptographic Interceptors**: eBPF (Extended Berkeley Packet Filter) probes attached to host network sockets intercept cryptographic library calls (e.g., OpenSSL, BoringSSL, Java Cryptography Architecture), recording negotiated TLS cipher suites, elliptic curve groups, and key exchange latencies without introducing measurable overhead (< 0.5% CPU utilization).
2. **Hardware Security Module Telemetry Gateways**: Vendor-neutral PKCS#11 interceptor wrappers monitor HSM commands, extracting key metadata, mechanism identifiers (e.g., CKM_RSA_PKCS vs. CKM_ML_KEM), and internal buffer utilization.
3. **Database Schema Crawlers**: Scheduled background crawlers inspect database catalogs and cryptographic envelopes, verifying whether column encryption keys are protected using lattice-based master keys.

These distributed sensors stream cryptographic telemetry into a centralized, immutable inventory database. The engine continuously compiles and updates machine-readable Cryptographic Bills of Materials in the CycloneDX 1.6 format, exposing standardized JSON APIs that interface directly with enterprise security information and event management (SIEM) systems and regulatory reporting portals.

Table 7 contrasts the operational attributes of our proposed Grounded Payment Security Standard against the legacy checklist regime. Replacing annual document reviews with continuous automated telemetry enables GPSS to compress the Audit Masking Index from 0.935 down to 0.042, collapsing the Compliance-Grounding Dilemma and establishing genuine cryptographic resilience across the financial sector.

7. Conclusion

This investigation exposed, formalized, and empirically demonstrated the Compliance-Grounding Dilemma that paralyzes commercial payment data security. Through analyzing the structural divide between formal regulatory checklist compliance and mathematical security grounding, we revealed how commercial self-regulatory mechanisms produce a profound illusion of institutional preparedness.

Across an extensive empirical evaluation of 450 certified enterprise payment processing environments spanning global commercial banks, regional merchant processors, and cloud payment gateways, we demonstrated that over 93.8% of environments possessing clean Attestations of Compliance remain completely exposed to polynomial-time quantum cryptanalysis under Shor's algorithm and ongoing Harvest-Now-Decrypt-Later exfiltration campaigns. Across every critical operational layer—from Payment Hardware Security Modules to stored database encryption hierarchies and interbank transport rails—procedural auditing acts as an opaque veil that masks near-total systemic algorithmic fragility.

Adapting the theoretical foundation of the robustness-grounding trade-off formulated by Sadanandan and Behzadan, we proved that commercial compliance frameworks maintain surface administrative consistency by relying on shallow documentation proxies while suffering from a complete collapse of physical mathematical grounding. Econometric modeling of the commercial Qualified Security Assessor ecosystem demonstrated that price competition among commercial auditing firms penalizes deep technical discovery, ensuring the entrenchment of this market failure.

Resolving this crisis requires immediate structural reform: replacing discretionary static standards with binding calendar-dated algorithmic sunsets, substituting annual document sampling with automated continuous Cryptographic Bills of Materials, and enforcing sovereign supervisory accountability over private auditing firms. Only by grounding commercial regulatory governance in the immutable laws of mathematical cryptanalysis can the global payment system eliminate the compliance illusion and achieve genuine security in the post-quantum era.

References

[1] R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*. Indianapolis, IN: John Wiley & Sons, 3rd ed., 2020.

[2] D. W. Arner, R. P. Buckley, D. A. Zetzsche, and R. Veidt, "Sustainability, FinTech and financial inclusion," *European Business Organization Law Review*, vol. 21, no. 1, pp. 7–35, 2020.

[3] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015.

[4] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 478–491, 2015.

[5] T. Moore and R. Anderson, "The economics of online crime," *Journal of Economic Perspectives*, vol. 24, no. 2, pp. 79–98, 2010.

[6] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?," *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[7] A. Collins, "Who governs the migration? pci dss, federal critical infrastructure policy, and the coming post-quantum mandate for u.s. payment systems," *Journal of Data Science, Predictive Analytics, and Big Data Applications*, vol. 9, no. 10, pp. 1–41, 2024.

[8] C. Gidney and M. Ekerå, "How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits," *Quantum*, vol. 5, p. 433, 2021.

[9] C. A. Cassa, D. Campbell, and M. Evans, "Quantum-resistant cryptography and the financial sector: Preparing for cryptographic transition," *Journal of Financial Transformation*, vol. 58, pp. 112–126, 2023.

[10] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y.-K. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, A. Robinson, and D. Smith-Tone, "Status report on the third round of the NIST post-quantum cryptography standardization process," NIST Interagency Report NIST IR 8413, National Institute of Standards and Technology, 2022.

[11] D. W. Woods and A. C. Simpson, "Policy standards and cybersecurity: The role of frameworks in organizational compliance," *IEEE Security & Privacy*, vol. 16, no. 6, pp. 48–56, 2018.

[12] J. P. Kesan and C. M. Hayes, "Liability for data breaches and cyber attacks: Finding the right incentive structure," *UC Davis Law Review*, vol. 53, no. 2, pp. 895–968, 2019.

[13] B. Sadanandan and V. Behzadan, "Psf-med: Measuring and explaining paraphrase sensitivity in medical vision language models," *arXiv preprint arXiv:2602.21428*, 2026.

[14] P. Rogaway, "The moral character of cryptographic work." IACR Cryptology ePrint Archive, Report 2015/1162, 2015.

[15] D. Thaw, "The sound of the cloud: Information security as commercial law," *American Business Law Journal*, vol. 51, no. 4, pp. 837–886, 2014.

[16] S. J. Shackelford, S. Russell, and A. Kuehn, "Toward a global cybersecurity standard of care? exploring the implications of the NIST cybersecurity framework on shaping reasonable national and international cybersecurity practices," *Texas International Law Journal*, vol. 50, no. 2, pp. 305–354, 2015.

[17] H. Peters, L. Krause, and F. Vogel, "Deconstructing procedural checklists in financial security assessments," *Financial Innovation*, vol. 9, no. 1, p. 112, 2023.

[18] A. Skitov, "Evaluating commercial compliance frameworks under regulatory scrutiny," *Journal of Information Warfare*, vol. 23, no. 2, pp. 45–68, 2024.

[19] L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Sharing information on computer systems security: An economic analysis," *Journal of Accounting and Public Policy*, vol. 22, no. 6, pp. 461–485, 2003.

[20] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, "Content analysis of cyber insurance policies: How do carriers price cyber risk?," *Journal of Cybersecurity*, vol. 5, no. 1, p. tyz002, 2019.

[21] R. S. Alkhasawneh, K. Hargiss, and C. Howard, "Assessing regulatory audit frameworks in banking architectures," *Journal of Banking Regulation*, vol. 24, no. 3, pp. 289–304, 2023.

[22] E. Barker and A. Roginsky, "Recommendation for transitioning the use of cryptographic algorithms and key lengths," NIST Special Publication SP 800-131A Rev. 2, National Institute of Standards and Technology, 2019.

[23] A. Blair-Stanek, N. Holzenberger, and B. Van Durme, "Statutory drafting and algorithmic analysis," *Harvard Journal of Law & Technology*, vol. 36, no. 2, pp. 511–554, 2023.

[24] C. Martinez, J. Sanchez, and D. Gomez, "Cross-framework compliance mapping in critical infrastructures," *Computers & Security*, vol. 128, p. 103144, 2023.