Scale to Stewardship: The Governance Reckoning for India's PA–PG Ecosystem

India's digital payments story has, for long, been framed around scale and speed—daily transaction values running into trillions and the rapid mainstreaming of digital finance. That phase of expansion has now reached an inflection point. Recent regulatory actions and supervisory assessments indicate a clear shift: Payment Aggregators and Gateways are transitioning from growth-driven FinTechs to regulated financial utilities. The entrepreneurial agility that enabled rapid ecosystem build-out is now being weighed against the requirements of institutional discipline, robust governance, and operational resilience. This reassessment reflects a shared recognition that velocity, while transformative, also obscured structural weaknesses that can no longer be overlooked.

This shift is not a critique of India's technology stack, which remains globally competitive. Rather, it reflects concern that governance frameworks in several entities have not evolved at the same pace as technological capability. In recent supervisory cycles and the 2025–26 regulatory directions, the Reserve Bank of India has signalled a reclassification of PAs and PGs as integral components of financial market infrastructure. Consequently, supervisory expectations have deepened. Inspections now focus squarely on substance over form, with a clear message: compliance must be demonstrable in operations, not merely documented. The earlier light-touch approach has given way to close scrutiny, where gaps between policy and practice are treated as material risks with direct implications for authorization and continuity.

1. The Supervisory Lens: Risks & Operational Fissures

A. Merchant Onboarding and the 'Shell Merchant' Risk

The most critical risk emerging from supervisory reports is the onboarding of "mule" or "shell" merchants. Entities are frequently onboarded with focus on document collection rather than intent verification. As a result, it was observed that entities were assigning low risk Merchant category Code (MCC) to high-risk line of business. The key issue in it is PAs often rely on automated, superficial KYC checks (e.g., just verifying a GSTIN/PAN. etc.) leading to a risk where 'bad actors' use these shell merchant accounts to process funds for illegal betting apps, unauthorized forex trading, or crypto scams. The PAs become an unwitting conduit for money laundering through this gap. Inspectors have found instances where the nature of business declared during onboarding had zero correlation with the actual transaction patterns (e.g., a "grocery" merchant processing ₹50 lakh in high-velocity transactions at 2 AM).

B. Escrow Operations: The Trust Deficit

The Escrow Account is the single most important mechanism in PA operational mechanism that manufactures trust in a trustless environment. However, operational lapses here are frequently noticed through co-mingling of funds. A recurrent issue noticed was the usage of "Nodal" or "Escrow" funds into the PA's own operational accounts to manage liquidity crunches or refund buffers. This is a cardinal sin in payment processing. In the eyes of the regulator, this is not a treasury error; it is a violation of the public trust. It showed that the occurrence of settlement latency, i.e., delays in T+1 settlement not due to bank holidays, but due to internal treasury mismanagement by the PA.

C. Cross-Border Leakages (PA-CB)

With the rise of the PA-Cross Border (PA-CB) model, the complexity has multiplied. It is observed that Import/Export payments being netted off illegally, or funds for "software services" actually being diverted for capital account transactions (which are strictly regulated under FEMA). The resultant impact through regulatory action is witnessed in recent embargoes and pauses on major players. It wasn't just about "KYC paperwork"; it was about the *s*anctity of the flow of funds.

2. Operational Challenges: The 'Governance Deficit' and others

The transition from a tech-startup to a Regulated Entity (RE) was a long journey. The biggest challenge for PAs today is not technology; it is **Governance**.

- Tech vs. Compliance Culture Clash is noticed in which **i**n many PAs, the Product Head dictates the roadmap, and the Compliance Officer is merely a sign-off authority. In a regulated entity, this hierarchy must change. Empowering the Chief Compliance Officer (CCO) and CISO with veto power over product launches that do not meet prudential safety standards, is a necessity.

- Many PAs try to act as marketplaces, settling funds to sub-merchants they have no direct contract with, effectively becoming an aggregator for other aggregators. PAs must dismantle this practice, where funds are settled to a master merchant or tech platform rather than the actual service provider. This practice known as "Nesting" destroys the audit trail, as the PAs do not know the "Ultimate Beneficial Owner" (UBO) The regulatory mandate is unequivocal: the chain of custody must be linear and visible, requiring the PA to contract with and settle directly to the ultimate beneficiary, thereby eliminating the opaque risk of funds pooling in unregulated intermediaries.

- Another concerning trend is the information asymmetry within the Board room of these entities. There exists a palpable gap between the technical reality of cyber risk and the Board's understanding of it. When cyber security is viewed as an IT support function

rather than a strategic imperative or third-party outsourcing decisions are okayed without any questions/queries, the entity becomes vulnerable to systemic risks.

- Physical infrastructure risk is emerging as a silent but material vulnerability in the PA–PG ecosystem. A significant share of India's payment backbone—data centres, network exchanges, and telecom aggregation points—is geographically concentrated, with around 34% of critical nodes located in flood-prone or climate-stressed zones. Extreme weather events can therefore disrupt payment continuity through power outages, fibre damage, and site inaccessibility, even when cyber controls remain intact. For systemically important payment intermediaries, climate resilience must be treated as an operational risk—requiring geographic diversification, climate-aware infrastructure choices, and realistic stress testing of disaster recovery arrangements

3. Outsourcing and Cyber-Fragility

A modern PA is rarely a monolithic entity; it is a stack of APIs, stitching together services from cloud providers, video-KYC partners, and fraud detection vendors. This creates a **"Fourth Party" blind spot**. PAs might audit its cloud provider, but do they audit the vendor they use for SMS alerts? Recent outages in the ecosystem weren't caused by the banks or the PAs, but by sub-vendors deep in the supply chain. This **concentration risk** is systemic; if 70% of the industry relies on the same third-party API for Video-KYC, a single failure there becomes a sector-wide paralysis.

Furthermore, the nature of **Cyber Risk** has mutated significantly. Hackers are no longer just trying to brute-force passwords; they are exploiting **API logic flaws**. Vulnerabilities in 'Third party API Integration' is an area of major concern. It was observed from seen cases where attackers manipulated the "refund amount" parameter in an API call to process refunds larger than the original transaction. This is not a failure of a firewall; it is a failure of logic.

This brings us to **IT Resilience**. There is a stark difference between reliability (the system works) and resilience (the system recovers). Many PAs treat Disaster Recovery (DR) drills as a checkbox exercise, conducting them on weekends when traffic is low. But real outages happen on Black Friday or during Diwali sales. If PAs haven't tested their DR switching under peak load, they haven't tested it at all.

What Supervisory Reviews Are Revealing

Recent reviews have surfaced a pattern of structural weaknesses. Some of them with specificity are briefly narrated.

- Business users raise requests for new functionality without formal 'Understanding Documents' (UD) that clarify requirements. IT teams proceed without business sign-off, leading to flawed merchant onboarding workflows.
- 19% of merchant onboarding fraud in 2024 involved synthetic identity fraud using AI-generated UPI IDs
- Vendor IT Team raises change requests, but *no assessment* is performed for vendor-driven changes. Third-party support is part of the application core team, yet not held accountable for failures.
- Over-reliance on unvetted vendors for core payment processing has created single points of failure. 45% of PA outages originated from third-party infrastructure gaps
- 78% of PAs lack enforceable audit rights in vendor contracts, creating blind spots in payment infrastructure.
- Vendors routinely sub-contract critical functions (e.g., encryption, transaction routing) without PA oversight
- If a change fails, systems must revert to original state using backup or configuration restoration. *No such process exists* for escrow account configurations
- 62% of PAs store transaction logs on offshore servers, enabling jurisdictional arbitrage during breach investigations
- Covert data exfiltration via steganography tools embedded in payment SDKs.
- AI-generated fraud surged by 300% YoY; traditional rule-based systems are ineffective.
- Legacy PG systems using pre-quantum encryption (e.g., RSA-2048) risk decryption by quantum computers by 2030.
- VAPT recommendations and security incidents trigger change requests, but *no validation* occurs post-implementation. Critical devices (firewalls, access points) are updated without testing. Over 60% of inspected entities lacked pre-implementation validation for network changes
- Emergency changes require MD/CEO approval. *In practice, IT teams bypass approval, implementing changes during outages without risk assessment.
- Physical infrastructure for payment systems—data centers, telecom towers—faces acute climate risks. 34% of critical nodes are in flood-prone zones

The Reserve Bank of India's supervisory review 2024 has delivered a stark warning: Payment Aggregators (PAs) and Payment Gateways (PGs) are failing to address systemic risks that could cripple India's ₹1.2 trillion daily payment ecosystem. These risks are not hypothetical—they are documented violations.

The Path Forward

The regulatory signal is clear. The focus has shifted from procedural compliance to operational resilience. The expectation is not merely about ‘controls exist’, but that they function as intended—consistently and under stress.

For policymakers, there is merit in continuing to surface anonymised supervisory learnings. Transparency around failure modes accelerates collective learning. For industry leaders, the choice is stark. Governance gaps now carry tangible costs—loss of consumer trust, supervisory sanctions, and penalties that can materially impair business viability. India’s digital payments infrastructure is a national asset. Securing it requires moving beyond growth narratives to stewardship. The next phase of the ecosystem will be defined not by how fast it scales, but by how well it is governed.

RBI Supervision # PAs & PGs # Fintech Cos. # Digital Payments

DFS # NPCI # PCI