Critical Outsourcing Risk Management

A Payment Services Case Study

How a multinational payment company transformed fragmented vendor management into a strategic capability for safe growth and regulatory confidence.

3.4 trillion transactions handled globally in 2023 (McKinsey Global Payments Report 2024). Digital adoption accelerating worldwide.

99.8% of transaction volume now digital (RBI H1 2025). Digital payments grew from **2,071 crore** to **18,592 crore** (FY 2017-18 to FY 2023-24) — **44%** CAGR. UPI transactions: **129%** CAGR growth (Ministry of Finance India).

93% of asset managers experienced cybersecurity incidents in past year (CFO.com 2025). **46%** of organizations piloting AI for predictive risk analytics (PwC Global Compliance Survey 2025).

The Challenge: Fragmented Vendor Management

As the company's regulated entity in India expanded technology outsourcing, existing practices proved inadequate—creating significant compliance and operational risks.

Inconsistent Risk Assessment

Ad-hoc questionnaires and subjective criteria created blind spots across the vendor portfolio.

Unclear Governance

Dispersed responsibilities with no single accountability point led to delayed responses.

Minimal Monitoring

Annual audits replaced continuous oversight—risks went undetected until incidents occurred.

Regulatory Gaps

Practices didn't systematically align with RBI Framework, creating compliance exposure.

The Stakes Were High

> Scaling operations safely and maintaining regulatory approval demanded effective third-party risk management.

The Solution: A Systematic Transformation

Our engagement began with a diagnostic assessment and cross-functional workshops to transform risk management.

01

Comprehensive Risk Assessment

Standardized evaluation framework, quantitative and qualitative dimensions.

02

Structured Governance

Formal model with clear roles, Vendor Risk Committee, and escalation protocols.

03

Performance Monitoring

Integrated system for metrics, leading indicators, and real-time dashboards.

04

Regulatory Compliance

Embedded controls across the vendor lifecycle, calibrated to RBI Framework.

Risk Assessment Methodology

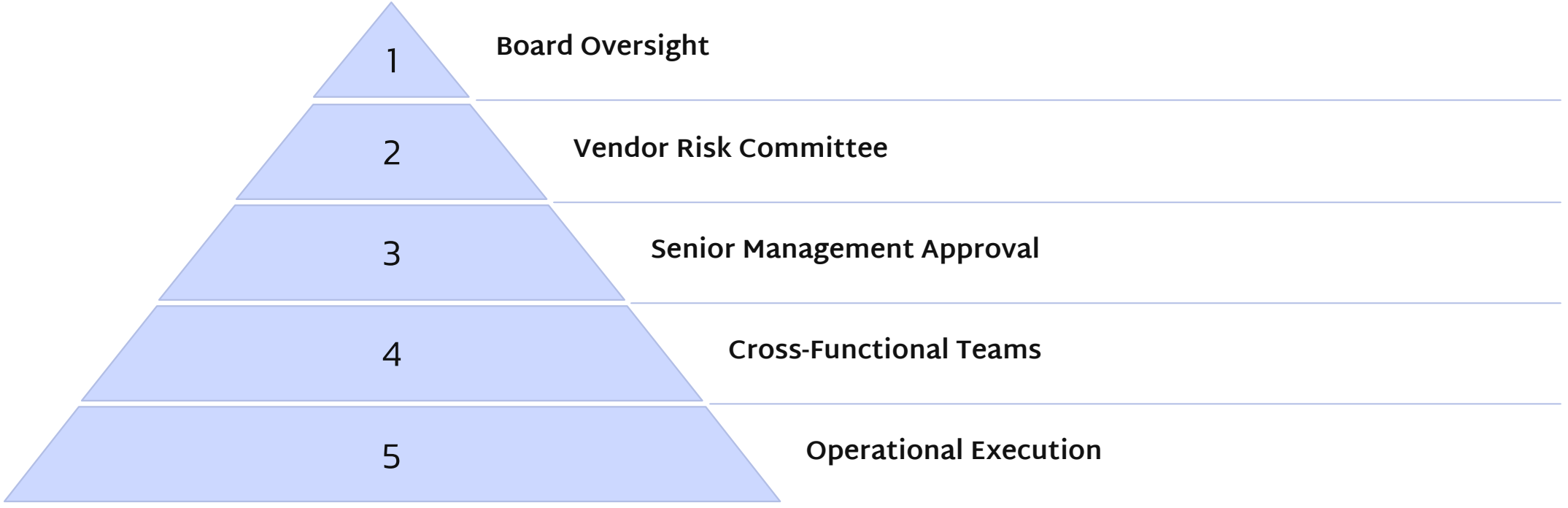
Standardized Evaluation

Vendors classified into risk tiers based on service type and operational importance. Critical vendors received proportional scrutiny while maintaining efficiency.

Key criteria assessed:

- Financial stability
- Operational resilience
- Cybersecurity maturity
- Regulatory compliance history
- Business criticality

Governance Architecture



Centralized accountability replaced fragmented decision-making. Escalation protocols defined issue resolution timeframes and governance levels, ensuring consistent and defensible vendor management.

The Impact: Measurable Transformation

Enhanced Transparency

Comprehensive vendor portfolio visibility with clear metrics. Leadership receives structured reporting for informed strategic decisions.

Operational Resilience

Continuous monitoring identifies issues before escalation. Early warning indicators enable proactive vendor engagement.

Regulatory Confidence

Robust controls demonstrate governance maturity to RBI regulators, reducing risk during examinations.

Strategic Scalability

Systematic framework enables safe expansion of technology outsourcing while maintaining disciplined risk management.

From Compliance to Capability

Compliance Checklist

Reactive, fragmented approach

Strategic Capability

Proactive, systematic framework

Competitive Advantage

Safe growth enabler

Key Takeaway

Systematic third-party risk management evolves from a compliance checklist into a strategic capability that enables safe growth, regulatory confidence, and operational resilience in an increasingly complex payment services environment.