SISA

Customer Success Story

How SISA Helped a Leading Indian Bank Assess and Govern 100+ Vendors Through a Unified Third-Party Risk Management (TPRM) Framework

About The Customer

The customer is an Indian private sector bank with 1,500+ banking outlets and, 2,070+ ATMs spread across different states in India and overseas representative offices at Abu Dhabi and Dubai. With a customer base of over 19 million, and a large network of remittance partners around the world, the bank handles more than one fifth of India's total personal inward remittances, approximately. It has remittance arrangements with more than 110 banks and exchange companies around the world.

The bank operates as a full-service financial institution in India, structured across four primary business segments: Retail Banking, Wholesale & Corporate Banking, NRI Banking, and Treasury Operations. It follows a "financial supermarket" model, integrating traditional banking with specialized fintech and para-banking products.

Business Challenge

As financial institutions deepen reliance on cloud, fintech, Managed Service Providers (MSPs), technology partners, and outsourced vendors, third-party risk has become a major operational and regulatory priority. However, traditional vendor assessments are often fraught with fragmented methodologies and inconsistent evidence requirements while offering limited visibility into vendor control environments.

To meet regulatory and internal policy requirements, the bank needed to conduct Vendor Audit and Due Diligence at scale, assess vendors based on service criticality and data sensitivity, and strengthen compliance across its vendor ecosystem.

Besides, the bank faced additional challenges on operational front, that included:

01 Lack of comprehensive audit reports covering both identified observations as well as compliant controls, for complete visibility into the overall control environment.

02 Delays in coordinating with vendors, including follow-ups, evidence collection, and periodic status updates to the relevant stakeholders.

03 Challenges in delivering accurate, consistent, and high-quality audit reports within the agreed timelines.

Against this backdrop, the bank sought a trusted partner capable of executing large-scale vendor assessments while enhancing governance, consistency, and regulatory alignment across its vendor ecosystem.

SISA's Solution

SISA designed and executed a risk-based Third-Party Risk Management (TPRM) program covering over 100 vendors categorized as L3 (Low Impact), L4 (Medium Impact), and Technology Service Providers (TSPs). Assessments were tailored based on vendor criticality, nature of services provided, regulatory applicability, data sensitivity, and technology dependencies. The assessment methodology incorporated requirements from RBI Master Directions on IT Outsourcing, DPDPA, PCI DSS, and the bank's internal risk management framework. Beyond compliance validation, the assessment focused on governance maturity, security controls, privacy practices, operational resilience, incident management capabilities, subcontractor oversight, and regulatory readiness across the vendor's ecosystem.

Risk-Based Vendor Assessment Model

To ensure assessment effort was proportionate to vendor risk, SISA applied a risk-based assessment model that considered:

- Criticality of services provided to the bank
- Customer and business data processed by the vendor
- Access to banking systems and infrastructure
- Regulatory and compliance obligations applicable to the service
- Cloud, outsourcing, and technology dependencies
- Geographic and operational risk factors
- Subcontractor and fourth-party dependencies

This approach enabled the bank to focus assessment depth and remediation efforts on vendors presenting the highest operational, regulatory, and information security risks.

SISA's assessment followed a structured five-phase approach that combined regulatory alignment, vendor-specific due diligence, evidence-based validation, and continuous project tracking to help the bank gain clearer visibility into its third-party control environment.

SISA's 5-Step Framework to TPRM

Phase 1

Pre-Onboarding Checks

The engagement began with structured pre-onboarding to define scope, vendor category, and assessment type for each third party. This included obtaining the approved scope and vendor classification from the bank, completing conflict-of-interest checks to ensure assessment independence, and receiving final onboarding confirmation from business teams.

Phase 2

Project Initiation

SISA initiated the assessment with vendors and bank stakeholders to establish governance, timelines, ownership, and communication protocols. Formal kick-off meetings were conducted with the vendor and the bank's business and compliance teams to align on the audit methodology, evidence expectations, reporting approach, submission timelines, and the set-up of secure evidence-sharing channels such as SharePoint, and escalation mechanisms.

Phase 3

Project Execution

SISA conducted detailed vendor assessments based on the agreed checklist, service profile, risk category, and applicable regulatory requirements. This included business and service walkthroughs, interviews, workshops, document reviews, evidence collection, and validation against customized checklists mapped to RBI outsourcing requirements, DPDPA, and PCI DSS. Online evidence verification calls were also conducted to confirm the authenticity and relevance of submitted evidence.

Phase 4

Reporting

Post fieldwork, SISA prepared structured audit reports with control-wise assessment results. The team conducted internal reviews with the bank's business and compliance stakeholders, held vendor debriefing sessions to clarify observations, and submitted final reports with clear findings, practical recommendations, and closure expectations.

Phase 5

Remediation Validation & Closure

The final phase focused on gap closure, remediation tracking, and formal project closure. SISA shared identified gaps and remediation expectations with vendors, revalidated closure evidence, conducted closing meetings where required, published final reports after validation and sign-off, and provided periodic status updates to the bank until all vendor assessments were completed.

SISA planned the overall delivery strategy, project schedule, and vendor-wise tracking system under strictly defined turnaround times for each activity. To reduce the administrative burden of repetitive annual vendor spreadsheets, SISA applied multi-framework and unified control inheritance mapping that helped streamline evidence gathering across regulatory standards. Actionable, risk-prioritized recommendations were provided to support practical remediation and continuous improvement.

Business Impact

SISA's TPRM program delivered value beyond regulatory compliance by helping the bank establish a more structured, scalable, and risk-focused approach to vendor governance.

Enhanced Regulatory Readiness

The engagement improved the bank's ability to demonstrate compliance with RBI outsourcing requirements, DPDPA obligations, and PCI DSS expectations through a consistent and documented vendor assessment process.

Improved Third-Party Risk Visibility

The bank gained comprehensive visibility into the control environment, risk posture, and compliance status of more than 100 vendors, enabling informed risk management decisions and prioritization of remediation activities.

Reduced Operational Burden

SISA assumed responsibility for vendor coordination, evidence collection, audit scheduling, follow-ups, reporting, and remediation validation, significantly reducing the administrative effort required from the bank's business, procurement, compliance, and information security teams.

Stronger Vendor Governance

The program established a repeatable framework for vendor onboarding assessments, periodic reviews, remediation tracking, and ongoing third-party oversight, strengthening the bank's overall TPRM maturity.

Actionable Risk Reduction

Risk-prioritized observations and practical remediation recommendations enabled vendors and bank stakeholders to address control weaknesses systematically and improve their security, privacy, and compliance posture.

Scalable Foundation for Future Growth

The engagement provided the bank with a scalable assessment model capable of supporting future vendor onboarding, regulatory reviews, and continuous third-party risk management initiatives.

Conclusion

Through its risk-based assessment methodology, unified control framework, and scalable delivery model, SISA helped the bank strengthen vendor governance, improve regulatory readiness, and establish a sustainable foundation for ongoing third-party risk management. The engagement demonstrates how organizations can transform vendor assessments from periodic audits into a continuous risk governance capability.

About SISA

SISA is a global leader in cybersecurity for the payment ecosystem, operating at the intersection of AI, cybersecurity, and payments. Trusted by leading brands and financial institutions across 40+ countries, SISA secures over 1,000 organizations by helping them anticipate threats, strengthen resilience, and protect critical payment infrastructure. Powered by real-world breach intelligence, SISA enables organizations to stay ahead of evolving cyber risks. Follow SISA on LinkedIn for the latest insights on cybersecurity, payment security innovation, and emerging technologies.

SISA's Portfolio of Forensics-driven Cybersecurity Solutions

Compliance

Payment Security

- PCI DSS Compliance
- PCI PIN
- PCI 3D Secure (3DS)
- PCI P2PE Compliance
- PCI S3
- PCI S-SLC
- PCI CP (Card Production)
- PCI SAQ Compliance
- Facilitated PCI SAQ
- Quarterly Health Check-ups
- Central Bank Compliance

Strategy & Risk

- SWIFT
- HIPAA
- ISO Management System Services
- NIST
- SOC Compliance
- HITRUST Certification
- Information Security Risk Assessment
- CSA STAR Assessment & Certification
- Crisis Management Exercise / Crisis Management & Incident Response Simulation Exercises
- Indian Regulatory Cybersecurity Audit & Assurance Services

Unified Audits

Managed Compliance

Security

Security Testing

- Application Security Testing
- Infrastructure & Network Security
- Cloud & Container Security
- IoT Security Testing
- Adversary-Led Ransomware Simulation
- Red Teaming

ProACT Agentic SOC

Digital Forensics & IR (DFIR)

- Payment Forensics Investigation
- Internal Forensic Investigation
- Acquirer Led Investigation
- Ransomware Incident Response
- Breach and Attack Simulation
- Compromise Assessment
- Cloud Forensics
- Retainer Services
- Digital Threat Report Briefing Session

PRISM

- Prism Discovery (AIBOM)
- Prism Strike (Gen AI app PT)
- Prism Secure (Model Security)
- Prism Observe (Live AI App monitoring)

Quantum Security

Privacy

Data Protection and Governance

- SISA Radar (Discovery & Classification)

Data Privacy Consulting Services

- DPDPA (India) Compliance Consulting
- GDPR
- CCPA

SISA is a global cybersecurity leader for the payments ecosystem

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia

To learn more about SISA's offerings visit us at www.sisa.ai or
Contact your SISA sales representative at contact@sisa.ai