2025
ASIA-PACIFIC
COMMUNITY
MEETING

PCI DSS Excellence:

Integrating Governance, Risk, and Strategy

PCI Security Standards Council

concentrix

Rishi Rajpal

Global Vice President – Global Security
Concentrix Solutions Corporation

PCI Security Standards Council

Navigating PCI-DSS

A Service Provider's Perspective

In today's rapidly evolving digital landscape, service providers face increasing challenges in maintaining PCI-DSS compliance while effectively managing governance, risk, and strategy.

Attackers exploit trusted relationships between clients and vendors. A compromised vendor can become a gateway to multiple downstream clients.

Cyber Criminals

Service Providers

Client's Infra

Key Impacts

Reputational Damage
Loss of client trust and market credibility.

Financial Losses
Remediation costs, legal liabilities, and potential lost business.

Operational Disruptions
Downtime, data loss, or supply delays.

Increased Scrutiny
Stricter audits, compliance checks, and security demands from clients.

Loss of Business Opportunities
Risk of being excluded from new or existing engagements.

PCI Security Standards Council

Guardians of Cardholder Data

The Essential Role of Service Providers in PCI-DSS Compliance

Empowering PCI Compliance

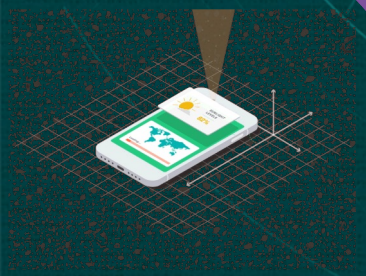
Securing the Payment Ecosystem

Beyond Compliance

PCI DSS

Trusted Partners in Protection

Service Providers at the Core



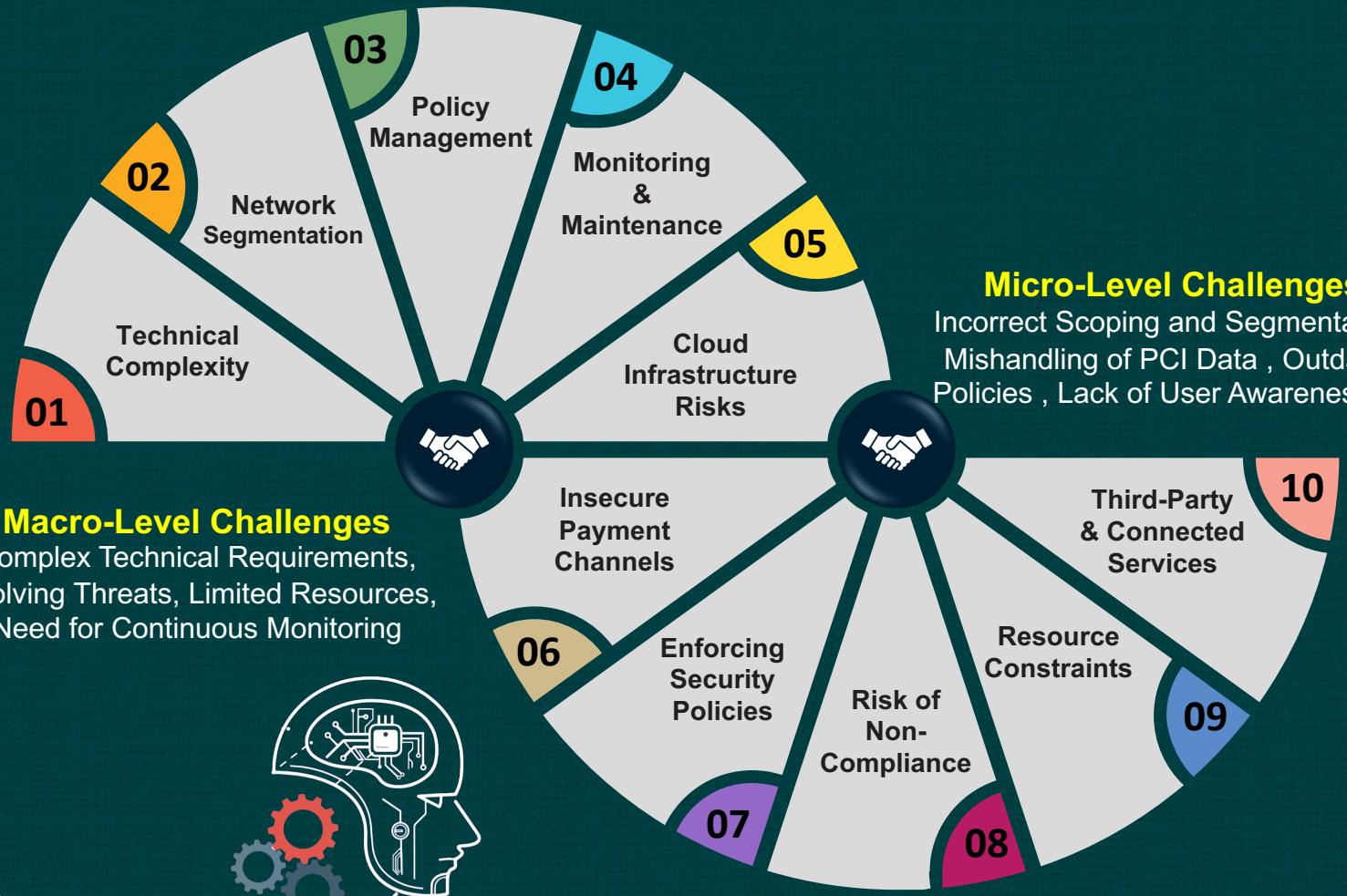
Operational Excellence in PCI Compliance Support

- Adhering to PCI DSS
- Proactive Security
- Collaborative Compliance
- Supporting Merchant Compliance

PCI Security Standards Council

Navigating Complexity

Challenges for Service Providers in a Cyber-Driven World



Micro-Level Challenges
Incorrect Scoping and Segmentation, Mishandling of PCI Data , Outdated Policies , Lack of User Awareness, AI

Macro-Level Challenges
Complex Technical Requirements, Evolving Threats, Limited Resources, Need for Continuous Monitoring

PCI Security Standards Council

AI : Adding Fuel To Fire ?

PROMPT INJECTION SCAM

Exposes need for AI monitoring in cardholder data environments. Fake price promise, **public embarrassment**

RETAIL BOT UNAUTHORIZED DISCOUNTS

Requires access control and transactional logging under PCI DSS. **$3.5 million** lost in just 48 hours

FINTECH AI MAKING PAYMENTS

Necessitates robust authentication and audit trails for AI transactions. leading it to execute **$4 million** in unauthorized transfers

“IMPROMPTER” DATA EXTRACTION

High data exposure risk, possible PII/cardholder data leak

DEEPFAKE VOICE AUTH BYPASS

Undermines secure authentication; high-risk under AI regulations. , enabling unauthorized **$25 million USD** in transfers.

PCI Security Standards Council

Governance, Risk Management and Compliance

Strategic Must-Do's

Executive Oversight

Involvement of Leadership is Critical for setting direction and ensuring accountability.

Defined Roles & Responsibilities

Clear assignment of PCI roles and responsibilities across security, compliance, IT, Business, and other teams.

Risk Management

Protecting the Cardholder Data Environment (Accurate CDE scoping – Crucial, Periodic Risk Assessments, Risk Register and Corrective Actions, PCI Asset Inventory Maintenance).

Third-Party Oversight & Monitoring

Service Providers must also comply with PCI requirements under governance controls.

Continuous Monitoring

Regular audits, compliance checks, and performance reviews , KPI dashboards to ensure ongoing compliance and health checks.

PCI Security Standards Council®

AI Powered Compliance

Automating PCI in the Age of Intelligence

- Behavioral biometrics for continuous user authentication
- AI-enabled data classification by sensitivity & type
- Intelligent access anomaly detection & control enforcement

- AI-driven automated scanning & risk identification
- ML-based vulnerability prioritization for efficient remediation
- Proactive patching using AI-powered workflows

- Continuous AI-based compliance surveillance
- Automated policy review & audit documentation generation
- AI-augmented audit readiness & real-time reporting

- Real-time anomaly detection across logs, traffic, and endpoints
- Predictive analytics for threat anticipation
- Enhanced malware & phishing defense using behavioral AI

- Automated incident isolation & mitigation actions
- AI-assisted forensic log analysis for faster breach resolution

PCI Security Standards Council®

Shortest Route to PCI DSS Compliance

Cheat Sheet for Service Providers

Secure Network & System Hardening

- Secure and maintain PCI systems
- Manage threats with updates & patches

Cardholder Data Protection

- Encrypt, manage keys, and tokenize data
- Minimize and retain data only as needed

Access Controls & Authentication

- Use least privilege + MFA
- Unique IDs with activity logs
- Restrict physical CHD access

Monitoring, Testing & Incident Response

- Run vuln scans, pen tests & log reviews
- Enable real-time monitoring & alerts
- Test & maintain breach response plan

Security Policies, Training & Governance

- CISO-led security policy & awareness training
- Separate implementation & verification teams

Continuous Compliance & Improvement

- Ongoing threat assessments
- Documentation & third-party reviews

PCI Security Standards Council®