2025
EUROPE
COMMUNITY
MEETING

# It’s Not You, It’s Us - Strategy for Building a Shared Security Responsibility Model With Your Service Providers

PCI Security Standards Council

## Troy Leach

Chief Strategy Officer
Cloud Security Alliance

## Ted Tanner

Principal Assurance Consultant
AWS Security Assurance Services

## Bruno Kovacs

Head of Security Standards
Card Payments
Cartes Bancaires (CB)

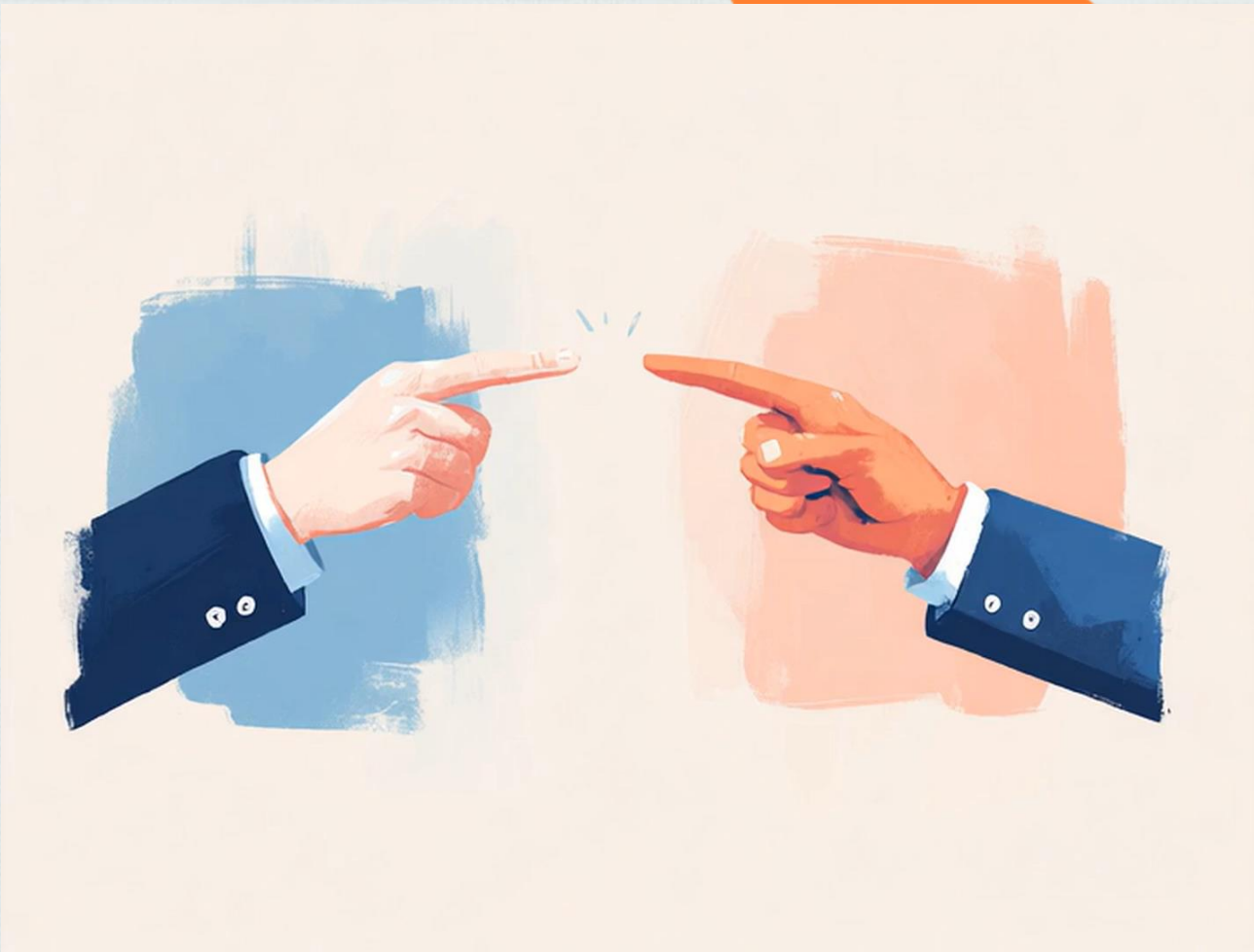
PCI Security Standards Council

# The Shift

## Secure organizations treat CSPs as extended security team

Old Model: Point fingers when compliance fails

New Reality:  PCI DSS v4.x Appendix A creates joint accountability



PCI Security Standards Council

# Collaborative Stakeholder Ecosystem

## Internal Partnership

IT Procurement and Security Teams should be aligned with PCI objectives

*A1.1*
*Does CSP separate all customer environments?*

## MTSP Partnership

Shared Security Responsibility Model for transparency and clarity

*A1.2*
*How do they commit to incident response or pentesting?*

## QSA/ISA Integration

Greater consistency and timeliness in evidence requests through machine language (e.g. OSCAL)

## Dynamic Capabilities

Continuous monitoring, security automation and harmonized governance when designing with dynamic features

PCI Security Standards Council

# Managing Every Cloud Service

- Open Controls Framework mapped to PCI DSS v4.x
- STAR registry is a free database of 3,400+ cloud service providers
- Provides SSRM attestation by CSPs for consideration

CAIQ™ CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE

| Question ID | Question | SSRM Control Ownership |
|---|---|---|
| A&A-01.1 | Are audit and assurance policies, procedures, and standards established, documented, approved, communicated, applied, evaluated, and maintained? | |
| A&A-01.2 | Are audit and assurance policies, procedures, and standards reviewed and updated at least annually? | CSP-owned<br>CSC-owned<br>3rd-party outsourced<br>Shared CSP and CSC<br>Shared CSP and 3rd-party |
| A&A-02.1 | Are independent audit and assurance assessments conducted according to relevant standards at least annually? | |

*Quick way to review hundreds of CSP claims for security responsibility expectations and PCI DSS requirements*

PCI Security Standards Council

# Partnership in Practice

## Provisioning digital cards from a multi-tenant environment

PCI Security Standards Council

# Partnership in Practice

## Case study: cloud-based digital cards provisioning

- French domestic scheme digital platform connecting Card Issuers, Token Requestors and Token Service Provider.
- Move-to-cloud decision driven by the business.
- Shared accountability between CB and TPSPs for tens of thousands of card enrolments per day.

## Initial challenges and risk considerations

- Supply chain – operations spread across multiple TPSPs.
- Reduced oversight and transparency. Multi-tenant cryptography-as-a-service seen as “black box”.
- Dependency on the underlying CSP technology and vendor lock-in could create risks to business continuity.
- Exposure to extraterritorial jurisdiction.

*TPSP: Third-Party Service Provider*

*CSP: Cloud Service Provider*

PCI Security Standards Council

# Collaboration Success Factors From GRC Perspectives

## Security assurance requirements

- Setting a security assurance framework that is fit for purpose – in collaboration with your TPSPs.

## Engaging with TPSPs for regulatory compliance

- Make sure TPSPs are aware of their share of responsibilities (e.g., GDPR, DORA).
- Leverage TPSP-led initiatives supporting regulatory compliance.

## Know your SSRMs

- Cloud service level
- Security framework level
- Cyber-security regulations
- Data privacy regulations
- …

## Work with your TPSPs

- Resolve transparency issues with 1:1 discussions.
- Resolve contractual issues.
- Leverage managed (key) services, GRC tools, automate when possible.

*CSA CCM: Cloud Security Alliance Cloud Controls Matrix*

*SSRM: Security Shared Responsibility Matrix*

PCI Security Standards Council

# Collaboration Success Factors (Business)

Ability of TPSP to implement regional functional requirements (API, protocols…)

Ability of TPSP to meet our service continuity requirements

Provide the means to test this capability

Ability of TPSP to accommodate interoperability requirements for multi-cloud deployments and exit strategies

# Partnership Foundations

## Cloud Providers as Extended Teams

Shift from "vendor-client" to "integrated security partnership" mindset

Leverage cloud providers as extensions of your security and compliance programs

## Responsibility Boundaries

Clearly define where responsibility lines are drawn for each CSP service used

Document expectations in your own service-specific matrix

## Service Provider Security Investments

Access to advanced security capabilities at fraction of in-house costs

Benefit from cloud providers' extensive security expertise and threat intelligence

## Cloud Provider Capabilities

Automation to monitor for and remediate drift

APIs to integrate compliance monitoring into existing tooling

# Operationalizing Cloud Governance

**Policy-Driven Governance**

Centralized policy management for consistent control implementation

Automated guardrails that enforce compliance requirements

**Compliance Automation ROI**

Time and resource savings – preparation, evidence collection

Reduce human error

Enhanced data security

**Boundary Verification**

Continuous monitoring of control effectiveness across environments

Automated permissions, segmentation testing

# Key Takeaways

## Leverage TPSP Offerings

Cloud provider tools have vast capabilities to enhance your security of payment and business processes

## Leverage Regulatory Compliance Initiatives

Harness ICT Providers' cyber resilience efforts to meet your PCI DSS validation more efficiently.

## Leverage Existing Resources

Take advantage of existing and emerging assurance techniques to help with third-party validation

PCI Security Standards Council