PCI Security Standards Council®

Legend of AI and Cloud Security

Troy Leach

Chief Strategy Officer
Cloud Security Alliance

Son Ho

President -CSA Vietnam Chapter
Co-founder & VP – Robusta Technology

PCI Security Standards Council

About CSA and Vietnamese Chapter

CSA Vietnam Chapter founded in 2015, with 3 co-founders and 15 starting members.

The chapter has organized many Vietnam Summits, webinars, local meetings as well as participating in local IT industry's events.

Our objectives and missions include the following:

- Promote secure cloud adoption in Vietnam and recruit members (volunteers) for the CSA Vietnam Chapter.
- Enhance cloud and cybersecurity knowledge within the community.
- Network with local and global peers facing similar cloud security challenges.
- Advocate best practices for cloud security, providing education and consulting on CSA's international standards and frameworks.

PCI Security Standards Council®

What We Hope You Take Away

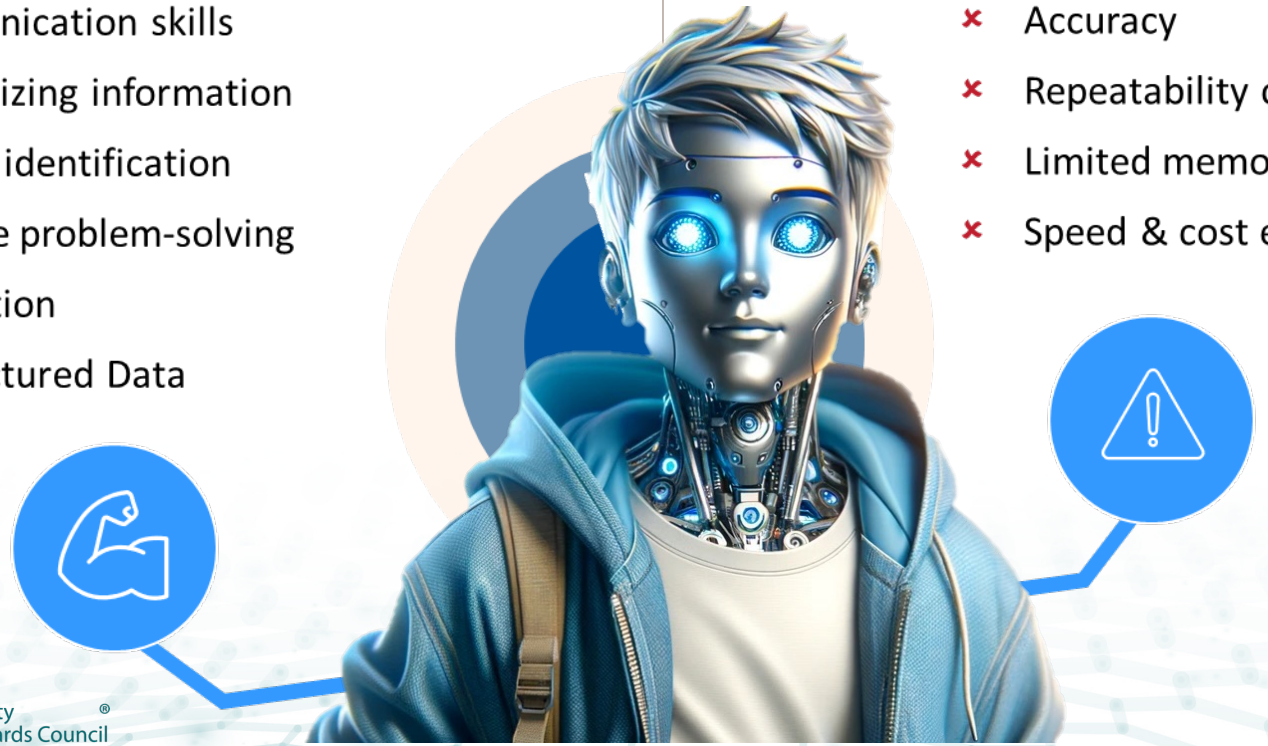
- Impactful Differences of GenAI and Cloud
- Identify what we can leverage from our established best practices and experiences
- Identify where we must be pioneers in security and auditing

PCI Security Standards Council

What is AI Good At?

AI Strengths:

- ✓ Reasoning and logic
- ✓ Communication skills
- ✓ Synthesizing information
- ✓ Pattern identification
- ✓ Creative problem-solving
- ✓ Translation
- ✓ Unstructured Data



AI Limitations:

- × Non-deterministic behavior
- × Accuracy
- × Repeatability challenges
- × Limited memory retention
- × Speed & cost efficiency

"Genius 13-year-old. Overconfident with short attention span and no street smarts"

PCI Security Standards Council

AI and Cloud Adoption in Payments

Substantial changes that have occurred in recent ~~years~~ months

Payment Data in Cloud

- Large volume of payment processing
- Immediate accessibility to global resources
- Continuous Assurance
- Critical Back Up Assurance
- Scalability to modify immediately

Payment Data in AI

- Personalization of Services
- Identify Payment Patterns
- Automation of policy and procedures
- Use of Synthetic Data

PCI Security Standards Council

New Opportunities with GenAI + Cloud

"Just Walk Out" technology, which uses AI and cloud computing to enable checkout-free shopping experiences, processes millions of transactions annually

65% of large retailers have implemented some form of AI

Cloud adoption in the retail payments industry has reached higher than 80%,

40% of retailers experimenting with GenAI for payments

McKinsey: GenAI could add equivalent of $2.6T – 4.4T of value annually

PCI Security Standards Council

Data + GenAI Will Drive Major Transformations in Payments

Where Payment Data May Exist

Unstructured Data

Google Drive
Google Cloud Storage
GCP Firebare
Slack
Azure Files
OneDrive
Amazon S3
Box
DropBox
NFS
SMB
Oracle Object Storage

DataCommand Graph
Single Source of Truth

GCP BigQuery
Snowflake
MongoDB
IBM DB2 Cloud
MariaDB
Salesforce
Azure Cosmos DB
Apache Hive
Amazon DynamoDB
Workday
Databricks
MySQL

Structured Data

GenAI Models

Multicloud
AI Models + Agents

AI Agents

GenAI Apps & Innovation

- Copilots & Assistants
- Business Process Automations
- New Category of Apps
- Insights & Analytics

GenAI Apps & Assistants

PCI Security Standards Council

Example of AI Agent in Payments

- Increase in use for chatbots and other consumer interfaces
  - What happens when AI creates its own company policy?
- Overprivilege of access to AI Assistants
  - What happens when users AI assistants have access to everything?
  - MS report stating more than 50% of accounts have super privilege to access sensitive information

PCI Security Standards Council

Top Security Uses for AI

Reasoning and Logic enables better **Rule Creation**

Creative Problem Solving Empowers **Attack Simulation**

Pattern Identification Increases **Regulatory Adherence**

Synthesizing large data sets Improves **Detection**

21%	Rule creation	13%	Natural language to search
19%	Attack simulation	13%	Threat summarization
19%	Compliance violation monitoring	13%	Data loss prevention, IP protection
16%	Network detection	11%	User Behavior analysis
16%	Reduce false positives	10%	Automated report generation
15%	Training development and support	10%	Endpoint detection
14%	Anomaly classification	9%	Event log summarization

PCI Security Standards Council®

AI Proactive Security In Payments

Emerging techniques that are here today and will help you tomorrow

Incident Investigation

Can conduct Root Cause Analysis by combing through massive amounts of data quickly to identify anomalies in network traffic and system logs to pinpoint origin of attack

AI tools can reconstruct the sequence of events leading up to an incident

Intelligence Analysis

Aggregate and analyze threat intelligence from multiple sources, continuously to report on emerging attack vectors

Can be trained to initiate predefined responses such as isolating affected systems

Training and Onboarding

AI can analyze data from different department and roles to understand unique challenges and generate training material relevant to the employee

When staff make an inquire for elevated access which is not permitted, AI can Slack the individual to coach them on why access was denied

Documentation and Reporting

Can monitor all changes to the environment and create continuous assurance that the all documentation is current

Can generate multi-queries to analyze various regulations and use cases for data and assign controls to relevant framework

PCI Security Standards Council®

AI Agent Example for New Payment Transaction

Identifying legitimacy of new payment transaction in network

- Example of how AI would evaluate risk from intel gathered from Jira, Slack, meeting minutes
- New payment transaction identified.

Payment processor is a trusted provider & only outbound calls are allowed

Engineering documentation and discussions have identified this new payment provider being implemented

Payment processor libraries were introduced to code repo “payment-lib” on 3.3.2024

A **discussion with Anna who is the active contributor** to “payment-lib” occurred at 1:22pm PT 3.3.2024 via Slack to confirm the domain stripe.com is allowed outbound

PCI Security Standards Council

Company Policy for LLM or Cloud Services

Basics to be mindful when staff engage with public models and infrastructure

- Identify AI and Cloud security professional(s) responsible for PCI responsibilities
- Catalog all approved LLM and cloud activities and scan for shadow access
- Create an official corporate AI Policy
- Communicate and Train on AI Policy
- Monitor activity and perform pentesting
- Stay informed on latest changes in LLM security

Cloud Security Risk in Payments

Top Threats t

1. Misconfigu
2. Identity & A
3. Insecure In
4. Inadequate
5. Insecure T

2024		2022
Misconfiguration & Inadequate Change Control	1	Identity & Access Mgmt (IAM)
Identity Access & Mgmt (IAM)	2	Insecure Interfaces and APIs
Insecure Interfaces and APIs	3	Misconfiguration & Inadequate Change Control
Inadequate Selection/ Implementation of Cloud Security Strategy	4	Inadequate Selection/ Implementation of Cloud Security Strategy
Insecure Third-Pary Resources	5	Insecure Software Development
Insecure Software Development	6	Insecure Third-Party Resources
Accidental Cloud Disclosure	7	System Vulnerabilities
System Vulnerabilities	8	Accidental Cloud Disclosure
Limited Cloud Visibility/ Observability	9	Misconfiguration & Exploitation of Serverless & Container Workloads*
Unauthenticated Resource Sharing	10	Advanced Persistent Threats
Advanced Persistent Threats	11	Cloud Storage Data Exfiltration*

*Security issues not in the top 11 for 2024

PCI Security Standards Council

Cloud Security Opportunities in Payments

Industry Research

- **Cloud Security Guidance**
  - Zero Trust Methodology
  - CI/CD
  - Security Monitoring and Ops
  - Resiliency
  - Cloud Telemetry & Security Analytics

Protecting Payment Data

- Confidential Computing
- Fully Homomorphic Encryption (FHE)
- Cloud Enclaves
- Data Lakes
- Network Security Zones
- Cloud HSM

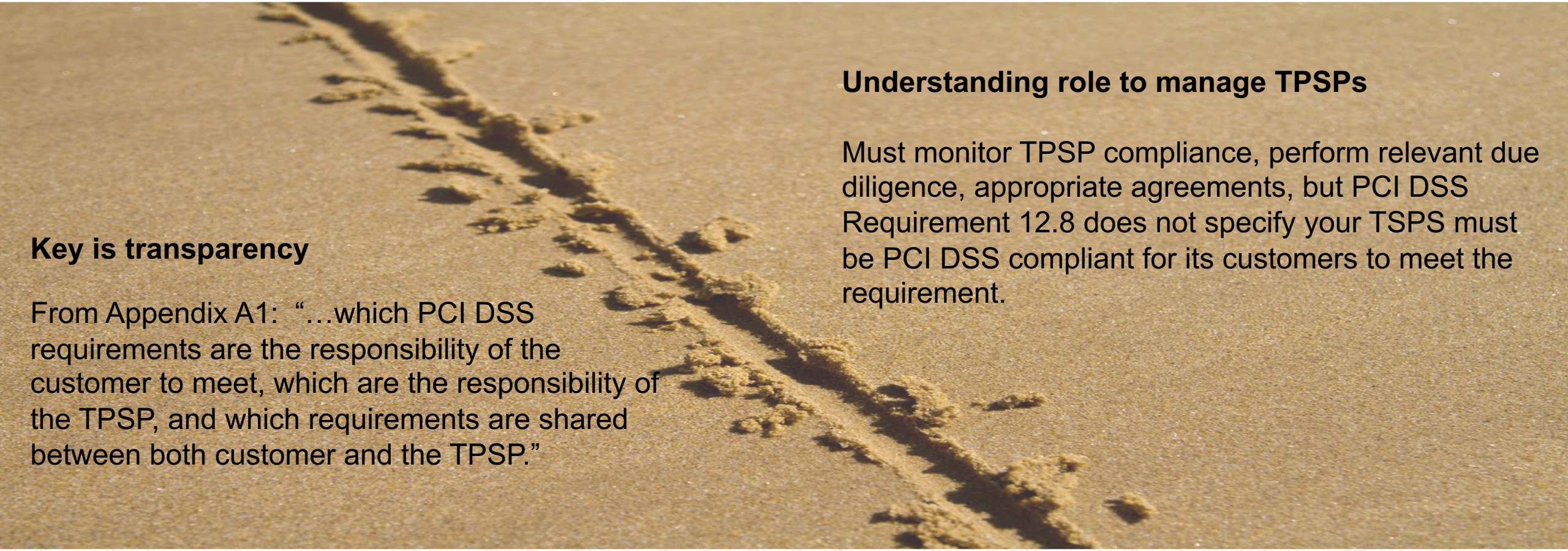
PCI Security Standards Council

Shared Security Responsibility Model

A common interpretation of cloud service responsibility

PCI Security Standards Council

Shared Security Responsibility Model



Key is transparency

From Appendix A1: "…which PCI DSS requirements are the responsibility of the customer to meet, which are the responsibility of the TPSP, and which requirements are shared between both customer and the TPSP."

Understanding role to manage TPSPs

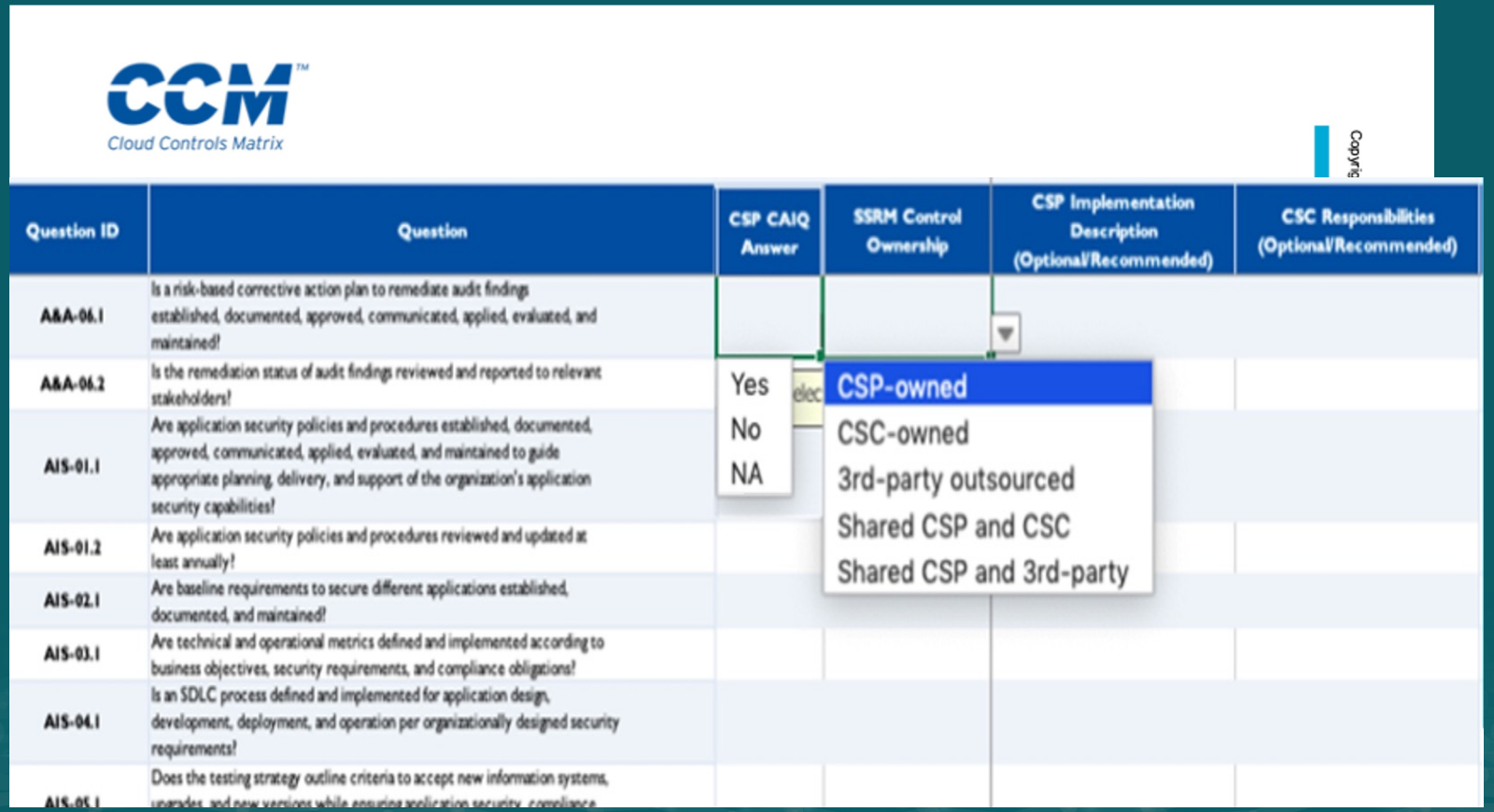
Must monitor TPSP compliance, perform relevant due diligence, appropriate agreements, but PCI DSS Requirement 12.8 does not specify your TSPS must be PCI DSS compliant for its customers to meet the requirement.

How SSRM Within Cloud Controls Matrix Works

CSA's Shared Responsibility Model works in with same principles of PCI Council's: *PCI DSS Cloud Computing Guidelines*

As well as PCI SSC's *Information Supplement: Third-Party Security Assurance*

SSRM is embedded as part of the Cloud Controls Matrix



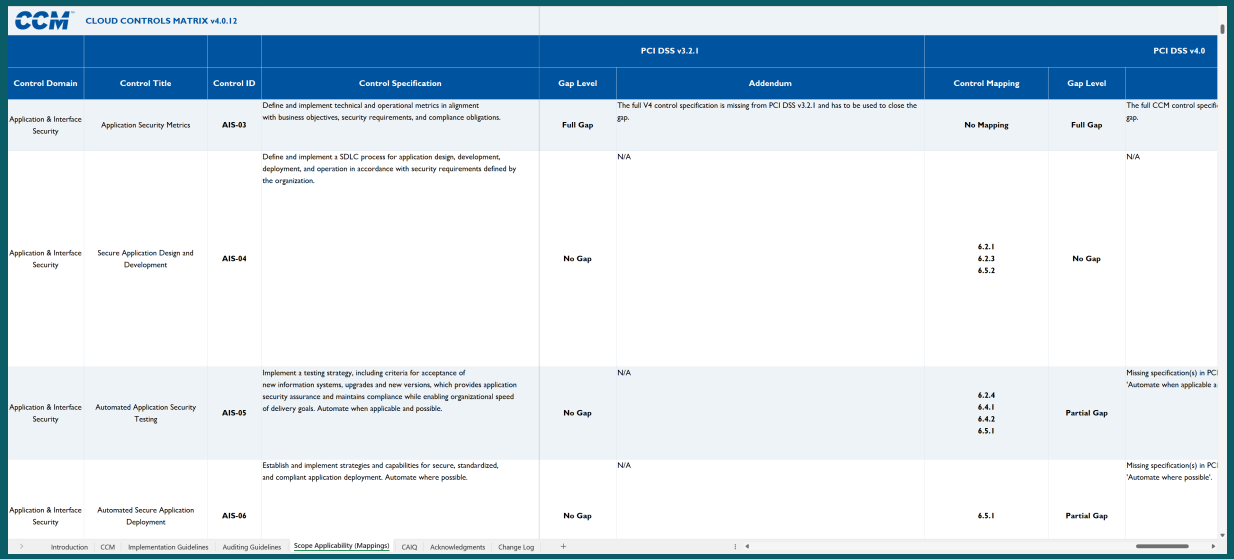
PCI Security Standards Council

Mapping of PCI DSS v4.0 to CCM v4

A method to identify shared responsibilities from the CSP perspective

- Analyze self-assessment or independent assessments for ISO 27001, SOC2 that have evidence for security practices of TPSPs

- Could be used as one source
  - 77% No or Partial Gap
  - 23% Full Gap due to different focus



CCM CLOUD CONTROLS MATRIX v4.0.12

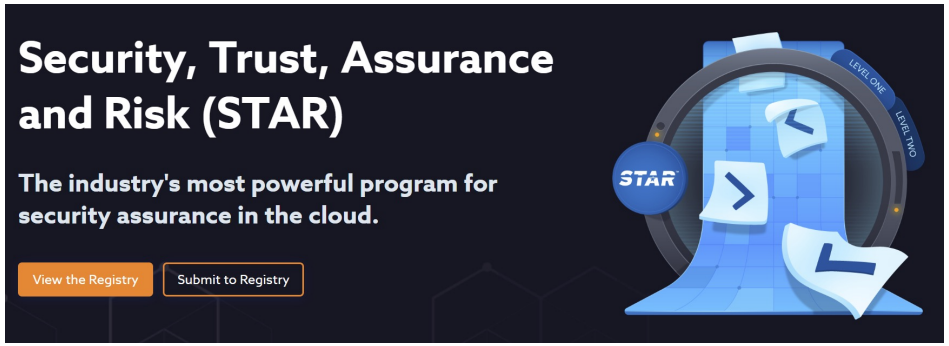
				PCI DSS v3.2.1		PCI DSS v4.0		
Control Domain	Control Title	Control ID	Control Specification	Gap Level	Addendum	Control Mapping	Gap Level	
Application & Interface Security	Application Security Metrics	AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	Full Gap	The full V4 control specification is missing from PCI DSS v3.2.1 and has to be used to close the gap.	No Mapping	Full Gap	The full CCM control specifi gap.
Application & Interface Security	Secure Application Design and Development	AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	No Gap	N/A	6.2.1 6.2.3 6.5.2	No Gap	N/A
Application & Interface Security	Automated Application Security Testing	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance while enabling organizational speed of delivery goals. Automate when applicable and possible.	No Gap	N/A	6.2.4 6.4.1 6.4.2 6.5.1	Partial Gap	Missing specification(s) in PCI 'Automate when applicable a
Application & Interface Security	Automated Secure Application Deployment	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	No Gap	N/A	6.5.1	Partial Gap	Missing specification(s) in PCI 'Automate where possible'.

Introduction | CCM | Implementation Guidelines | Auditing Guidelines | Scope Applicability (Mappings) | CAIQ | Acknowledgments | Change Log

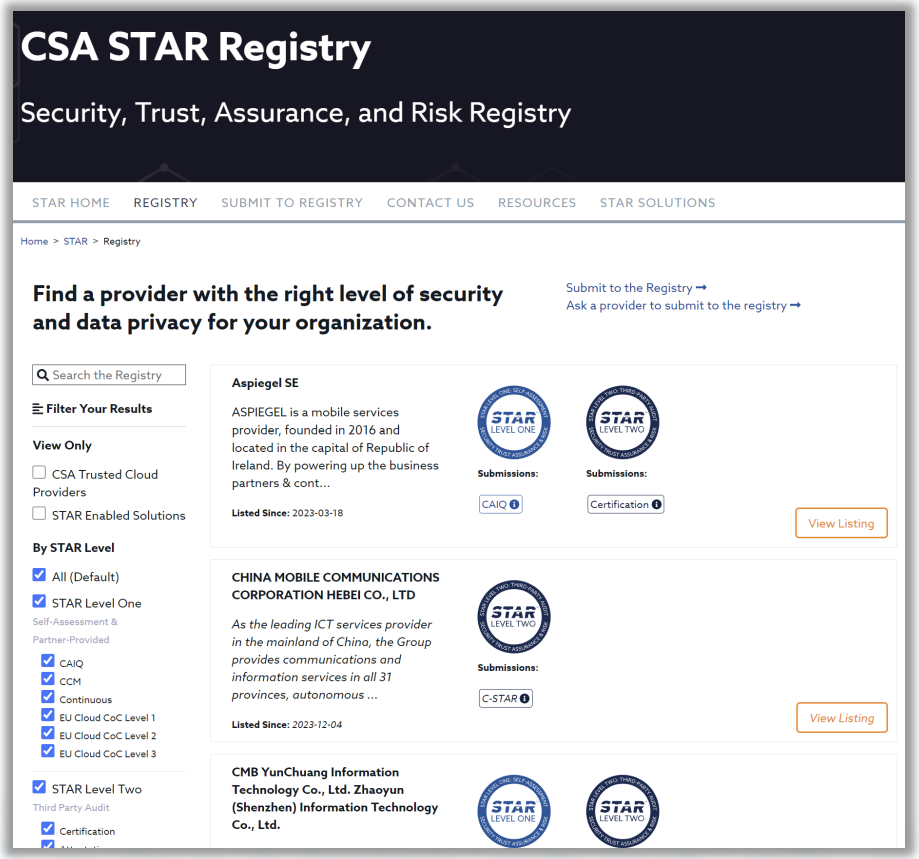
PCI Security Standards Council®

Cloud Service Provider Reports Available in STAR

- STAR Registry is a free database for both cloud customers and cloud providers to share the results of their self-assessment or third-party assessments.



https://cloudsecurityalliance.org/star



PCI Security Standards Council

Thank you

Free Resources and Contact Information for CSA

- International CSA website:
  - *http://cloudsecurityalliance.org*
- Local Chapters:
  - *https://cloudsecurityalliance.org/chapters*
- CCM (PCI DSS Mapping within Framework):
  - *https://cloudsecurityalliance.org/research/CCM*
- CSA Vietnam Chapter's website: csavietnam.org
- Key contacts of CSA Vietnam Chapter:
  - Mr. Ho Thanh Son (Son Ho): www.linkedin.com/in/sonhovn
  - Mr. Cao Nguyen Viet Hung (Philip Cao): www.linkedin.com/in/philipcao

PCI Security Standards Council®


PCi
Security
Standards Council
®