# PCI SSC Community Meeting Workshop Summary

# PCI DSS v4.0.1 – Challenges and Success Stories

**Workshop Objective:** Provide merchants, service providers, and other stakeholders an opportunity to share challenges and successes implementing PCI DSS v4.0.1

| Workshop Discussion Questions |
|---|
| How would you describe your organization's current stance on PCI DSS v4.0.1? |
| Which elements of v4.0.1 are going smoothly or already delivery value for your security program? |
| Where have you faced the greatest difficulty? |
| What recent changes in requirements, processes or business practices have had the biggest impact? |
| Looking ahead, what would a successful v4.0.1 implementation look like in your organization and what collaboration would you like to see from the industry? |

## Industry Insights:

- ✚ More organizations treating PCI DSS as a year-round security program, versus an annual compliance exercise.
- ✚ Automated evidence collection and compliance processes are increasingly used.
- ✚ Tokenization has reduced scope and simplified assessments.
- ✚ Targeted Risk Analysis (TRA) has streamlined compensating controls and improved flexibility.
- ✚ Clarifications (e.g., 90-day timeframe requirements) have reduced ambiguity.
- ▬ Increased documentation and evidence complexity are resource intensive.
- ▬ Increased authentication requirements (12-character passwords, MFA, etc.) require significant user education and system configuration changes.
- ▬ Transitioning to cloud environments and managing third-party relationships adds requirement adherence complexity.
- ▬ The use of audit and GRC tools is growing, but customization and integration remain challenges.
- ▬ Limited use of Customized Approach due to complexity.

| Ongoing Industry Opportunities |
|---|
| Facilitated peer discussions and workshops for information sharing are considered high-value. |
| Continued practical guidance, templates and use cases from PCI SSC are important resources. |
| Industry interest in additional ongoing global education on payment data security best practices. |