
PCi
Security
Standards Council
®

PCI Security Standards Council

Ace Your PCI DSS v4.0 Assessment

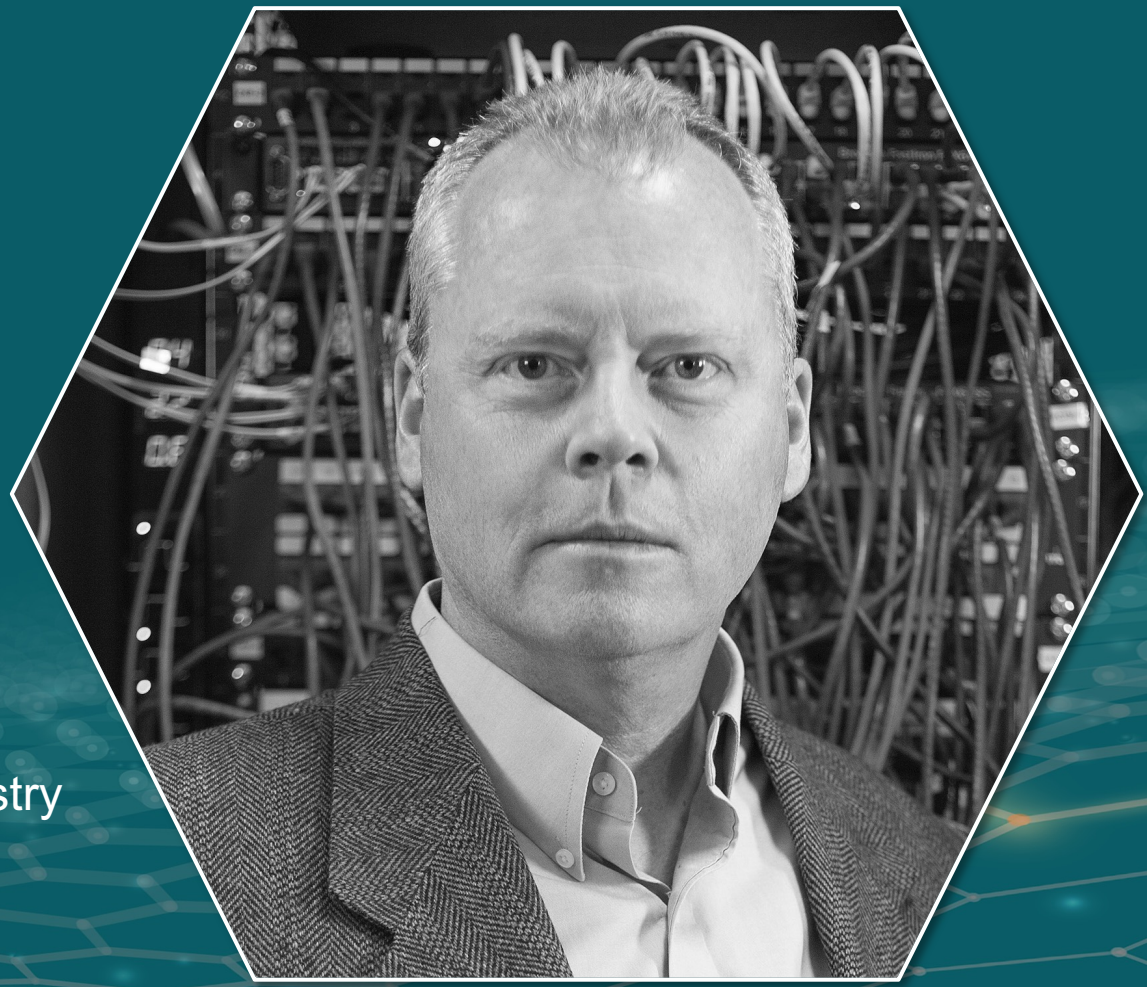
QSA Secrets for Success

PCI Security Standards Council®

Gary Glover

VP of Assessments, USA

securityMETRICS®



- 20 years in Cybersecurity and Payment Card Industry
- Participate in SIG's, GEAR, etc.
- 10 years as a Software Developer
- 7 years as a Mechanical Engineer

Agenda

- Summary of Changes
- Preparation Tips
- Immediately Applicable Requirements
- Common Issues in 2024
- Future Dated Requirements Summary
- Hardships for 2025
- Ecommerce Skimming Issues
- Looking Forward
- Key Takeaways

PCI Security Standards Council®

Changes to PCI DSS v4.0

- 53 new requirements apply to all entities
- 11 new requirements for service providers
- 13 of this total are effective immediately
- Till March 31, 2025 not much different than v3.2.1

PCI Security Standards Council

Preparation Tips

What to Think About Before Diving In?

- Do your homework
- Project management, milestones and goals
- Good network and data flow diagrams
- Scoping, get the right group together
- Plan for extra assessment time
  - Addressing future dated requirements
  - Report writing by QSA

PCI Security Standards Council®

Preparation Tips

What Do I Consider Between 2024 and 2025 Assessments?

- Finishing v4.0 ROC just before March 2025 deadline
  - Are you off-the-hook for future dated requirements?
    - Point in time audit, yes
    - Don’t forget periodic requirement evidence
  - Moving ROC date earlier to avoid future dated requirements…BAD IDEA
- Consider discussion with QSA before implementing some future dated requirements
  - Keyed hash algorithm procedures (3.5.1.1)
  - Inventory of payment page scripts loaded or executed (6.4.3)
  - Internal MFA access and MFA features (8.4.2, 8.5.1)
  - Authenticated internal scans (11.3.1.2)
  - Payment page tamper detection solution (11.6.1)

PCI DSS v4.0 Immediately Applicable

Quick Summary

- VA scans for SAQ A (iFrame or hosted order page)
- Formal reconfirmation of scope annually (12.5.2)
- Roles and responsibilities for performing activities in each PCI DSS section (x.1.2)
- Raised bar on service providers for compliance responsibility documents for customers

PCI Security Standards Council®

2024 Compliance Assessments

Hints/Pitfalls

- QSA noted problems
  - Service provider responsibility acknowledgement documentation (12.8.2)
  - VA scanning for small merchants with iFrame ecommerce
  - Most are putting off future dated requirements, even simple ones
  - More overall documentation paperwork is required
- QSA noted successes
  - Clients say 4.0 is easy to complete without the future dated
  - Most clients are taking preparation for future dated requirements seriously
  - Getting more QSA questions on future requirements since July

PCI DSS 4.0 Future Dated Requirements

Biggest Changes

- Keyed hashes (3.5.1.1)
- Phishing protection & training (5.4.1, 12.6.3.1)
- Payment page script management and detection (6.4.3, 11.6.1)
- Targeted Risk Analysis Processes
- MFA for all access to CDE (8.4.2)
  - MFA system features (8.5.1)
- Authenticated internal VA scans (11.3.1.2)
- Scope validation process and documentation (12.5.2.x)
  - After significant changes (12.5.2.1)
- Execute IRP if card data detected (12.10.7)

PCI Security Standards Council®

Hardships Expected by QSAs for 2025

- Pushing off compliance till 2025
- Keyed hashing not well understood
- Implementing new MFA scope
- Targeted risk analysis process needs strengthening
- Authenticated internal scanning solutions
- Script inventory and testing (6.4.3, 11.6.1)
- Rescoping documentation process after changes
- IRP Testing after detection of PAN, need process to detect…

PCI Security Standards Council®

Needed Characteristics of 11.6.1 Script Solutions

How Do I know if my Solution is Good?

- Data Collection
  - Browser based (DOM level)
  - See entire checkout process
- Analysis
  - Javascripts (static and dynamic)
  - HTTP Headers
  - Indicators of Compromise
    - Accepted source used to classify IOC's
- Reporting
  - All anomalies documented

PCI Security Standards Council

Skimming Forensics - Level 4 Merchants

Why 6.4.3 and 11.6.1 are Needed Requirements

- Data compiled from 2000+ ecommerce forensic investigations
- Most were Level 4 merchants
- Investigations covered both merchant and service provider payment pages
- Results
  - In 100% of cases, skimming scripts were present on **merchant pages**
  - None discovered on service provider pages
- Clearly illustrates need for these requirements even for small merchants

PCI Security Standards Council

Looking Forward

- Future dated requirements, now is the time
- More detailed evidence generally needed for v4
- Experience with v4 changes will get more familiar
- ROC template has been simplified since first release
- Customized approach not used much so far

PCI Security Standards Council

Key Takeaways

- No real big secrets: organize, manage, do your homework
- Have good data flow diagrams
- Know your service providers, collect all needed documentation
- Spend time on your scoping process and document it
- ROC reporting generally taking more time, plan accordingly
- Don’t push off future dated requirements any more

Thank You!

PCI Security Standards Council®


PCi
Security
Standards Council
®