

**Assessment Evidence Collection Techniques  
Workshop  
Notes and Outcomes  
Europe Community Meeting**



# Assessment Evidence Collection Techniques Workshop

## Facilitator:

John Elliott – Jscrambler

## Room Leader

Aimee Cary – Virtual

## Goals:

- **Facilitate Knowledge Sharing:** Encourage participants to share their experiences, success stories, and lessons learned related to evidence collection in payment security assessments. Promote the exchange of practical insights and real-world examples from diverse organizations within the payment card industry.
- **Identify Best Practices:** Collaboratively identify and document best practices for effective evidence collection. Highlight innovative approaches and techniques that have proven successful in various contexts.
- **Discuss Common Challenges:** Explore common challenges and obstacles encountered during the evidence collection process. Foster a supportive environment where participants can openly discuss difficulties and seek advice from peers.
- **Develop Strategies for Improvement:** Brainstorm and discuss strategies to overcome challenges and enhance evidence collection methods. Focus on actionable steps that can be implemented within participants' organizations to drive improvements.
- **Promote Industry-wide Improvement:** Encourage a collective effort towards raising the standards of evidence collection across the payment card industry. Discuss how individual and organizational efforts can contribute to broader industry advancements.
- **Create Actionable Takeaways:** Ensure participants leave the workshop with clear, actionable insights and steps they can implement in their organizations. Summarize key points and best practices discussed during the workshop for future reference.

## Objective:

To share and discuss ideas, experiences, success stories, and lessons learned in assessment evidence collection. Participants will identify best practices, common challenges, and strategies for driving industry-wide improvement.

The workshop aims to enhance the collective knowledge and capabilities of participants, ultimately contributing to more robust and effective evidence collection techniques within the payment card industry.

## Identify Best Practices:

Each group to discuss and identify 3-5 best practices for evidence collection.

## Identify Challenges & Strategies:

- What are the most common challenges in evidence collection?
- What strategies have been effective in overcoming these challenges?
- How can organizations drive industry-wide improvement in evidence collection techniques?

## Identify Proposed Actions

- **Organizations:** Identify action step they will take back to their organization.
- **PCI SSC:** Identify potential actions for PCI SSC (develop guidance, training module, addition to standard or qualification requirements)

## Assessment Evidence Collection Techniques Workshop – Barcelona Outputs

Moderator: John Elliott – Jscrambler

### Identify Best Practices:

- Automation
  - GRC platform, scheduled tasks & scripting
- Support
  - Senior leadership (buy-in)
- Processes
  - Harmonize evidence to be used for more than just PCI assessments
  - Define scope early and create diagrams
- Communication of roles & responsibilities
  - Use of a matrix/checklist
  - Mapping to the standard
  - Give clear deadlines & enforce

### Identify Challenges:

- Defining the correct roles & Responsibilities
- Education/Interpretation of evidence and requirements
- Prioritization & time management
  - Treated as project rather than BAU
- Assessors
  - Variance in opinion
  - Different tools/portals used

### Identify Strategies:

- Automation
  - Use templates
- Timing
  - Preassessment exercises
  - Check in with QSAs as evidence is collected
  - Harmonize evidence collection for other standards
- Planning
  - Agenda
  - Use ISAs
  - Single point of contact
  - Work with the QSA through the year

### Drive Improvement:

- Knowledge sharing
- Assign roles & responsibilities
- Continuous process with tracking
- Include workpapers a full packet with the ROC

### Proposed Actions (Organizations):

- Understand the “why” for PCI DSS Compliance
- Enforce ownership, roles & responsibilities
  - Support from Senior Management
- Have regular check ins with people responsible for evidence
- Continuous process. BAU not project
- Review orientation process
  - Reinforce PCI standard evidence collection in onboarding/orientation
- Allow Assessors to review evidence before the start of assessment

### Proposed Actions (PCI SSC):

- Develop Guidance
  - Automation/AI in evidence collection
  - Best practice for evidence collection
  - Evidence examples in the guidance column of DSS
  - Additional scoping guidance
- Training
  - Better evidence collection training for ISAs/QSAs
    - Available outside of the PCI Portal
  - Scoping specific training
- Tools
  - Automation of RoC, AoC & SAQs
- Online FAQs
  - Make the search features better

### Next Steps:

- NACM & EUCM Workshop outputs to be collated
- Board of Advisors to prioritize potential actions at December meeting
- PCI SSC and Executive Committee to review in November
- PCI SSC will communicate resulting actions with PCI Community as part of 2025 engagement activities