2022 Assessor Session

Moderated by: Elizabeth Terry, Senior Manager, Community Engagement
PCI Security Standards Council

PCI Security Standards Council®

Anti-Trust Reminder

Council meetings involve participation by industry competitors, and it is the intention of the Council to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas and be aware of and not participate in any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Council meetings and in connection with its activities are described in the Council Antitrust Policy, and include the following:

- *Do not discuss prices, discounts, awards, barriers to entry, or other economic terms with other members*
- *Do not divide markets ("you stay out of my territory and I'll stay out of yours")*
- *Do not exclude others from joining or participating*

A copy of the Council's Antitrust Policy can be found here:
https://www.pcisecuritystandards.org/antitrust_policy/

If you become aware of any activity that may be in violation of any of these laws, please bring them promptly to the attention of a PCI SSC representative.

PCI Security Standards Council®

Today’s Discussion Topics

- Introductions
- PCI DSS v4.0 Update
- Certifications Update
- Training Update
- AQM Corner
- Live Q&A

Speaking Today

Elizabeth Terry
Senior Manager, Community Engagement

John Bloomfield
Manager, Data Security Standards

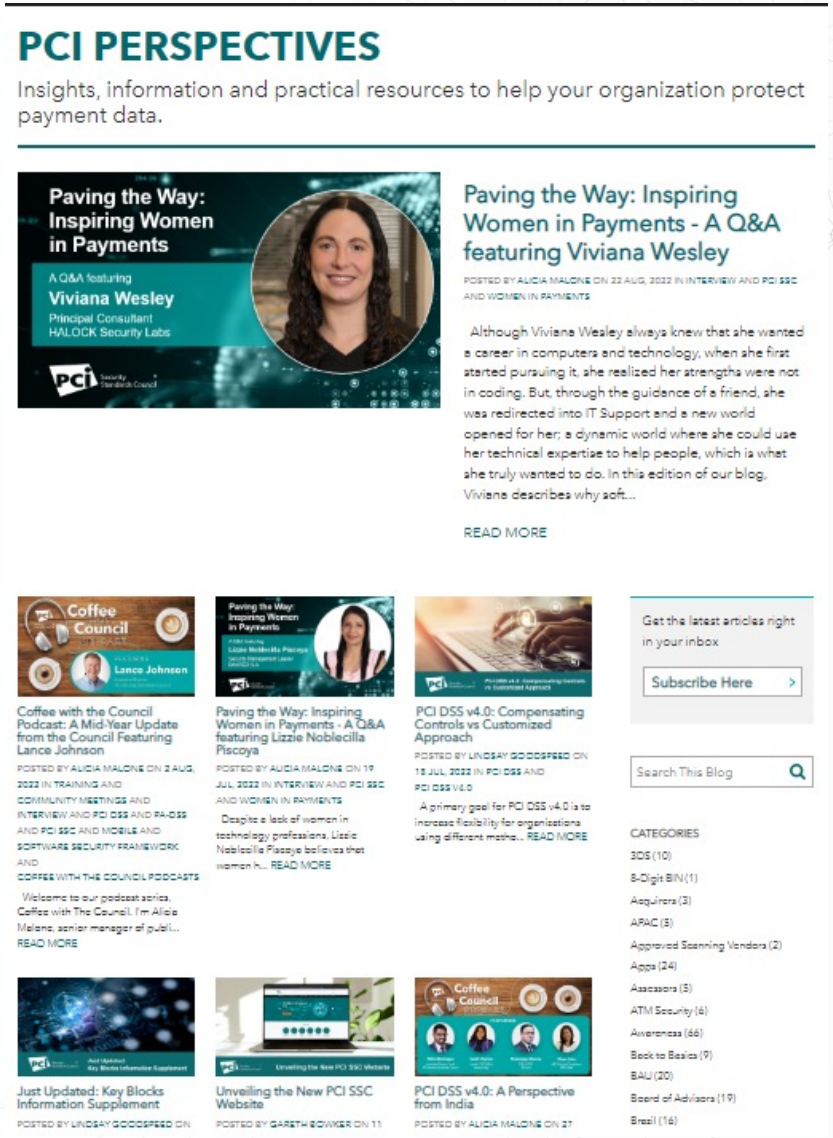
Travis Powell
Director, Training Programs

Matthew O'Connor
Director, AQM

PCI Security Standards Council®

Stay Informed

- ✓Subscribe to the PCI Perspectives Blog
- ✓Subscribe to Press Release RSS Feed
- ✓Follow PCI SSC:
  - Twitter: @PCISSC
  - LinkedIn: LinkedIn.com/company/pcissc



PCI SSC 2022 Community Events and Industry Programs

Event dates and locations are subject to change based on restrictions related to COVID-19

Be In The Know, Become A PO

Events and Speaking Engagements

Call for Speakers - Now Closed

Europe
Community Meeting
18-20 October
Milan, Italy

Registration Now Open

Sign-up for the Vendor Showcase!

Asia-Pacific
Forum
16 November
Online

Registration Now Open

Global Content Library

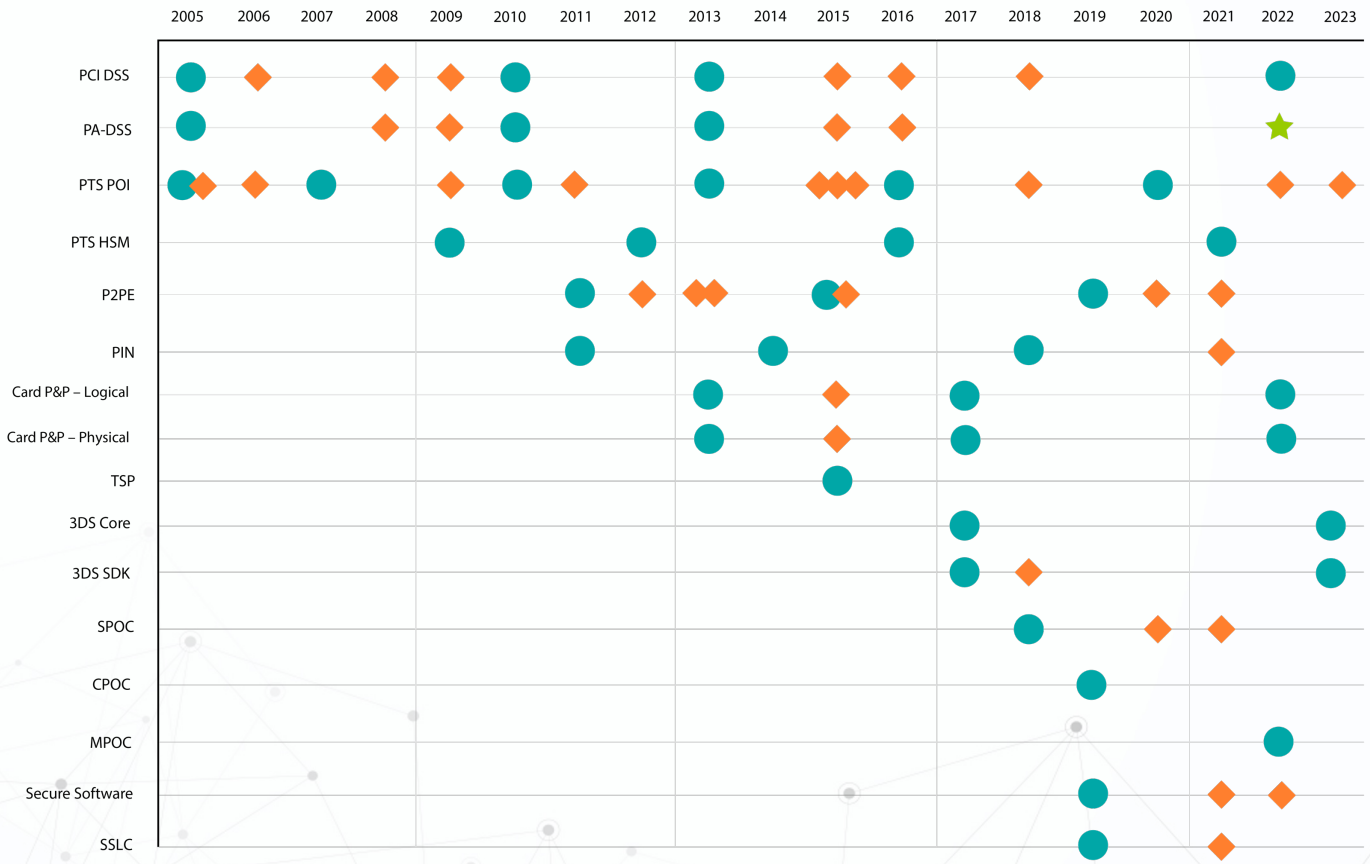
Central location for members of our community to access streamed content.

Standards Revision Cycles

PCI Security Standards Council

Standards Revision History

- Major Revision
- Minor or Other Revision
- Retirement



PCI Security Standards Council

PCI DSS v4.0 Updates

Matthew O’Connor, Director, AQM
John Bloomfield, Manager, Data Security Standards

PCI Security Standards Council®

PCI DSS v4.0 Updates

- Updates/Clarifications for Reporting Options
- Remote Assessments
- Customized Validation

PCI Security Standards Council

But Before We Get Into PCI DSS v4.0...

Let's recalibrate on the role of the assessor and assessor quality

These principles can be validated by four criteria:

- Consistency
- Credibility
- Competency
- Conscientiousness

Principle 1

- Best interest of assessor clients is upheld

Principle 2

- Assessor company adheres to Qualification Requirements

Principle 3

- Assessor employee adheres to Qualification Requirements

Principle 4

- Assessor procedures and reporting are consistent

Principle 5

- Assessor appropriately interprets the PCI Standards as applicable to their client's systems and environment

Principle 6

- Assessor stays current with industry trends and PCI SSC updates

Principle 7

- All opinions rendered are factual, documented and defendable

Principle 8

- Assessor maintains a positive relationship with PCI SSC

PCI Security Standards Council

Security as a Continuous Process

- "In Place With Remediation" or IPWR is NOT intended to be a change in anything but **reporting**
- Feedback from GEAR and BoA led PCI SSC to revisit IPWR; intention is to facilitate documenting areas identified for improvement outside of compliance documentation

Principle 1

- Best interest of assessor clients is upheld

Principle 7

- All opinions rendered are factual, documented and defendable

PCI Security Standards Council

Difference Between Not Applicable and Not Tested

Not Applicable

Assessor documents testing performed to confirm the Not Applicable status

Example: No PAN exists in environment

Requirements specific to PAN are Not Applicable

Not Tested

Assessor does not perform any testing and does not know whether the requirement applies or is In Place

Example: Only requirements for Prioritized Approach Milestones 1-4 are included in the assessment

All other requirements are Not Tested

PCI Security Standards Council®

Uses of Not Tested: The Good and The Bad…

Organization wants to include only certain requirements

Acquirer asks merchant to include only Prioritized Approach Milestones 1-4

An organization includes only requirements for a newly implemented technology

A service provider includes only requirements for a data center hosting service

Organization has requirements that are not in place

Organization wants “Not Tested” results while it implements corrective actions

NO!

PCI Security Standards Council

New Reporting Options

Full Assessment

Partial Assessment

PCI Security Standards Council

PCI DSS v4.0 Updates – Remote Assessment

PCI Security Standards Council®

Remote Assessment/Testing Activity

1.3 Remote Assessment Activities

1.3.1 *Overview of Remote Testing Activity*

To what extent were remote testing methods used for this assessment?	☐ All testing was performed onsite ☐ A combination of onsite and remote testing methods was used ☐ All testing was performed remotely
If remote testing was used for any part of the assessment, briefly describe why onsite testing was not feasible or practical.	<Enter Response Here>

1.3.2 *Summary of Testing Performed Remotely*

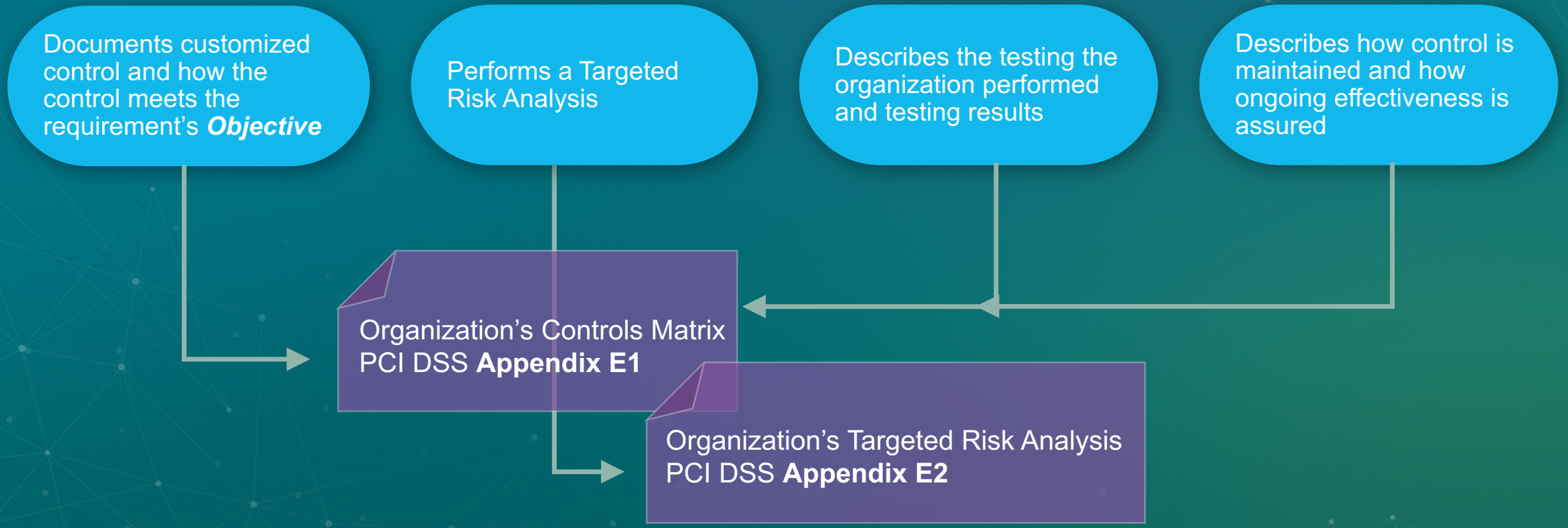
Type of Testing Activity	Were remote testing methods used to perform this testing activity during the assessment?		For all testing activities performed using remote methods:	
			Describe the methods used to perform the remote testing.	Describe any alternative and any additional testing activities that were performed to confirm assurance in the test result.
Examine documentation	☐ Yes	☐ No	<Enter Response Here>	<Enter Response Here>
Interview personnel	☐ Yes	☐ No	<Enter Response Here>	<Enter Response Here>
Examine/observe live data	☐ Yes	☐ No	<Enter Response Here>	<Enter Response Here>
Observe process being performed	☐ Yes	☐ No	<Enter Response Here>	<Enter Response Here>
Observe physical environment	☐ Yes	☐ No	<Enter Response Here>	<Enter Response Here>
Interactive testing	☐ Yes	☐ No	<Enter Response Here>	<Enter Response Here>

1.3.3 *Assessor Assurance in Assessment Result*

If remote testing methods were used for the assessment, identify whether the assessor was able to:		
Complete a thorough assessment using appropriate remote testing activities as described in QSA Program Guide?	☐ Yes	☐ No
Achieve a high degree of confidence that the assessment resulted in a complete evaluation of the entity's in-scope environment for all applicable requirements?	☐ Yes	☐ No
Achieve a high degree of confidence in the accuracy and integrity of the evidence observed and reviewed?	☐ Yes	☐ No
Achieve a level of confidence in the remote testing results that is commensurate to the level of confidence that would have been achieved via onsite testing?	☐ Yes	☐ No
Achieve a high degree of assurance in the overall assessment result?	☐ Yes	☐ No

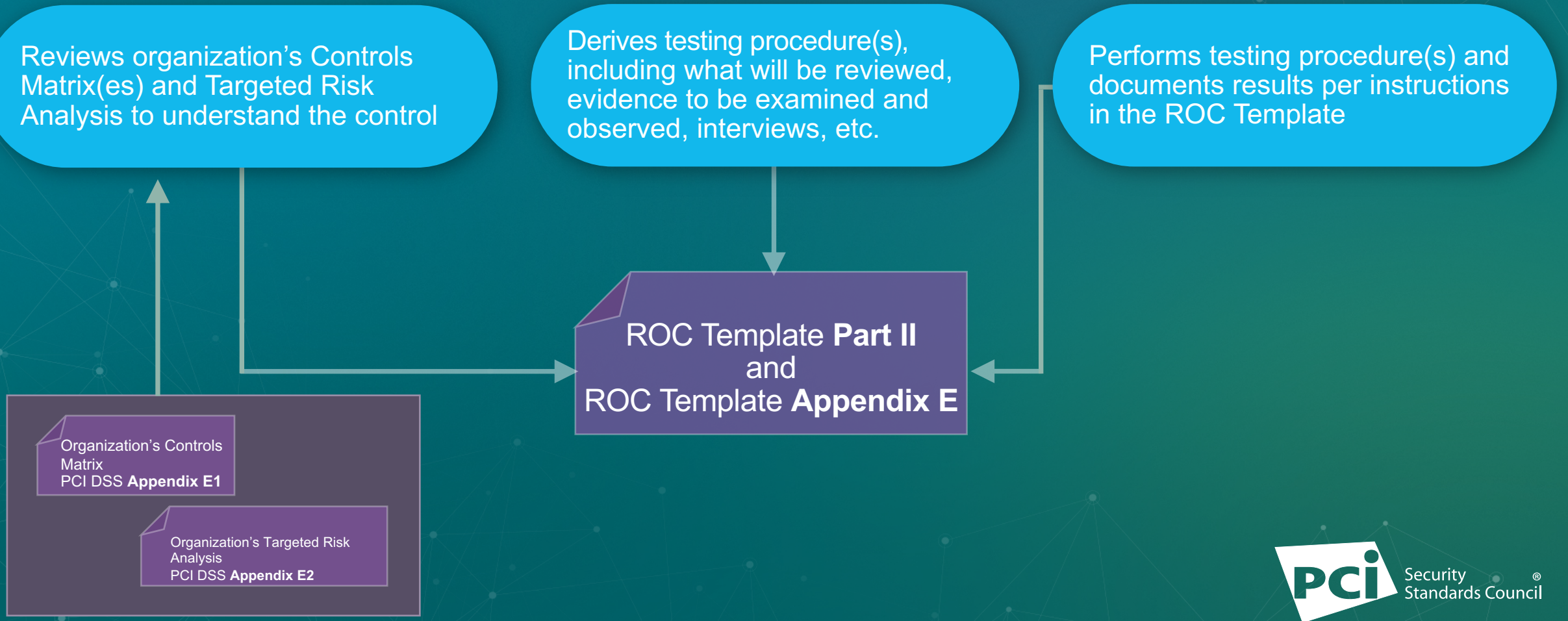
PCI Security Standards Council®

Customized Validation: The Organization's Role



PCI Security Standards Council

Customized Validation: The Assessor's Role



PCI Security Standards Council®

Program Updates

Travis Powell, Director, Training Programs

PCI Security Standards Council®

Changes to QSA Program Docs

Changes to QSA Program Guide and QSA Qualification Requirements

No new requirements planned for QSA Program:

Removed the future dating for the requirement QA reviewers within QSA Companies must have a PCI certification

Note: *This requirement took effect on March 31, 2022*

Added a best practice to the Program Guide for QSA Companies to document their sampling methodology.

Section added to Program Guide with guidance on conducting Remote Assessments..

Appendix added to Program Guide to provide guidance on Evidence Retention including with respect to Customized Validation.

..

PCI Security Standards Council

PA-DSS Program Closure

Important Dates and Activities

April 2022

After 29 April 2022

Requalification and training fees will be pro-rated for PA-QSAs that are *not* also Secure Software Assessors

October 2022

28 October 2022 – PA-DSS Program closes

- After this date, the list of PA-QSAs will be removed from the PCI SSC Website
- Change submissions to listed PA-DSS applications must be complete and have a paid invoice by this date
- Accepted change submissions will have until 31 March 2023 to complete
- All applications currently listed as “Acceptable for New Deployments” will be moved to the “Acceptable only for Pre-Existing Deployments” list
- PA-QSA Companies that would like to continue assessing software applications after this date, including PA-QSA(P2PE)s, will need to qualify under the Software Security Framework as a Secure Software Company
- Portal access to historical PA-DSS records is not guaranteed after 28 October 2022

March 2023

31 March 2023

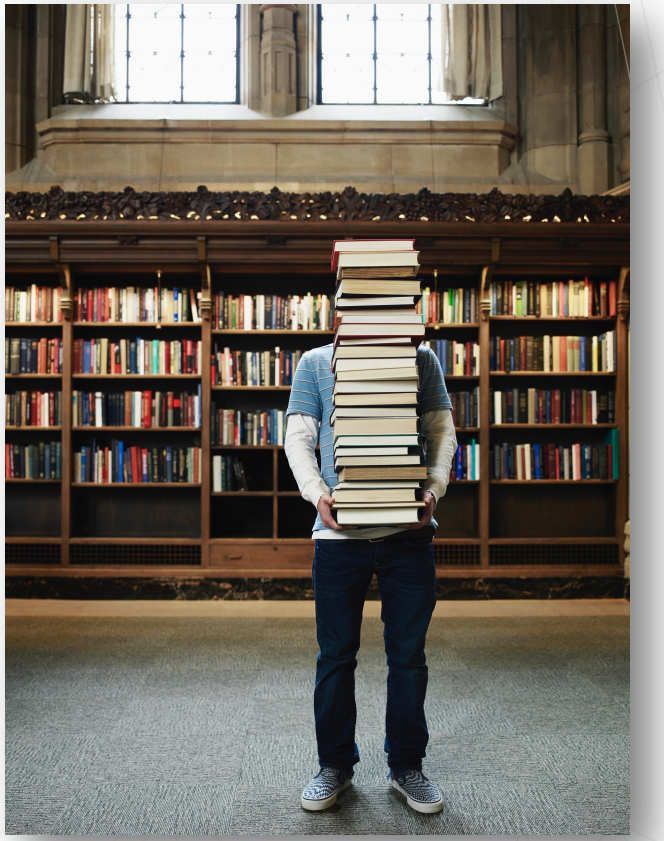
Any in-flight PA-DSS change submissions must be completed. Those that do not complete by 8pm EST will be closed.

PCI Security Standards Council

Associate QSA Program Update

Launched in 2017, AQSA has grown to 40 participating QSA Companies with over 100 Qualified AQSAs

- Purpose of the program was to provide a development path for security professionals to gain experience to be QSAs
- Requirements are either a university degree in IT related studies or two years IT related field work
- Same training and exam as QSAs
- Will be listed on the PCI website
- Can assist with Assessments under the guidance of their mentor



PCI Security Standards Council

P2PE Program Changes

Anticipated Changes to P2PE Program

- Allow QPA prerequisite to becoming P2PE Assessor
- Remove requirement to have completed 2 Secure Software Assessments for new P2PE Application Assessors
- Change P2PE Assessor designations to:

QSA (P2PE)	→	P2PE Assessor
PA-QSA (P2PE)	→	P2PE Application Assessor

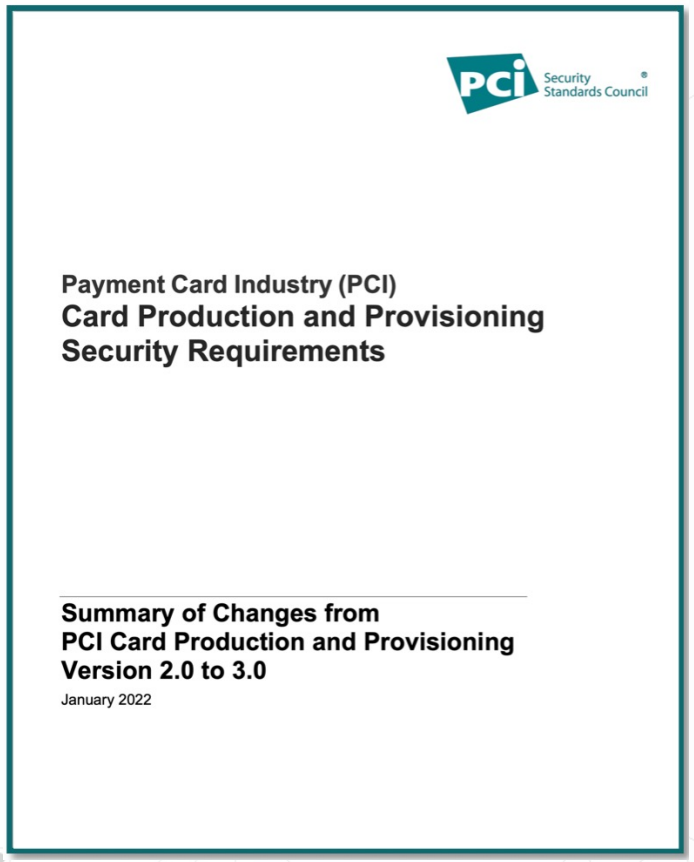
- Q4 2022 targeted for changes

PCI Security Standards Council

Card Production Security Assessor

Version 3.0 released in January

- CPSA Program Guide and Qualification Requirements updated in March
- Transitional training for v3.0 now available!
- Once trained, Assessors can submit reports using v3.0 1 October 2022
- CPSAs must be using v3.0 no later than 1 January 2023



PCI Security Standards Council

Software Security Framework

Module C – Web Software

- Publication expected Q4 2022
- Training for Module C expected no later than Q1 2023
- Once available, Assessors will have to complete training and exam as part of QRs

PCI Security Standards Council

Training Updates

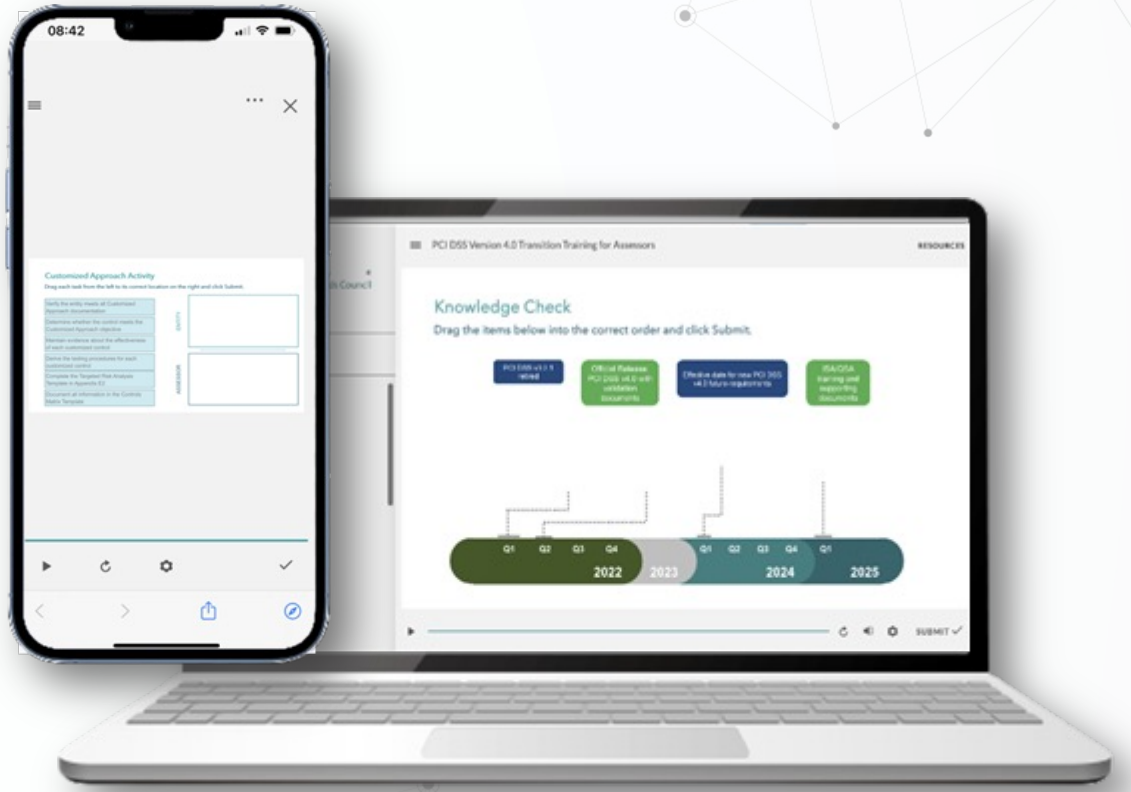
Travis Powell
Director, Training Programs

PCI Security Standards Council®

New CBT Platform

Benefits of the New Platform

- Starting in 2022 Training switched to **a new computer-based training (CBT) platform**
- The new platform allows for the creation of **highly interactive multimedia training courses**
- The addition of **engaging videos, case-studies, and scenarios** to aid the learning experience
- Responsive design allows courses to be taken on **a variety of device types**

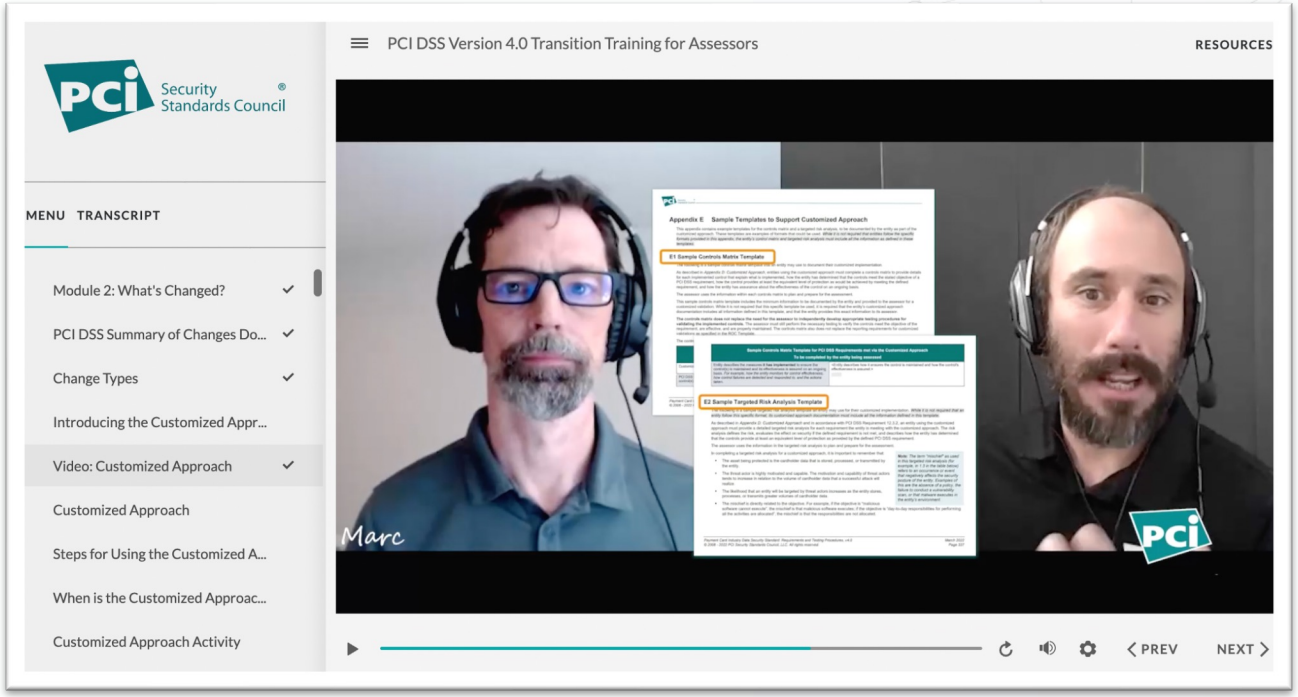


PCI Security Standards Council

New CBT Platform

More Engaging and Interactive

First course developed with the new platform was **PCI DSS Version 4.0 Transition Training for Assessors.**



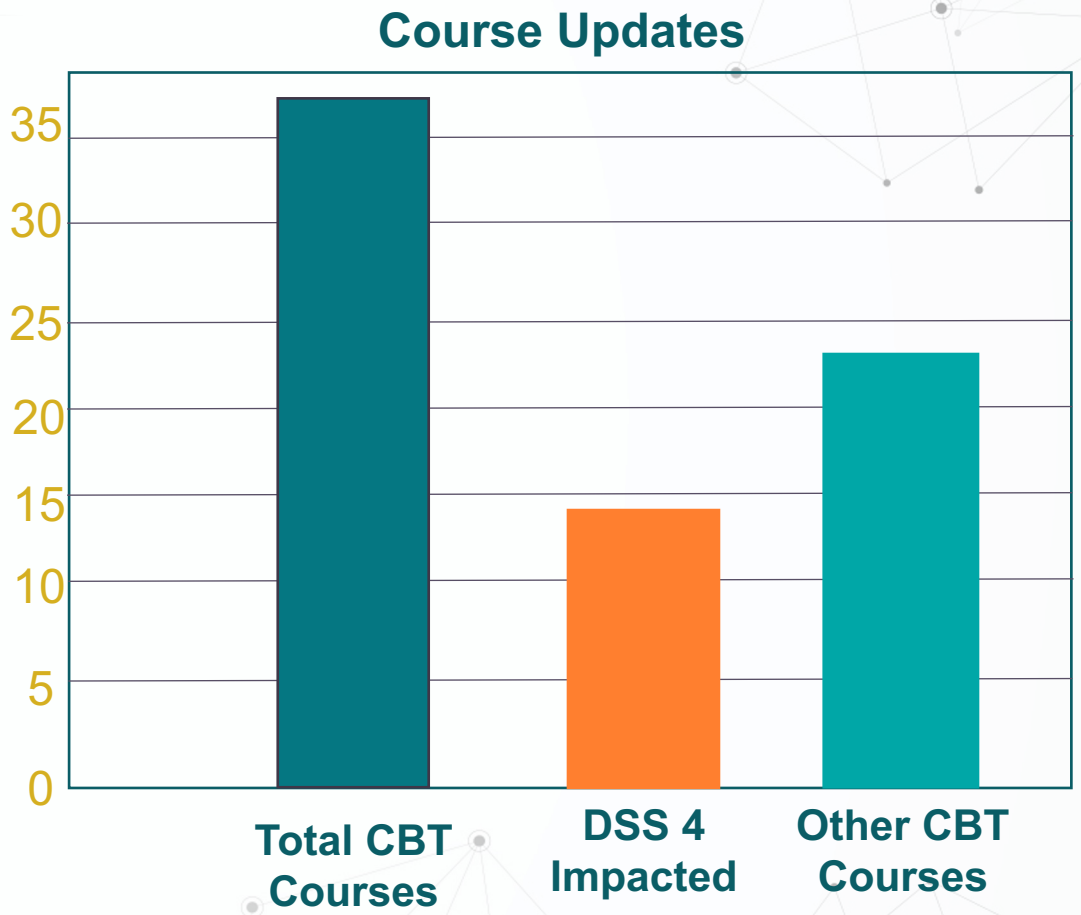
PCI DSS Version 4.0 Transition Training for Assessors Course

PCI Security Standards Council

New CBT Platform

PCI DSS v4.0 CBT Update Overview

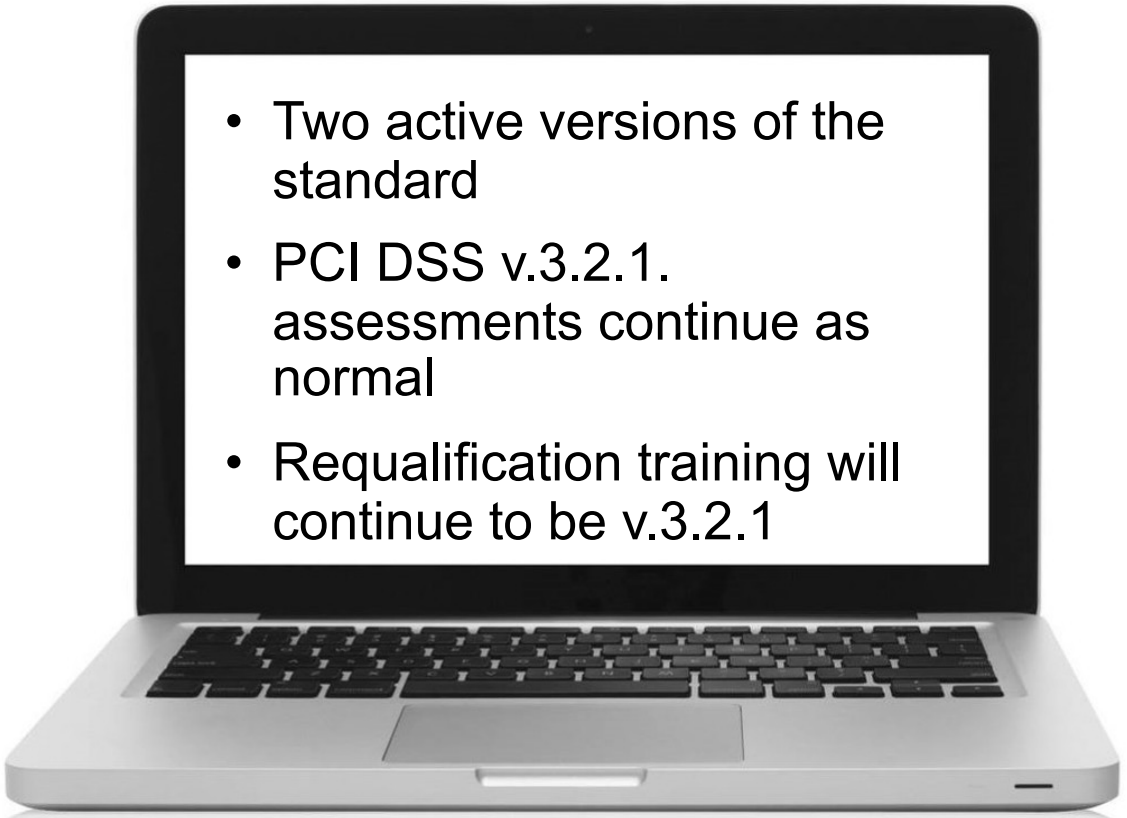
- Efforts to modularize training to reduce repeat content
- Updates to improve consistency across courses
- Target to have all courses updated and / or migrated by end of 2023 early 2024
- Priorities include ASV, PCIP, PCI Forensic Investigator, and QSA/ISA as priority for DSS v4.0 updates



PCI Security Standards Council

PCI DSS v4.0 Transitional Training

What Happens Now That PCI DSS v4.0 is Released?



PCI Security Standards Council®

PCI DSS v4.0 Transitional Training

When Can I Perform PCI DSS v4.0 Assessments?

- Complete the PCI DSS v4.0 CBT transitional course
- Training covers changes to the standard, ROCs, AOCs, SAQs and more!
- Short non-proctored exam will be required for Assessors prior to performing PCI DSS v4.0 Assessments
- QSAs, AQSAs, and ISAs who complete the v4.0 training and successfully pass the exam will have their website listings updated

PCI Security Standards Council

PCI DSS v4.0 Transitional Training

What about PCIPs or Everyone Else?

- PCI DSS v4.0 general training is available now for PCIPs!
- Training is informational, no exam will be required until included as part of regular requalification process
- General training for everyone else is on track for Q1 2023

PCI Security Standards Council

Knowledge Training

What is Knowledge Training?

- Formerly known as Informational Training
- Learners will complete the same training and exam as existing Assessors
- Individuals are not validated to perform Assessments, purely knowledge training
- Badges will only show completion against the specific training and version of the Standards that was trained
- Audience would typically be non-Assessors, Merchants, Service Providers, Solution Providers, Acquirers, and Vendors

PCI Security Standards Council

Knowledge Training

Assessor Company QA Requirements

- Certain programs have requirements for QA reviewer training for major releases
- Updates will be made as required to additional programs
- **As of March 1, 2023, all quality-assurance reviews must be conducted by personnel that are either CPSA Employees or other personnel that have completed CPSA Informational Training. CPSA Information Training must be completed initially and after every major update in the Card Production Security Requirements prior to reviewing submissions under the new release.*

**PCI Qualification Requirements for Card Production Security Assessors, v1.1*

PCI Security Standards Council

Knowledge Training Programs

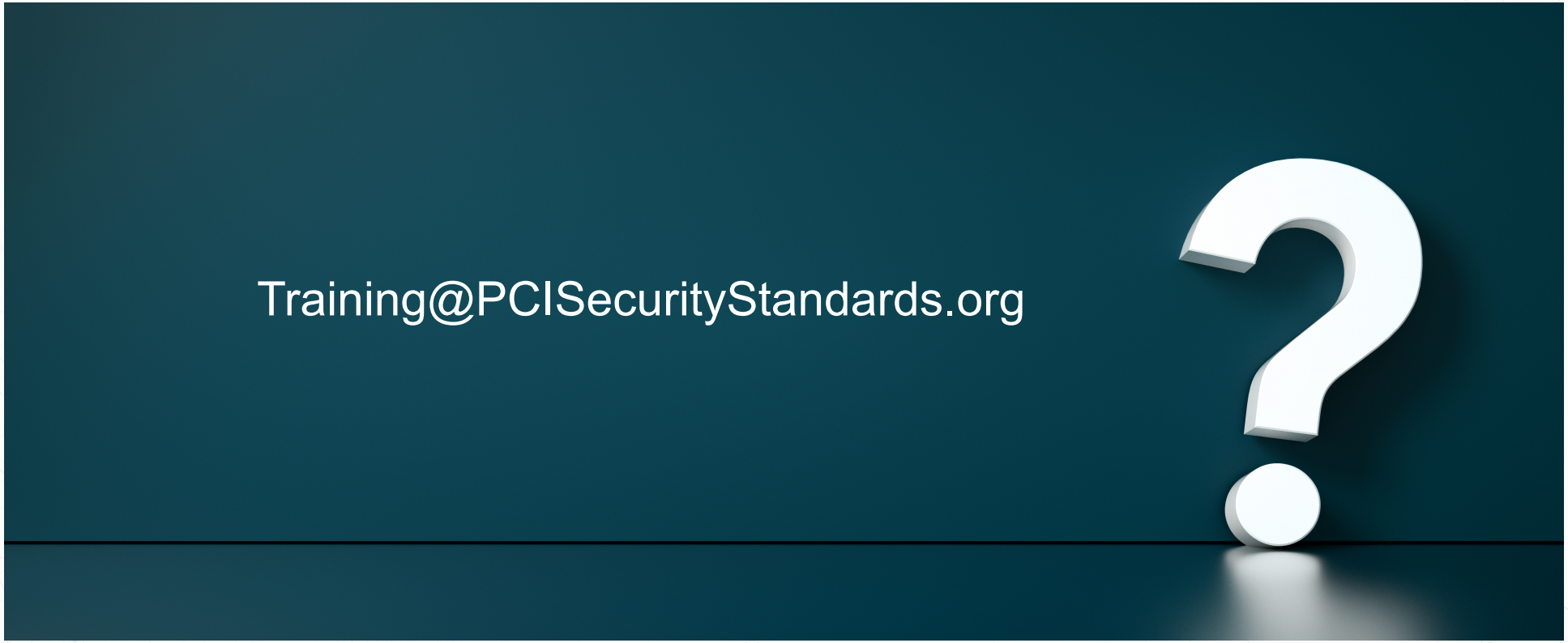
Launched – 5 October 2022

- Card Productions Security Assessor Logical
- Card Production Security Assessor Physical
- Point to Point Encryption
- Qualified PIN Assessor
- Secure SLC Assessor
- Secure Software Assessor
- 3DS Core (3-Domain Secure)

PCI Security Standards Council

Questions

Training Questions?



PCI Security Standards Council

AQM Corner

Matthew O’Connor
Director, AQM

PCI Security Standards Council®

AQM - Agenda

- Meet the Team
- QSA Questionnaire
- AQM Challenges
- Coming Soon

Quality is not an act; it is a habit ~ Aristotle

PCI Security Standards Council

AQM – Meet the Team

Andrew Hardie

Bonnie Kalb

Jeanette O'Grady

Matt Ball

Barbara Cunningham

Carl Wakelin

Kristine Mountfort

Randy Rieth

Excellent firms don't believe in excellence - only in constant improvement and constant change ~ Tom Peters

PCI Security Standards Council®

QSA Questionnaire

Benefits to All Parties

Quality improvement for the QSAC, leading to indirect benefits to assessed entities, acquirer(s) and wider cardholder community

Understand how the QSA Qualifications are implemented

PCI Security Standards Council

QSA Questionnaire

Key Findings (Positive Things)

Improvement and change between consecutive years, where issues from the previous year have been addressed

Well produced documentation implementing the QSA requirements

Compensating Control Worksheets - improvements

PCI Security Standards Council

QSA Questionnaire

Key Findings (Issues)

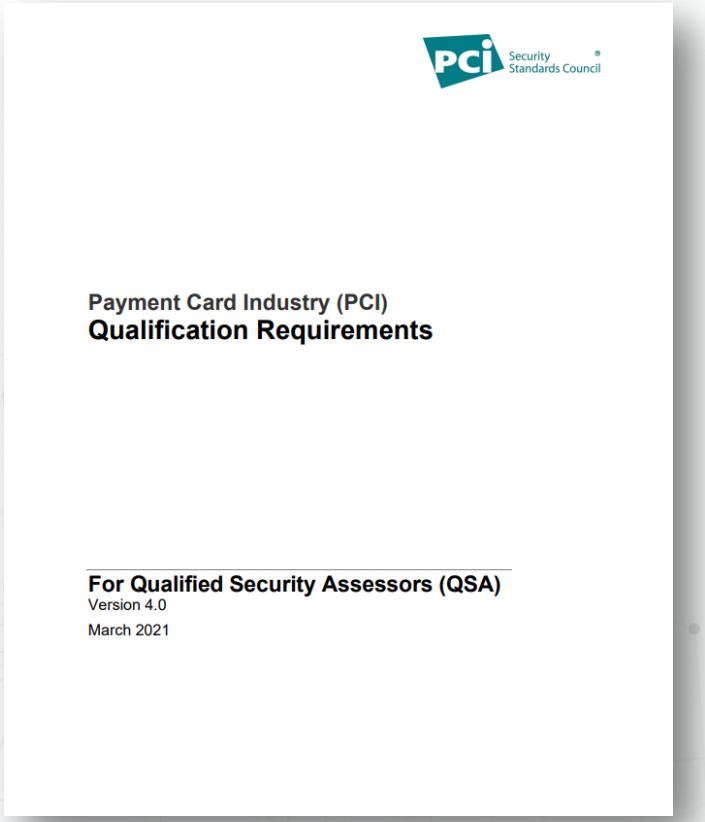
QSA Qualification Requirements

Assessment Specific

PCI Security Standards Council

QSA Questionnaire

Key Findings – QSA Qualification Requirements



- Independence clauses
- Evidence Retention
- Incident Response
- Documentation (general)
- Compensating Controls

PCI Security Standards Council

QSA Questionnaire

Key Findings – Assessment Specific

Lack of apparent verification that CHD does not exist beyond CDE

Lack of detail about the methods and rationale used to determine scope

Redacting the QSA name

PCI Security Standards Council

QSA Questionnaire Key Findings

Across all expected documentation (primarily the QA manual) we tend to note:

- Lack of document ownership
- Suspect version control and review histories
- Lack of intent for review
- Lack of clause for assessors to review the PCI SSC website.

QSA Questionnaire Key Findings

ROCS

PCI Security Standards Council

Software Security

- Assessment Scope
- Table 3.7 Software Testing Performed
- ROV Date of Report
- Vendor Evidence

If you can't explain it simply, you don't understand it well enough ~ Albert Einstein

PCI Security Standards Council

Software Security

Not sure? Ask.

Send your question to the Program Manager.

software@pcisecuritystandards.org

Please do not just “submit and hope”.

PCI Security Standards Council

AQM – Recent Challenges

At a high level AQM covers:


PA-DSS


Secure Software


Software Lifecycle


Point to Point Encryption


3DS SDK


QSA Questionnaires


PIN Audits


CPSA Audits


PCI DSS Audits


AQSA

You seldom improve quality by cutting costs, but you can often cut costs by improving quality ~ Karl Albrecht

PCI Security Standards Council

AQM – Recent Challenges

- PA-DSS
- PCI DSS v4.0
- Secure Software
- QSA Questionnaire
- Resourcing

PCI Security Standards Council

AQM – Recent Challenges

Remember, don’t wait until the end of October to get your PA-DSS submissions in!

PCI Security Standards Council

AQM – Coming Soon

QSA Questionnaire – analysis of collated data

If you can't explain it simply, you don't understand it well enough ~ Albert Einstein

PCI Security Standards Council

AQM – Coming Soon

QSA Questionnaire – analysis of collated data

ISO approach to AQM review findings:

FINDINGS AND OBSERVATIONS		
Requirement(s)	**AQM Comments**	**Type**
2A-1.2	The assessor did a great job here documenting how the assessor used "GoToMeeting" to interview the vendor. Thank you!	MR001 (AQMC001)
2A-2.1.b	Great job of documentation!	MR002 (AQMC002)
2B-1.8.c	Please identify the P2PE Assessor who confirms the versioning methodology is in accordance wit the P2PE Program Guide requirements.	MIN001
2B-1.11.a; 2B-1.11.b	The purpose of this requirement is to ensure that if internal version numbers are used by the vendor, that those internal version numbers are mapped to the published version numbers. This is different than ensuring there is no mapping of version numbers. Please clarify whether there are internal versioning numbers used by the vendor that are not the same as those published externally.	MIN002

PCI Security Standards Council

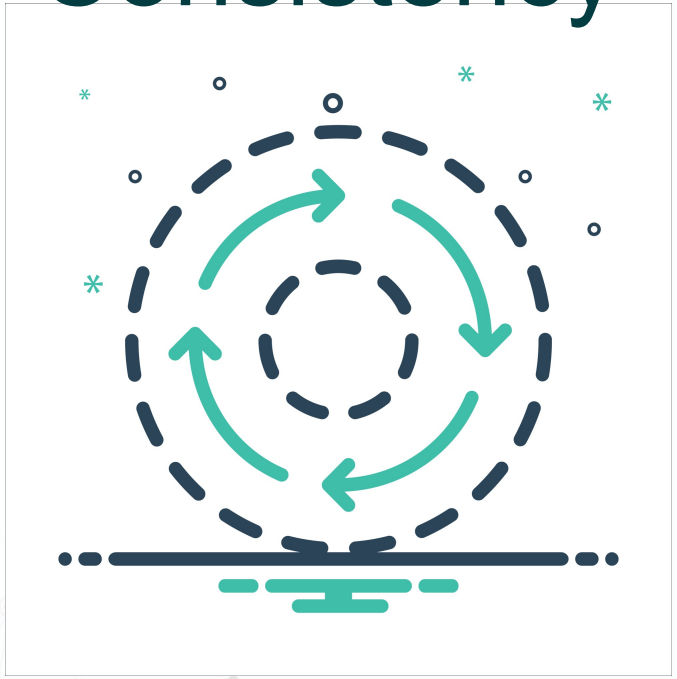
AQM – Coming Soon

Findings Table	SECTION or REQUIREMENT	AQM Comment	AQM Reviewer	Submission Type	Review Date	AQM Ref	Review Rating
EXECUTIVE SUMMARY / SUMMARY OVERVIEW	3.3 Key-management processesFigure 5 - LMK/MFK Key Management	Information Only: The narrative includes "…KCVs are written are written down or…".	Matthew O'Connor	P2PE Component	19-Mar-21	C185	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	32-7.b	The response is a positive statement confirming that the requirement is in place. The assessor should describe how the observed configurations verified that time and date stamps are synchronised.	Matthew O'Connor	P2PE Component	19-Mar-21	C185	NEEDS IMPROVEMENT
OVERALL FINDINGS	Inconsistencies	Please see findings listed below.	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
EXECUTIVE SUMMARY / SUMMARY OVERVIEW	2.4	AQM would expect the test HSM to be listed here if its intended purpose is to provide a backup for the production HSM, see assessor response in 19-4.d.	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	18.3	Please provide additional clarification as to why this would not be applicable as the KIF is a service provider and is storing keys within the HSM.	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	19.2	Did the assessor intend for the response to say, "Public/Private keys are not used"?	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	19.3	Did the assessor intend for the response to say, "Public/Private keys are not used"?	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	23-1.a	AQM would expect the assessor to list the procedures and interviewed personnel that were used to determine if keys are generated using a reversible key-calculation method.	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	23-2.a	AQM would expect the assessor to list the interviewed personnel that were used to determine if keys variants are utilized	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	23-2.b	AQM would expect the assessor to list the documentation that was used to determine if keys variants are utilized	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	23-2.c	AQM would expect the assessor to detail the review process of the listed documents, to determine variants are not used external to the logical configuration that houses the MFK.	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	26-1.c	Logs are to be archived two years after key destruction. The assessor should attest that logs were reviewed back to generation or initial receipt for all current keys and keys that have been destroyed in the last two years.	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
FINDINGS AND OBSERVATIONS	29-2.b	Does the sampling of one device provide reasonable assurance of chain of custody?	Randy Rieth	P2PE Component	11-Mar-21	C190	NEEDS IMPROVEMENT
OVERALL FINDINGS	Inconsistencies	Please see below.Please note that any findings prefixed with "Information Only" may be left as is (AQM do not require changes for these).	Matt O'Connor	P2PE Component	31-Jan-20	135	NEEDS IMPROVEMENT
EXECUTIVE SUMMARY / SUMMARY OVERVIEW	3.1 Scoping Details	Did the assessor confirm the methods or processes used to identify all elements in scope? The current wording infers that HIT defined their own scope.	Matt O'Connor	P2PE Component	31-Jan-20	135	NEEDS IMPROVEMENT

PCI Security Standards Council®

…And Finally

Consistency



The only real mistake is the one from which we learn nothing ~ Henry Ford

PCI Security Standards Council®

2022 Assessor Session Q & A

PCI Security Standards Council®

Thank You!

PCI Security Standards Council®