Payment Card Industry (PCI)

Card Production Security Assessors (CPSA) Logical and Physical

Program Guide

Version 1.1

March 2022

Document Changes

Date	Version	Description
April 2019	1.0	This is the first release of the *PCI CPSA Program Guide.*
March 2022	1.1	▪ Added requirement for CPSAs to have appropriate skills for assessments ▪ Added requirement that CPSAs must be trained on the version of Card Production Security Requirements they are using ▪ Added guidance regarding remote assessments ▪ Added Appendix B to provide additional QA guidance ▪ Performed minor clarifications in language throughout

Contents

1 Introduction

This Program Guide provides information to CPSA Companies and CPSA Employees pertinent to their roles in connection with the PCI SSC Card Production Security Assessor (CPSA) program. Information regarding the qualification of CPSA Companies and their employees can be found in the *PCI CPSA Qualification Requirements* on the Website. Companies wishing to apply for CPSA Company status should first consult the *CPSA Qualification Requirements*. Capitalized terms, used but not otherwise defined herein, have the meanings set forth in Section 4 below, or in the *CPSA Qualification Requirements*, as applicable.

2 Related Publications

This document should be reviewed in conjunction with other relevant PCI SSC publications, including but not limited to current publicly available versions of the following, each available on the Website.

Document name	Description
Payment Card Industry (PCI) Card Production and Provisioning Logical Security Requirements (Card Production Logical Security Requirements)	Lists the specific technical and operational security requirements used by assessors to validate Logical PCI Card Production and Provisioning compliance.
Payment Card Industry (PCI) Card Production and Provisioning Physical Security Requirements (Card Production Physical Security Requirements)	Lists the specific technical and operational security requirements used by assessors to validate Physical PCI Card Production and Provisioning compliance.
PCI Card Production and Provisioning Attestation of Compliance (Card Production AOC)	A form for Card Production Entities and CPSA Companies to attest to the results of a PCI Card Production Assessment (Logical and/or Physical), as documented in the CPSA Report on Compliance.
PCI SSC Programs Fee Schedule	Lists the current fees for specific qualifications, tests, retests, training, and other services.
PCI SSC Remote Assessment Guidelines and Procedures	Detailed guidelines and procedures for performing PCI SSC program assessments remotely.
PCI Card Production Security Assessor (CPSA) Qualification Requirements	Defines the set of requirements that must be met by CPSA Companies and CPSA Employees in order to perform their respective roles in connection with PCI Card Production Assessments.
PCI Card Production and Provisioning Template for Report on Compliance (Card Production ROC)	The mandatory template for use in completing a Card Production Report on Compliance. Provides detail on how to document the findings of a PCI Card Production Assessment. There is one template for use with the PCI Card Production Logical Security Requirements and one template for use with the PCI Card Production Physical Security Requirements.

Document name	Description
CPSA Feedback Form	Gives the Card Production Entity an opportunity to offer feedback regarding the CPSA and the assessment process. https://www.pcisecuritystandards.org/assessors_and_solutions/Card Production Security_Assessors_feedback

3 Updates to Documents and Security Requirements

This Program Guide is expected to change as necessary to align with updates to the PCI Card Production Security Requirements and other PCI SSC Standards. Additionally, PCI SSC provides interim updates to the PCI community through a variety of means, including required CPSA Employee training, e-mail bulletins and newsletters, frequently asked questions, and other communication methods.

PCI SSC reserves the right to change, amend, or withdraw security requirements, qualification requirements, training, and/or other requirements at any time.

4 Terminology

For purposes of this Program Guide, capitalized terms not otherwise defined are defined as set forth below or in the current version of the corresponding PCI SSC document referenced below. All such documents are available on the Website:

Term	Definition / Source / Document Reference
Assessor Portal (Portal)	Web-based application made available to PCI qualified assessors to access PCI program documentation and forms.
CPSA Agreement	The then-current version of (or successor document to) the *CPSA Company Agreement* attached as Appendix A to the *PCI CPSA Qualification Requirements*.
CPSA Company	A company that has been qualified, and continues to be qualified, by PCI SSC to perform PCI Card Production Assessments.
CPSA Employee	An employee of a CPSA Company who has been qualified, and continues to be qualified, by PCI SSC to perform PCI Card Production Assessments (Logical and/or Physical).
CPSA List	The then-current list of CPSA Companies published by PCI SSC on the Website.
CPSA Program Manager (PM)	The PCI SSC staff member charged with overseeing the CPSA Program activities and providing support and answering inquires on the CPSA Program. Contact pcicard@pcisecuritystandards.org.
CPSA Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Card Production Security Assessors (CPSA)*, as from time to time amended and made available on the Website.

Term	Definition / Source / Document Reference
CPSA Requirements	With respect to a given CPSA Company or CPSA Employee, the applicable requirements and obligations thereof pursuant to the CPSA Qualification Requirements, the CPSA Agreement, each addendum, supplement, or other agreement or attestation entered into between such CPSA Company or CPSA Employee and PCI SSC, and any and all other policies, procedures, requirements, validation or qualification requirements, or obligations imposed, mandated, provided for, or otherwise established by PCI SSC from time to time in connection with any PCI SSC Program in which such CPSA Company or CPSA Employee (as applicable) is then a participant, including but not limited to all policies, procedures, requirements, standards, obligations of all applicable PCI SSC training programs, quality-assurance programs, remediation programs, program guides, and other related PCI SSC Program materials, including without limitation those relating to probation, fines, penalties, oversight, remediation, suspension, and/or revocation.
Card Production Entity	A company that performs card production and provisioning activities such as card manufacturing, chip imbedding, data preparation, pre-personalization, card embossing, integrated chip (IC) and magnetic-stripe personalization, PIN generation, PIN mailers, card carriers, and distribution.
Card Production Security Requirements	The set of security requirements as documented in the then-current *Payment Card Industry (PCI) Card Production and Provisioning Logical Security Requirements* and *Payment Card Industry (PCI) Card Production and Provisioning Physical Security Requirements.*
PCI Card Production Assessment	An assessment of a Card Production Entity to determine its compliance with the PCI Card Production Security Requirements as part of the PCI CPSA Program. The reviews are conducted by CPSA Companies and their employees.
PCI SSC	PCI Security Standards Council is the standards body that maintains the PCI SSC Standards and supporting programs and documentation.
Remediation	The PCI Assessor Quality Management (AQM) process for addressing identified quality issues at CPSA Companies.
Website	The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.

5 Roles and Responsibilities

There are several stakeholders in the CPSA Program. The following sections define their respective roles and responsibilities.

5.1 Participating Payment Brands

The Participating Payment Brands independently develop and enforce the various aspects of their respective programs related to compliance with PCI Card Production Security Requirements, including, but not limited to:

- Managing compliance enforcement programs—e.g., policies, procedures, mandates, and due dates
- Determining the compliance status of the assessed entity
- Establishing penalties and fees
- Determining the card production entities that need to comply and be validated
- Endorsing qualification criteria
- Responding to cardholder data compromises

Note: *Contact details for the Participating Payment Brands can be found in Card Production and Provisioning Technical FAQ on the Website.*

5.2 PCI Security Standards Council

PCI SSC is the standards body that maintains the PCI SSC Standards and supporting programs and documentation. In relation to the CPSA Program, PCI SSC:

- Maintains the PCI Card Production Security Requirements and related validation requirements, programs, and supporting documentation.
- Provides training for and qualifies CPSA Companies and CPSA Employees to perform PCI Card Production Assessments.
- Lists CPSA Companies and CPSA Employees on the Website.
- Maintains an Assessor Quality Management (AQM) program. See Section 8, "Assessor Quality Management," for additional information.
- Does not approve Card Production ROCs from a technical perspective.

Note*: PCI SSC does not assess entities for PCI Card Production compliance.*

5.3 CPSA Companies and CPSA Employees

A CPSA Company is an organization that has been qualified as a CPSA Company by PCI SSC, has been added to the CPSA List and, through its CPSA Employees, is thereby authorized to validate adherence to the PCI Card Production Security Requirements in accordance with applicable CPSA Program requirements.

The Primary Contact at the CPSA Company is the liaison between PCI SSC and the CPSA Company.

Responsibilities of CPSA Companies and their CPSA Employees in connection with the CPSA Program include, but are not limited to, the following:

- Adhering to the CPSA Requirements and this Program Guide
- Successfully completing all applicable CPSA Program training requirements
- Maintaining knowledge of and ensuring adherence to current and relevant PCI Card Production guidance located in the Document Library section of the Website
- Performing PCI Card Production Assessments in accordance with the PCI Card Production Security Requirements, including but not limited to:
  - Selecting employees, systems, and system components to accurately represent the assessed environment when sampling is employed
  - Effectively using the *Card Production Reporting Template* to produce Reports on Compliance (Card Production ROC)
  - Completing the *PCI Card Production Attestation of Compliance* (CPSA AOC)
  - Validating and attesting as to an entity's compliance with the PCI Card Production Security Requirements
  - Maintaining documents, workpapers, and interview notes that were collected during the PCI Card Production Assessment and used to validate the findings
  - Applying and maintaining independent judgement in all PCI Card Production Security Assessment decisions
  - Conducting follow-up assessments, as needed
  - Assessing the level of compliance the entity has achieved with respect to PCI Card Production Security Requirements (Logical and/or Physical)
  - Submission of reporting as described in the PCI Card Production Assessment Audit Process below
- Refer to Appendix B, "Appendix B: Eight Guiding Principles Validated by Four Criteria (Four Cs)," to understand PCI SSC's baseline for assessor quality.

Note: *While the Primary Contact's role includes helping facilitate and coordinate with PCI SSC regarding administrative or technical questions, Primary Contacts as well as CPSA Companies and CPSA Employees are strongly encouraged to check the FAQs published on the Website prior to contacting PCI SSC with questions.*

5.4 Card Production Entity

A Card Production Entity performs card production and provisioning activities such as data preparation, manufacturing, pre-personalization, card embossing, chip embedding, card personalization, chip personalization, PIN generation, PIN mailers, card carriers, and distribution.

The role of PCI Card Production Entities in connection with the CPSA Program includes the following:

- Understanding compliance and validation requirements of the current PCI Card Production Security Requirements.
- Maintaining compliance with the PCI Card Production Security Requirements at all times.
- Selecting a CPSA Company (from the CPSA List) to conduct their PCI Card Production Assessment, as applicable.
- Providing sufficient documentation to the CPSA Company to support the PCI Card Production Assessment.
- Having documentation requested by the CPSA Employee prior to the Card Production Assessment assembled at the beginning of the assessment.
- Providing related attestation—e.g., proper scoping and network segmentation.
- Remediating any issues of non-compliance as required.
- Signing the PCI Card Production Attestation of Compliance (CPSA AOC).
- Providing feedback on CPSA performance in accordance with the CPSA Feedback Form on the Website.
- Notifying Participating Payment Brands if they suspect or discover a cardholder data breach.

6 Qualification Process

To determine that CPSA Companies and CPSA Employees possess the requisite knowledge, skills, experience, and capacity to perform PCI Card Production Assessments in a proficient manner and in accordance with industry expectations, each company, and at least one individual employee thereof performing PCI Card Production Assessments (Logical and/or Physical) must at all times be qualified by PCI SSC as a CPSA Company or CPSA Employee (as applicable), and then must maintain that qualification in Good Standing in accordance with the CPSA Requirements.

CPSA Employees are qualified to perform PCI Card Production Assessments only to the major version of the *PCI Card Production Security Requirements* for which they have successfully completed training and examination.

The following sections introduce the procedures, requirements, and forms that are applied by the PCI SSC to qualify a CPSA Company and CPSA Employee to assess compliance with the *PCI Card Production and Provisioning Security Requirements.* The qualification process is described in detail within a separate *PCI Card Production Security Assessor Qualification Requirements* document.

6.1 CPSA Company Qualification

To begin the application process, a candidate CPSA company should obtain access to the PCI Assessor Portal to facilitate completion of the applications and submittal of supporting documentation. See Section 6.4 below for more details on the Assessor Portal.

The qualification criteria for the CPSA Company are in the CPSA Qualification Requirements document. The CPSA Company application can be found as Appendix C in that document and is also available online in the Assessor Portal.

In order to achieve qualification as a CPSA Company, the candidate company and at least one of its employees must satisfy all applicable CPSA Requirements (defined in the CPSA Qualification Requirements) applicable to CPSA Companies and CPSA Employees. All such CPSA Companies are then identified on the CPSA List on the Website, and all such CPSA Employees are added to the Website's search tool.

Only those CPSA Companies and CPSA Employees qualified by PCI SSC and included in the CPSA List on the PCI website are recognized by PCI SSC to perform PCI Card Production Assessments.

6.1.1 CPSA Company Business Requirements

- Business Legitimacy Requirements
  - Business license, legal history
- Independence Requirements
  - Code of Conduct policy and conflict of interest restrictions
- Insurance Coverage Requirements

6.1.2 CPSA Company Services and Experience

- The CPSA Company must possess applicable technical security assessment experience similar or related to PCI Card Production Assessments.
- The CPSA Company must have a dedicated information security practice that includes staff with specific job functions that support the information security practice.

6.1.3 CPSA Company Administrative Requirements

- Primary and secondary contact
- Background checks
- Quality Assurance (see Section 8 below)

6.2 CPSA Employee Qualification

6.2.1 Logical Assessor Skills and Experience

- Background Checks
- Industry Certification
- Advanced experience in cryptography, network security, system security, and IT auditing or security assessments
- Employee of CPSA company

6.2.2 Physical Assessor Skills and Experience

- Background Checks
- Advanced experience in physical security and physical security audits
- Experience in system security. System security refers to the logical security of systems that provide or enforce physical security—e.g., CCTV and access-control systems
- Employee of CPSA company

6.3 Requalification

All CPSA Companies must be requalified by PCI SSC on an annual basis. The annual requalification date is based upon the CPSA Company's *original qualification date*. Requalification requires payment of the annual CPSA Company fee and continued compliance with applicable CPSA Requirements.

A CPSA Employee must requalify with PCI SSC on an annual basis by their requalification date for each of their CPSA Program qualifications. In order to requalify:

Each CPSA-L must:

(a) Complete at least three (3) Logical PCI Card Production Assessments for different facilities over the previous one-year period ***and*** complete PCI SSC computer-based CPSA-L training course/exam.

or

(b) Successfully complete PCI SSC instructor-led CPSA Logical training course and exam.

Note: *CPSA Employees who do not complete the required number of assessments must register and complete PCI SSC CPSA Instructor-led training and exam prior to their requalification date to remain listed as an active assessor. PCI SSC CPSA Instructor-led training is subject to availability.*

Each CPSA-P must:

(a) Complete at least three (3) Physical PCI Card Production Assessments for different facilities over the previous one-year period ***and*** complete PCI SSC computer-based CPSA Physical training course/exam.

or

(b) Successfully complete PCI SSC instructor-led CPSA-P training course and exam.

The annual requalification date is based upon the CPSA Employee's *previous qualification date*. Requalification requires proof of training successfully completed and continued compliance with applicable CPSA Requirements. Regardless of when the CPSA Employee completes their requalification requirements within the grace period described below, the requalification date remains the same. *For example, a one-year requalification for a certification with a current qualification date of 15 November of a given year will be changed to 15 November one year later upon successful completion of requirements, regardless of whether the requalification was completed on 31 October or 25 November of that year.*

Note: *Negative feedback from Card Production Entities, PCI SSC, Participating Payment Brands, or others may impact the CPSA Company's and/or CPSA Employee's eligibility for requalification. (see Requirement 6.2 in CPSA Qualification Requirements)*

6.3.1 Requalification Timeframe

To help ensure adequate time to complete requalification requirements, CPSA Employees should note:

- Registration for requalification training must be completed prior to the CPSA Employee's qualification expiration date. A candidate who is not registered prior to that expiry date must re-enroll as a new candidate and successfully complete Instructor-led training.
- A two-week grace period is provided beyond the candidate's expiry date in order to complete requalification training; however, candidates will be removed from the CPSA Assessor List and will not be qualified by PCI SSC during this time and will not be requalified until the requalification exam is successfully completed.
- Access to the requalification course and exam will be granted only after payment is processed by PCI SSC, and candidates will have access to the exam up to four calendar weeks prior to, and two calendar weeks past their expiration date.
- If a candidate is registered for requalification training and fails to take the training or fails the exam within the defined period, payment will be forfeited in full and the individual must reapply as a new CPSA Employee candidate.

6.4 Fees

Each CPSA Company must pay an annual CPSA Company fee to maintain qualification as a CPSA Company. The CPSA Company fee as well as applicable CPSA Employee training fees are specified on the Website in the *PCI SSC Programs Fee Schedule* and are subject to change.

All fees must be paid in US dollars (USD) by check, by credit card, or by wire transfer to the PCI SSC bank account specified for such purpose on the lower half of the invoice.

The option for credit card payment is not offered on CPSA Company fee invoices. However, the option can be added to the invoice upon request. A fee of 3% of the total invoice will be added for processing.

6.5 CPSA Continuing Professional Education (CPE)

- CPSA Employees with active industry certifications[1] are not required to provide proof of CPEs to PCI SSC.
- A CPSA Employee with no active industry certifications[1] must earn a minimum of 10 CPE credits per year in accordance with the current version of the PCI SSC CPE Maintenance Guide.

[1] Industry certifications refer to those in List A and List B from Section 3.2 of the *CPSA Qualification Requirements*.

6.6 Primary Contact

The CPSA Company must designate a Primary Contact (via CPSA Company Application) to act as communication liaison to PCI SSC. The Primary Contact has sole authorization to submit, add, change, or delete assessor requests to PCI SSC related to the Program. PCI SSC must be notified immediately in writing if there is a change in the Primary Contact. The Primary Contact is not required to be an assessor.

Notices from PCI SSC to the Primary Contact may be communicated via the Assessor Portal, e-mail, registered mail, or any other method permitted by the CPSA Agreement.

It is the responsibility of the Primary Contact to respond to PCI SCC in a timely manner.

6.7 Assessor Portal

The Assessor Portal provides visibility and edit capability to CPSA Company account information and CPSA Employee details. It also provides information that is beneficial to CPSA Employees and helps facilitate their continued qualification. Qualified users are encouraged to review the information available via the Assessor Portal on a regular basis.

The Primary Contact is given initial access to the Assessor Portal once they complete and submit the online registration form on the Website.

Greater access to the Assessor Portal is granted to the Primary Contact once the company is qualified as a CPSA Company. CPSA Employees receive credentials and log-on instructions upon passing the CPSA Employee training exam, and PCI SSC enters their grades into the database. Primary Contacts receive a higher-level access than other employees.

Link to Assessor Portal: https://programs.pcissc.org/

The Assessor Portal includes the following information not available on the PCI Website:

- Library of published Assessor Newsletters
- Recorded Webinars
- CPSA Certificates in PDF format
- Primary contact name, e-mail, and address
- Individual Certification—i.e., CISSP, CISA, etc.—entry page with expiration date, if applicable

In addition to the items noted above, the Primary Contact has access to:

- Requalification training approval page for all CPSA Employees
- Insurance policies with respective expiration dates
- Complete list of all CPSA Employees for their Company and their respective qualification expiration dates
- Addresses for all CPSA training locations throughout the year

7 PCI Card Production Security Assessment Process

The policies and procedures by which compliance assessments are conducted are largely determined by the Participating Payment Brands but generally consist of the following milestones. The following sections describe what is a Participating Payment Brand responsibility and what PCI has defined as a requirement for the assessment process:

- Assessment Scheduling
- Assessment Preparation
- Facility Assessment
- Documenting the Assessment Results
- Assessment Result Submission
- Non-compliance Finding Remediation
- Evidence Retention
- Security Incident Response

Note: *Card Production Entities should consult with their Participating Payment Brands about their requirement for a Logical or Physical PCI Card Production Security Assessment.*

CPSA Employees must work only on those PCI Card Production Assessments for which they are qualified by PCI SSC, have appropriate skills, including technology and language, and have an appropriate understanding of the client's business.

7.1 Assessment Scheduling

To demonstrate compliance with the PCI Card Production Security Requirements, Card Production Entities may be required to have periodic PCI Card Production Assessments conducted as required by each Participating Payment Brand.

7.2 Assessment Preparation

To prepare for the assessment the assessor is expected to review the findings from the previous assessment. The assessor will determine the audit scope based on Card Production activities performed. The Card Production Entity must have completed the self-assessment portion of the Card Production ROC.

7.3 Facility Assessments

PCI Card Production Assessments are required to be conducted by a CPSA Company through its CPSA Employees, in accordance with the PCI Card Production Security Requirements, which contain requirements, testing procedures, and guidance to ensure that the intent of each requirement is understood.

Compliance with the PCI Card Production Security Requirements (Physical and Logical) is conducted onsite. Any controls that are assessed offsite must be identified and the results documented in the Card Production ROC. The Card Production ROC must accurately represent the assessed environment and the security controls evaluated by the CPSA Employee.

The use of remote assessment methods may be a suitable alternative in scenarios where an onsite assessment is not feasible.

Please refer to the *PCI SSC Remote Assessment Guidelines and Procedures* for both guidelines and procedures that may be adopted to determine whether all or part(s) of the facility assessments can be conducted remotely.

Prior to the engagement, the CPSA Company must consult with the Participating Payment Brands to determine any compliance impacts associated with the use of remote assessments.

7.4 Documenting the Security Assessment Results

For each PCI Card Production Assessment, the resulting Card Production and Provisioning Report on Compliance (Card Production ROC) must utilize the most current Card Production ROC Reporting Template then in effect. When the Card Production Security Requirements and/or the associated ROC is updated, the document version in effect will be determined by the implementation schedule announced for each update. The Card Production ROC must be accompanied by a Card Production Attestation of Compliance that summarizes whether the assessed entity is in compliance with the security requirements and identifies any related findings. The Card Production AOC must be signed by a duly authorized officer of the CPSA Company. The Card Production AOC summarizes the Card Production Entity that was assessed as either in compliance or not in compliance with the PCI Card Production Security Requirements, and any identified findings. The current security requirements and Card Production ROC and AOC Templates are available on the PCI Website.

The intent of requiring a signature from a “duly authorized officer” is to ensure that the CPSA Company is aware of and has formally signed off on the work being done and, accordingly, recognizes its obligations and responsibilities in connection with that work. Although the signatory’s job title need not include the term “officer,” the signatory must be formally authorized by the CPSA Company to sign such documents on the CPSA Company’s behalf and should be competent and knowledgeable regarding the CPSA Program and related requirements and duties. Each organization is different and is ultimately responsible for defining its own policies and job functions based on its own needs and culture.

By signing the CPSA AOC, the assessed entity is attesting that the information provided in the Card Production AOC and accompanying Card Production and Provisioning Report on Compliance is true and accurate. The date on the Card Production AOC cannot predate the Card Production ROC.

The Card Production AOC is submitted to the requesting entity/entities according to applicable Participating Payment Brand rules.

7.5 Assessment Result Submission

The CPSA Employee is expected to submit the assessment results within one calendar month of the completion of the facility assessment.

7.6 Non-Compliance Finding Remediation

Non-compliance finding remediation is determined by the Participating Payment Brands.

7.7 Assessment Evidence Retention

As per Section 4.5 “Evidence (Assessment Workpaper) Retention” of the CPSA Qualification Requirements, CPSA Companies must gather evidence to support the contents of each Card Production ROC. The CPSA Company must secure and maintain, for a minimum of three (3) years from the Card Production ROC completion date, digital and/or hard copies of case logs, audit results, workpapers, e-mails, interview notes, and any technical information—e.g., screenshots, configuration settings—that were created and/or obtained during the PCI Card Production Assessment. This information must be available upon request by PCI SSC and Participating Payment Brands. The CPSA Company must also provide a copy of the evidence-retention policy and procedures to PCI SSC upon request.

If a Card Production Entity refuses to provide the CPSA Company with the documentary evidence—for example, because it contains information that is sensitive or confidential to the Card Production Entity—the CPSA Company and the Card Production Entity should work together to ensure that the evidence is retained securely at the Card Production Entity site and as required by the CPSA Qualification Requirements, including being made available to PCI SSC upon request for a minimum of three (3) years from the date of Card Production ROC completion of the applicable PCI Card Production Assessment. To accomplish the above, the CPSA Company will need to establish a formal agreement with the Card Production Entity that outlines each party’s responsibilities in the retention of evidence. Any agreement must be consistent with and comply with the disclosure requirements specified in the CPSA Agreement.

Even if the actual, documented evidence is to be retained by the Card Production Entity, the CPSA Company must keep records to identify the specific evidence that was used during the PCI Card Production Assessment—for example, digital and/or hard copies of the documents or testing results that are being retained by the Card Production Entity. The CPSA Company’s records should clearly identify which pieces of evidence were used for each requirement, how the evidence was validated, and the findings that resulted from each piece of evidence. The CPSA Company should retain enough Information to ensure that the complete, actual evidence used during the PCI Card Production Assessment can be identified for retrieval if needed; for example, in the event of an investigation or if a finding needs to be reviewed.

As part of the PCI SSC’s Assessor Quality Management (“AQM”) CPSA Program audit process (“CPSA Audit”), and in other AQM quality-assurance (“QA”) review work as needed, it is common for AQM to request both the CPSA Company’s Workpaper Retention Policy and a sample of PCI Card Production Assessment workpapers. This is to ensure the CPSA Company has a current documented, implemented Workpaper Retention process consistent with the requirements defined in the CPSA Qualification Requirements—including the appropriate level of detailed instructions with which the CPSA Employees must comply. AQM may additionally request blank and/or executed copies of the CPSA Company’s Workpaper Retention Policy agreement that each CPSA Employee is required to sign, and may request additional evidence to demonstrate that all assessment results and related materials relating to the PCI Card Production Assessments for the sampled Card Production ROC were in fact retained in accordance with the procedures defined in the Workpaper Retention Policy prior to releasing the final Card Production ROC for that PCI Card Production Assessment.

For details on what the CPSA Company’s Evidence Retention Policy must include, please see Section 4.5 of the CPSA Qualification Requirements document available on the Website.

7.8 Security Incident Response

A CPSA Employee must notify a Card Production Entity if, during any CPSA Program related service, they become aware of an actual or suspected breach of cardholder data within the Card Production Entity's environment. In addition, the CPSA Employee must notify the Card Production Entity in writing of the incident and related findings and inform the Card Production Entity of its obligations to notify the Participating Payment Brands in accordance with each Participating Payment Brand's notification requirements. The notification must be retained in accordance with the CPSA Company's evidence-retention policy along with a summary of the incident and what actions were taken. The CPSA Company must have a documented process for all the above actions.

8 Assessor Quality Management Program

The CPSA Company must have implemented an internal quality-assurance program as documented in its Quality Assurance Manual. The main purpose of the CPSA Audit is for PCI SSC to validate two points: (1) that the CPSA has documented quality-assurance processes as required per the CPSA Qualification Requirements; and (2) that those documented quality-assurance processes are implemented and sustained. As part of CPSA Audits, PCI SSC's Assessor Quality Management (AQM) team performs a holistic review of the CPSA Company's internal documentation required by the CPSA Qualification Requirements, as well as reviews of Card Production ROCs to provide reasonable assurance that the documentation of testing procedures performed is sufficient to demonstrate compliance. Refer to Appendix A to understand sample criteria against which CPSA Companies are measured during CPSA Audits.

A CPSA Audit by the PCI AQM team will result in a finding of:

- **Satisfactory –** A notification letter will be sent with specific opportunities for improvement listed. Mandatory call with AQM team to discuss.

  A "Satisfactory" finding indicates that the audit findings reasonably confirmed (1) the CPSA Company/Employee's on-going adherence to the current CPSA Qualification Requirements; (2) that the CPSA Company's quality policy documentation is implemented and maintained according to the CPSA Qualification Requirements; and (3) the CPSA Company/Employee's on-going general adherence to reporting requirements as evidenced by sampled CPSA ROCs.

- **Needs Improvement –** A notification letter will be sent with specific opportunities for improvement listed. Mandatory call with AQM team to discuss.

  A "Needs Improvement" finding indicates that there were minor findings and/or opportunities for improvement identified that assessors should address to ensure continued adherence with program documentation. Still, the audit findings reasonably confirmed (1) the CPSA Company/Employee's on-going adherence to the current CPSA Qualification Requirements; (2) that the CPSA Company's quality policy documentation is implemented and maintained according to the CPSA Qualification Requirements; and (3) the CPSA Company/Employee's on-going general adherence to reporting requirements as evidenced by sampled CPSA ROCs.

- **Unsatisfactory –** A notification letter is sent with specific opportunities for improvement. Mandatory call with AQM team to discuss Remediation.

  An "Unsatisfactory" finding indicates that there were serious findings identified during the CPSA Audit, including possible Violations to the CPSA Agreement. This finding will result in Remediation and/or Revocation, per the current CPSA Qualification Requirements. Audit findings that result in an Unsatisfactory finding mean that AQM could not confirm one or more of the following: (1) the CPSA Company/Employee's on-going adherence to the current CPSA Qualification Requirements; (2) that the CPSA Company's quality policy documentation is implemented and maintained according to the CPSA Qualification Requirements; and (3) the CPSA Company/Employee's on-going general adherence to reporting requirements as evidenced by sampled CPSA ROCs.

For further details on the Assessor Quality Management Program, please see the *CPSA Qualification Requirements* document available on the Website.

8.1 Ethics

The CPSA Company must adhere to professional and business ethics, perform its duties with objectivity, and limit sources of influence that might compromise its independent judgment in performing PCI Card Production Assessments.

PCI SSC has adopted a *PCI SSC Code of Professional Responsibility* (the "Code," available on the Website) to help ensure that PCI SSC-qualified companies and individuals adhere to high standards of ethical and professional conduct. All PCI SSC-qualified companies and individuals must advocate, adhere to, and support the Code. Among other things:

- CPSA Companies and CPSA Employees are prohibited from performing PCI Card Production Assessments of entities that they control or are controlled by, and entities with which they are under common control or in which they hold any investment.

Note: *CPSA Employees are permitted to be employed by only one CPSA Company at any given time.*

- CPSA Companies and CPSA Employees must not enter into any contract with a Card Production Entity that guarantees a compliant CPSA ROC.
- CPSA Companies must fully disclose in the CPSA Report on Compliance if they assess Card Production Entities who use any security-related devices or security-related applications that have been developed or manufactured by the CPSA Company, or to which the CPSA Company owns the rights, or that the CPSA Company has configured or manages.
- Each CPSA Company agrees that when it (or any CPSA Employee thereof) recommends remediation actions that include one of its own solutions or products, the CPSA Company will also recommend other market options that exist.
- Each CPSA Company must adhere to all independence requirements as established by PCI SSC. For a complete list, please see Section 2.2 in the CPSA Qualification Requirements.

8.2 Feedback Process

At the start of each PCI Card Production Assessment, the CPSA Company must direct the Card Production Entity to the CPSA Feedback Form on the Website and request that the Card Production Entity submit the completed form to PCI SSC through the PCI SSC website following the PCI Card Production Assessment.

Any Participating Payment Brand or Card Production Entity may submit CPSA Feedback Forms to PCI SSC to provide feedback on a PCI Card Production Security Assessment, CPSA Company, or CPSA Employee.

8.3 Security Remediation Process

CPSA Companies that do not meet all applicable quality-assurance standards set by PCI SSC may be offered the option to participate in PCI SSC's CPSA Company Quality Remediation program ("Remediation"). PCI SSC may offer participation in Remediation in connection with any quality-assurance audit, any Violation (as defined in the CPSA Qualification Requirements), or any other PCI SSC Program-related quality concerns, including but not limited to unsatisfactory feedback from Card Production Entities or Participating Payment Brands. The Remediation process includes:

- Remediation overview call and signed Remediation Agreement.
- Remediation Period of at least 120 calendar days.
- CPSA Company listing on the CPSA List updated to "red" to notify merchants/service providers.
- An AQM case manager assigned to the CPSA Company to offer support as it works to bring its quality level to the required baseline standard of quality.
- The expectation of strong commitment from the CPSA Company to achieve successful completion.
- Fees for review of work.

8.4 Revocation Process

A CPSA Company (or any CPSA Employee thereof) may be subject to revocation of its PCI SSC qualification ("Revocation") if found to be in breach of the CPSA Agreement or other CPSA Requirements, including without limitation, for any of the following:

- Failure to perform PCI Card Production Security Assessments in accordance with the PCI Card Production Security Requirements or CPSA Program.
- Violation of any provision regarding non-disclosure of confidential materials.
- Failure to maintain at least one certified CPSA Employee on staff.
- Failure to maintain physical, electronic, and/or procedural safeguards to protect confidential and sensitive information.
- Unprofessional or unethical business conduct.
- Failure to successfully complete applicable required PCI SSC training.
- Cheating on any PCI SSC exam.

Upon notification of pending CPSA Company Revocation by PCI SSC, the CPSA Company or CPSA Employee will have 30 calendar days in which to appeal in writing to PCI SSC.

Revocation will result in the CPSA Company or CPSA Employee being removed from the CPSA List or search tool, as applicable.

In the event of CPSA Company Revocation, the CPSA Company must immediately cease all advertising of its CPSA Company qualification. It must also immediately cease soliciting for and performing all pending and active PCI Card Production Assessments unless otherwise instructed by PCI SSC and comply with all post-revocation requirements specified in the CPSA Agreement.

Refer to the CPSA Qualification Requirements for details on the Revocation process.

9 General Guidance

9.1 Resourcing /Transfers

The CPSA Company is expected to arrange sufficient back-up of CPSA Employee resources so as not to impact a Card Production Entity's validation deadline in the event an assigned CPSA Employee is unable to complete a PCI Card Production Assessment.

CPSA Employees may transfer to other companies. The following should be noted when a CPSA Employee moves to a new company:

1. If the new company is not an active CPSA Company, the CPSA Employee's qualification will be inactive until employed by an active CPSA Company. Inactive status does not suspend or modify requalification deadlines. A CPSA Employee cannot requalify while its employer is not an active CPSA Company.
2. If the CPSA Employee moves to an active CPSA Company and is to be utilized by that CPSA Company as an CPSA Employee, the Primary Contact of the new CPSA Company must notify the CPSA Program Manager prior to permitting the CPSA Employee to participate in any PCI Card Production Assessment. The following information must be provided to the CPSA Program Manager:
   - Name
   - E-mail
   - Phone

9.2 PCI SSC Logos and Marks

Unless expressly authorized, a CPSA Company or CPSA Employee is not permitted to use any PCI SSC trademark, service mark, certification mark, or logo without the prior written consent of PCI SSC in each instance. A CPSA Program-specific logo is available on request via e-mail to the CPSA Program Manager.

***Note*:** *PCI SSC does not issue an official PCI seal, mark, or logo that companies can use when they achieve PCI Card Production compliance. Please note that the PCI SSC logo is a registered trademark and may not be used without authorization. You may not use or encourage or enable others to use the phrases or marks "PCI Compliant," "PCI Certified," " PCI Card Production Compliant," "PCI Card Production Certified," or "PCI" with check marks or any other mark or logo that suggests or implies compliance or conformance with PCI SSC standards*.

9.3 CPSA Company Changes

In the event that a CPSA Company requires an alias or a trade name added to its listing on the Website—for example, "trading as" or "doing business as" (DBA) scenarios—please contact the CPSA Program Manager for the *Assessor Name Change Request Form.*

9.4 FAQs and Guidance Documents

CPSA Employees should refer to the Frequently Asked Questions (FAQ) section of the PCI SSC Website to obtain further guidance on questions relating to PCI Card Production Assessments. The Website should be monitored on a weekly basis as information is updated. RSS feed updates are available for the PCI Standards in the Document Library.

Note: *Additional FAQs may also be found in the Frequently Asked Questions Category for each Standard in the Document Library on the Website.*

CPSA Employees should periodically familiarize themselves with all Information Supplements and guidance published to the Website.

Appendix A: Quality Criteria for CPSA

As part of AQM's monitoring of quality within the CPSA Program, AQM performs holistic CPSA Audits of CPSA Companies and solicits stakeholder feedback against the following general criteria:

- CPSA Company documentation (per the CPSA Qualification Requirements)
- Workpapers/Evidence Retention
- Ethics
- Reporting
- Additional Quality Criteria

Examples of quality criteria that AQM may seek to validate are as follows:

CPSA Company Documentation (per the CPSA Qualification Requirements)	
1	CPSA Company's QA Manual includes an accurate QA process flow, identification of QA manual process owner, and evidence of annual review by the QA manual process owner.
2	CPSA Company's QA Manual includes a requirement for all CPSA Employees to regularly monitor the Website for updates, guidance, and new publications relating to the CPSA Program.
3	CPSA Company's Code of Conduct Policy supports—and does not contradict—the PCI SSC Code of Professional Responsibility.
4	CPSA Company's Security and Incident Response Policy is consistent with PCI SSC guidance and is appropriately available within the CPSA Company.
Workpapers/Evidence Retention	
1	CPSA Company's Evidence Retention Policy includes all required content defined within the CPSA Qualification Requirements. For example, it includes formal assignment of an employee responsible for ensuring the continued accuracy of the Workpaper Retention Policy.
2	Relevant evidence is provided by CPSA Company for all validation activities that are required to be performed.
3	CPSA Company was able to provide a blank copy of the employee acknowledgement form for the CPSA Company's Workpaper Retention Policy, as well as produce copies signed by the CPSA Employee(s).
Ethics	
1	CPSA Company and CPSA Employees fulfilled the objective of providing an independent, unbiased representation of the facts of the case, including no significant or intentional omissions or misrepresentations of facts. *For example: Had the assessor fulfilled their obligation to inform the assessed entity of their responsibility to report suspected breaches to Participating Card Brands within 24 hours?*

2	CPSA Company and CPSA Employees maintained independence throughout the engagement and provided adequate reporting as to how this was validated and maintained.

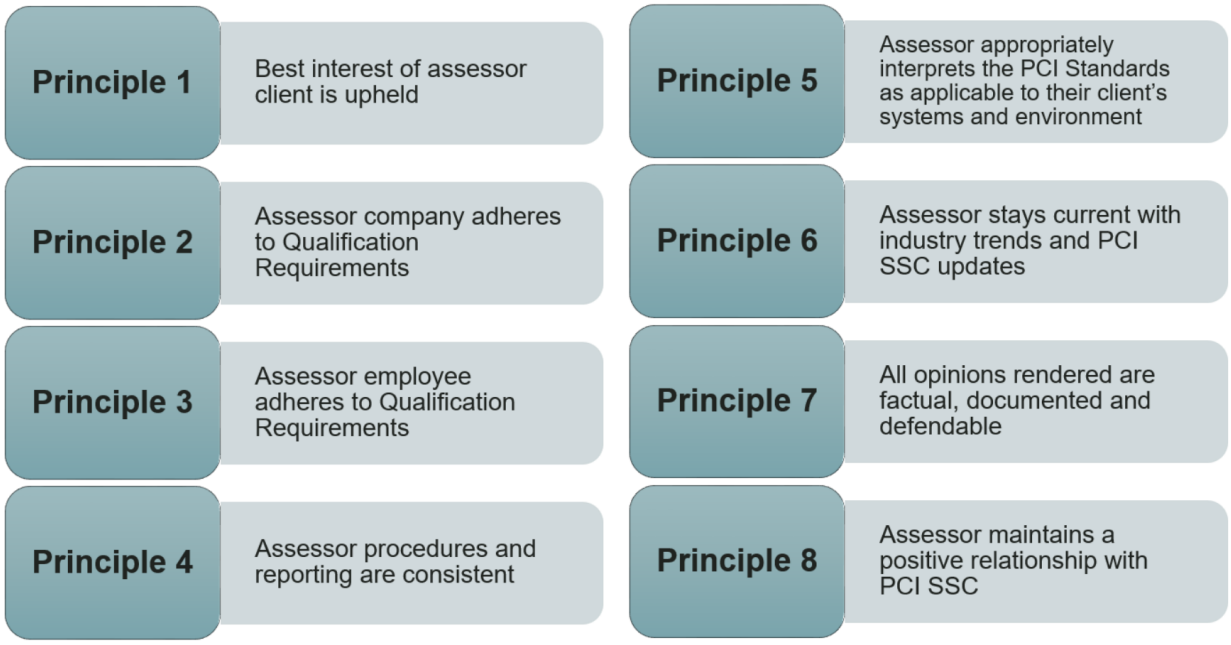
Reporting	
1	CPSA Company and CPSA Employees used the appropriate templates for reports.
2	CPSA Company and CPSA Employees submit Card Production ROCs to stakeholders in a timely manner, no later than four (4) weeks from completion of facility assessment.
3	CPSA Company and CPSA Employees provided clear, consistent detail as to how requirements were validated to be in place, avoiding excessive use of cut and paste. *For example, documented finding should be appropriate for the requirement; description in response should reflect a reasonable level of clarity.*
4	CPSA Company and CPSA Employees addressed all Reporting Instructions, and expected content is present and substantively addressed, including but not limited to: ▪ Facility identification ▪ Services confirmation ▪ Previous finding resolution status and details ▪ Facility and production environment description ▪ Network diagram(s) ▪ Key life cycle summary
5	CPSA Company and CPSA Employees provided a thorough response that includes details of testing and observation to validate the integrity of the segmentation within the Summary Overview.
6	When explaining how the CPSA Company and CPSA Employees evaluated that the scope was accurate and appropriate, CPSA Company and CPSA Employees included sufficient detail to demonstrate the findings that validated the scope (rather than just the method used), including reporting of conditions that impact audit scope.
7	CPSA Company and CPSA Employee responses go beyond repeating the verbiage within the Card Production ROC Reporting Template and include substantive and relevant detail as to how the testing procedure was in place/not in place.

Additional Quality Criteria	
1	CPSA Company and CPSA Employees maintain positive relations with the PCI SSC Members, including the Participating Payment Brands. As it relates to the PCI SSC Members accepting Card Production ROCs, this may include but is not limited to, delivery of items within discussed timelines, consistent communication/cooperation, etc.
2	CPSA Company and CPSA Employees adequately prepare for the audit, including but not limited to: • Define audit scope and expected activities • Audit scheduled when due • Establish onsite and/or remote (as applicable) viewing and access expectations
3	CPSA Company and CPSA Employees adequately perform the audit process, including but not limited to: • Identify changes since last audit • Verify previous finding status • Comply with test procedures and review appropriate evidence • Exhibit knowledge of requirements • Perform end of audit result review
4	CPSA Company and CPSA Employees adequately provide post-audit support, including but not limited to: • Finding clarification • Finding disputes

Appendix B: Eight Guiding Principles Validated by Four Criteria (Four Cs)

The Eight Guiding Principles represent a baseline for PCI SSC assessor companies and individuals (each an "Assessor") quality, and those principles can be validated by four criteria: consistency, credibility, competency, and conscientiousness—or "the Four Cs."

The Eight Guiding Principles are as follows:



PCI SSC reviews Assessor work product and stakeholder feedback with the expectation that the Assessor has followed the requirements of the applicable PCI SSC Program as documented in applicable Program documentation and has acted in the best interest of the customer in an ethical manner that results in factual, documented, and defendable opinions. Program participants must keep up with PCI SSC updates (included but not limited to updates to the CPSA Qualification Requirements and CPSA Program Guide, monthly Assessor Newsletter articles, published FAQs on the Website, and content from relevant webinars).

The Four Cs are useful measurements to evaluate the strength and quality of the Assessor's approach and/or conclusions and can help the Assessor ensure that work can be defended in a meaningful way.