# Payment Card Industry (PCI)
# Remote Assessment

## Guidelines and Procedures

**Version 1.0**

September 2021

# Document Changes

| Date | Version | Description |
|---|---|---|
| September 2021 | 1.0 | Initial release. |
| | | |

# Table of Contents

# 1 Introduction

Remote assessments involve the use of technologies to gather information, interview persons, and make observations in situations where onsite assessment methods are not possible or practical. Advancements in communication and collaboration technologies have made some remote assessment activities more accessible; however, there are also limitations and risks associated with the use of remote assessments. Table 1 describes some of the opportunities and challenges associated with performing assessment activities remotely.

**Table 1. Opportunities and Challenges Associated with Remote Assessments**

| Opportunities | Challenges |
|---|---|
| • Avoids exposure to health and safety risk factors and travel to unsafe regions<br>• Supports continuation of business and assessment goals during lockdown protocols<br>• Facilitates testing of a greater geographical range of locations<br>• Interviews with entity personnel are not restricted by physical location<br>• Potential for more assessors with specialist expertise to be involved in the assessment<br>• Facilitates assessments of areas that are in physically remote or difficult to access locations<br>• Mitigates challenges associated with personal accessibility needs<br>• Potential for increased sampling | • Misconception that a remote assessment requires less effort or rigor than an onsite assessment<br>• Reduced ability for assessor to witness controls and processes firsthand or as they occur<br>• Increased opportunities for non-compliances to be hidden or excluded from the review<br>• Additional confidentiality, integrity, and availability considerations for completion of assessment activities<br>• Additional considerations for ensuring evidence reliability and integrity<br>• Reliance on the availability and effectiveness of remote collaboration technologies<br>• Increased time needed for assessment preparation and planning, and to perform testing activities |

While onsite assessments continue to be the expected method for PCI SSC assessments, the use of remote assessment methods may provide a suitable alternative in legitimate scenarios (defined in Section *2.2*) where an onsite assessment is not feasible. This document defines procedures and guidelines to support the appropriate use of remote assessments, and includes:

- An overarching set of principles and procedures governing how remote assessment activities may be used in assessments to a PCI SSC standard. (Section *2*)
- Detailed guidelines and best practices on the use of remote testing methods for different types of testing activities. (Section *3*)
- Requirements and expectations for PCI SSC assessors regarding the use of remote assessment activities. (Section *4*)
- Report Template Addendum to document the use of remote assessment activities for PCI SSC Reports on Compliance (ROC) and Reports on Validation (ROV). *(Appendix A*)

The remote assessment approach defined herein is effective upon publication of this document.

***Note:** Some PCI SSC programs may have additional requirements related to the use of remote assessments. Refer to the Program Guide and Technical FAQs for the applicable standard/program to understand any additional requirements.*

## 1.1 Purpose and Intended Use

This document describes how remote assessment methods may be incorporated into practices for validating environments, solutions, and products to PCI SSC standards. These guidelines and procedures are intended to:

- Formalize an approach to support greater flexibility for completing assessments to PCI SSC standards where onsite testing is not feasible and remote assessments are allowed by the applicable compliance-accepting entity or PCI SSC validation program.
- Provide a consistent process for entities and PCI SSC assessors to follow.
- Incorporate assessment best practices into remote testing methods.
- Maintain assessor responsibility for determining whether remote testing produces a sufficient level of assurance to determine a finding.

These guidelines and procedures do not:

- Alter the applicability of a PCI SSC standard's security requirements to the entity or environment being assessed.
- Provide an option to validate to a PCI SSC standard without completing a full and thorough assessment.
- Solve all scenarios where onsite testing cannot be completed.

## 1.2 Applicability to PCI SSC Standards and Programs

These guidelines apply to the PCI SSC standards identified in Table 2, where the assessment is performed by a PCI SSC qualified assessor or PCI Recognized Laboratory, as applicable.

Table 2 also identifies whether the standard is associated with a PCI SSC validation program or a payment brand compliance program.

- PCI SSC validation program: Assessment results are associated with validation and listing on the PCI SSC website.
- Payment brand compliance program: Assessment results are associated with compliance programs defined and managed by a compliance-accepting entity, such as a payment brand or acquirer.

**Table 2. Applicable PCI SSC Standards and Programs**

| PCI SSC Standard | Associated with a PCI SSC Validation Program | Associated with a Payment Brand Compliance Program |
|---|---|---|
| P2PE | ✓ | |
| PA-DSS | ✓ | |
| Secure SLC | ✓ | |
| Secure Software | ✓ | |

| PCI SSC Standard | Associated with a PCI SSC Validation Program | Associated with a Payment Brand Compliance Program |
|---|---|---|
| CPoC[1] | ✓ | |
| SPoC[1] | ✓ | |
| 3-D Secure (3DS) Core | | ✓ |
| Card Production and Provisioning – Logical | | ✓ |
| Card Production and Provisioning – Physical | | ✓ |
| PCI DSS | | ✓ |
| PCI PIN | | ✓ |
| Token Service Provider (TSP) | | ✓ |

Except as noted in Table 2. Applicable PCI SSC Standards and Programs, the approach outlined in this document does not apply to lab-based evaluations of software or hardware performed by PCI Recognized Laboratories.

### 1.2.1 Remote Assessments and PCI SSC Validation Programs

For assessments associated with validation and listing on the PCI SSC website, the use of remote assessment methods is supported under the following conditions.

- It is not feasible or practical to perform the assessment activity onsite (refer to Section 2.2).
- The assessor is able to complete a thorough assessment using appropriate remote testing methods as described in this document.
- The assessor has a high degree of confidence that the assessment resulted in a full evaluation of the entity's in-scope environment for all applicable requirements.
- The assessor has a high degree of confidence in the accuracy and integrity of the evidence reviewed and observed.
- The assessor's level of confidence in the remote testing results is equal to the level of confidence they would have achieved through onsite testing.
- The assessor has a high degree of assurance in the overall assessment result.

If the assessor does not have sufficient confidence that these conditions have been achieved, the assessment results cannot be used for a PCI SSC validation program.

### 1.2.2 Remote Assessments and Payment Brand Compliance Programs

For assessments associated with a payment brand compliance program, the assessed entity should consult with the compliance-accepting entity prior to scheduling and conducting the assessment to confirm any requirements they may have regarding the use of remote assessments.

[1] Applicable to the assessment of requirements related to back-end systems, attestation components, and/or monitoring environments.

# 2 Remote Assessment Procedures

These procedures aim to support the most robust remote assessment methods possible that, in combination with other controls as needed, may help assessors attain the necessary level of assurance and confidence in the results of a remote assessment.

The following principles are to be followed when considering the use of remote assessment methods.

- Remote assessment activities must not reduce or negatively impact the security of the environment being assessed.
- Remote assessment activities must not require violation of a PCI standard security requirement in order to assess an environment to that standard.
- Remote assessment activities must be designed and implemented in a manner intended to avoid introducing additional risk of disruption to the entity's operations.
- Remote assessments must be performed with the same rigor and integrity as an onsite assessment.

## 2.1 Summary of Approach

PCI SSC's approach to remote assessments is summarized as follows:

- Onsite assessments continue to be the expected method for validation assessments.
- Where it is not feasible or practical to conduct an assessment activity onsite (refer to Section *2.2*), suitable remote testing alternatives may be considered as outlined in these guidelines.
- Remote assessments should be undertaken only after a thorough feasibility analysis.
- All measures should be taken to ensure that the results of a remote assessment activity are commensurate with those resulting from an onsite assessment.
- The use of remote assessment methods does not reduce an assessor's responsibility for ensuring the quality and accuracy of the assessment process.
- It is not always possible to complete an assessment remotely—for example, where the assessor is unable to fully observe the requisite systems or facilities remotely, or where full testing or verification of evidence can occur only onsite at the entity's location.
- Where an assessment activity cannot be completed remotely or does not provide the assessor with sufficient evidence to determine whether controls are properly implemented, the assessment is considered incomplete until onsite testing can be performed.
  - For assessments associated with a PCI SSC validation program, incomplete assessments are not accepted.
  - For assessments associated with a payment brand compliance program, the impact of an incomplete assessment on the entity's compliance is determined by the compliance-accepting entity.

Details for reporting incomplete assessment findings are provided in *Appendix A, Addendum for ROC/ROV: Remote Assessments*.

## 2.2 Determining the Need for a Remote Assessment

Because an onsite assessment can often provide greater insights and security assurance than a remote assessment, the use of fully remote assessments should be considered only when there are clear and unavoidable barriers that prevent an onsite assessment from taking place. Where such barriers do not exist, assessors are expected to perform onsite assessments as defined in the applicable standard and program.

Reasons for not completing an onsite assessment should be defendable and based on a rational and realistic evaluation of the situation. Legitimate reasons include scenarios where completion of an onsite assessment is hindered by external factors, for example:

- Restrictions on the ability to travel or meet in person due to health and safety concerns or government advisories.
- Geographic locations that are physically inaccessible or difficult to reach.

There may also be business and operational practicalities that support the use of remote assessment methods over onsite testing, for example:

- The entity operates in a virtual environment without physical premises or facilities. This includes scenarios where the entity has outsourced all its infrastructure to a third-party provider that has been separately assessed and all the entity's personnel work from home.
- The testing required for a particular location is limited to documentation reviews and interviews, and no requirements related to observation of processes, systems, or the physical environment apply to the location.

For many assessments, a combination of onsite and remote testing may provide a suitable balance, as it allows for increased efficiencies in the assessment process while enabling an appropriate level of assurance to be achieved in the assessment result. For example, documentation reviews can often be performed remotely without significant loss of assurance,[2] whereas observations of processes and environmental characteristics will generally require an onsite review.

Where it is not practical or feasible to perform an assessment activity onsite or the entity requests that the assessment be performed remotely, the entity and assessor should work together to determine whether and to what extent remote assessment methods could be used to meet the assessment objectives. If the use of remote assessment methods does not provide the level of assurance needed to produce an assessment result, an onsite assessment will be required.

### *2.2.1 Performing a Feasibility Analysis*

Where there are legitimate reasons or hinderances preventing an onsite assessment from taking place, a feasibility analysis should be performed to help the entity and assessor determine whether remote testing methods could provide a feasible alternative to onsite testing to facilitate completion of the assessment.

Testing activities that are typically suited to remote assessments include the following, but will depend on the specific circumstances:

[2] Some documentation may have security and/or integrity requirements that preclude the use of remote testing methods.

- Reviews of documentation – for example, reviews of policies and procedure documents, training materials, and records of personnel acknowledgment of their security responsibilities.
- Interviews – for example, to verify that personnel understand the policies and procedures, or to describe the process that was followed to record personnel's acknowledgment of their security responsibilities.

Testing activities that require the assessor to observe systems, physical controls, or processes being performed are typically the most challenging to complete remotely. Being onsite and actively observing the control or process in action is often the only way for an assessor to get a true picture of the entity's environment and make an accurate determination about what is implemented and whether a requirement is being met.

The use of remote testing methods as an alternative to onsite observation should be considered only after a thorough feasibility analysis has been completed.

Performing this analysis requires an understanding of the people, processes, technologies, locations, and physical facilities to be included in the assessment, as well as the methods and tools that are available for use during the assessment. These methods and tools need to be evaluated to determine whether their use will support completion of the required testing with accurate results.

The feasibility analysis should be completed prior to the commencement of any testing and is a joint effort between the assessors involved in the assessment and applicable entity personnel.

Some of the topics to be addressed in the feasibility analysis include:[3]

1. Confidentiality, security, and data protection requirements
   - Are requirements for maintaining the confidentiality, security, and protection of the entity's data clearly defined?
   - Are processes and controls available to ensure that confidentiality, security, and data protection requirements can be maintained throughout the assessment?
2. Availability and effectiveness of remote assessment technologies
   - Do the assessor and entity agree on the technologies to be used, and are all participants trained and comfortable in their use?
   - Are protocols for proper use of the technologies defined and documented?
   - Is there a stable online connection that provides high bandwidth and transmission quality?
   - Do the technologies allow access to relevant information required for the assessment?
   - Do the technologies allow for authentication of interviewees to confirm identity?
   - Do the technologies allow for unhindered observation of facilities, processes, and activities as required to complete the assessment?

[3] Adapted from ISO 9001 Auditing Practices Group Guidance on Remote Audits Editon1 2020-04-16

3. Entity personnel
   - Is it possible to access and interview all entity personnel who are relevant to the assessment?
   - Are authorized personnel present at entity locations to facilitate remote observations and walkthroughs?
4. Operational support
   - Does the entity have the personnel and resources available to support a thorough assessment process?
   - If, due to contingency situations, the entity is not operating as usual, do the processes and activities being observed during the assessment accurately represent the entity's current operations?
5. Assessment scope and completeness

   Are the complexities of the entity's operations and processes fully understood by the assessor to the extent that:
   - The scope of the assessment is accurately defined and accounts for all people, processes, technologies, locations, and facilities that are relevant to the assessment?
   - All assessment and testing activities can be completed and will result in a full evaluation of all applicable requirements?
6. Quality and reliability of digital evidence
   - Will documentation and data be provided of sufficient digital quality to enable verification of their content and attributes?

During the analysis, the entity and assessor should identify any challenges and potential risks associated with the remote testing and determine whether it is feasible for testing to be thoroughly completed to produce a high level of confidence in the assessment results.

The results of the feasibility analysis—including the risks and challenges associated with use of the remote testing methods, and any mitigating controls for overcoming the risks and challenges—should be documented and agreed upon by both the entity and assessor. A copy of the feasibility analysis results should be included with the applicable ROC/ROV. Entities and assessors may be required to produce the analysis upon request by the PCI SSC or applicable compliance-accepting entity.

### *2.2.2 Initial Results of Feasibility Analysis*

The feasibility analysis will help determine which testing activities are feasible to perform remotely and which will need to be performed onsite. The results of the analysis will typically support one of the following initial conclusions:

- It is feasible for the assessment to be fully completed at this time, through the use of onsite methods, remote methods, or a combination of onsite and remote methods.
- It is feasible for the assessment to be partially completed at this time.
- An assessment is not feasible at this time.

Only assessments that can be fully completed, either through onsite testing methods, a combination of onsite and remote methods, or through remote methods alone, may be considered for PCI SSC validation programs.

For assessments associated with a payment brand compliance program, entities should consult with their compliance-accepting entity to determine any compliance impacts associated with the use of remote assessments. Where it is not feasible for an assessment to be fully and accurately completed, the entity should consult with their acquirer and/or payment brand to understand their expectations regarding partial or incomplete assessments and any deferral considerations.

***Note:*** *The feasibility analysis determines whether the use of remote testing methods is feasible for a particular assessment. Determining that a remote testing method is feasible does not guarantee that use of the testing method will produce the level of assurance needed for the assessor to reach a finding; this will depend on how the remote testing method is implemented and used, whether the testing can be completed for all applicable components and areas, and whether sufficient evidence is provided for the assessor to make a determination. Assessors and entities should continue to monitor and evaluate the effectiveness of the remote testing methods throughout the assessment to confirm whether the testing methods are performing as intended and whether additional testing may be needed.*

## 2.3 Preparing for the Remote Assessment

Communication and consultation are crucial for the success of a remote assessment. Assessor and entity personnel should be engaged in a meaningful way before beginning the assessment and plan for open and frequent communication throughout the assessment.

One of the challenges with remote assessment planning is overcoming a mistaken belief that the remote assessment will be easier, quicker, or require less effort than an onsite assessment. In actuality, remote assessments typically require more preparation and planning, and can take more time to complete, than an onsite assessment.

Planning meetings should involve the relevant assessor and entity personnel and result in a clear definition of who, what, where, when, and how the assessment will be conducted. Testing activities should be fully scoped and scheduled in advanced as much as possible. Spending additional time on planning up front will facilitate an efficient assessment process.

Examples of topics that should be discussed and agreed to in the planning phase include:

- Agreeing on meeting times, duration, and objectives.
- Roles and responsibilities for all participants, including oversight and escalation procedures.
- The technologies and methods that will be used throughout the assessment, including for each testing activity and subject, how the technology will be used, and best practices for its use.
- Confirming permission in advance for any taking of screenshots or recordings.
- Protocols to be followed for authorizing capture of video and images, including personnel privacy considerations.
- Confirmation of controls and processes to be used to ensure that data confidentiality, integrity, and security requirements are met, and how these controls and processes will be communicated for all participants to follow throughout the assessment.

- Identifying the people, processes, technologies, and locations to be included in the assessment, including:
  - Details of documentation and data to be reviewed
  - Details of interview participants, schedules, and interview objectives
  - Details of walkthroughs and observations to be performed, including locations, personnel to be present, and access considerations for confidential or restricted areas
  - Details of any sample sets to be used, as defined by the assessor

With thorough planning, assessors and entities can ensure that adequate time and resources are assigned to meet assessment objectives.

### *2.3.1 Duration and Timing Considerations*

While the overall depth and breadth of a remote assessment remains the same as an onsite assessment, the reliance on remote technologies may result in additional time being needed to complete individual testing activities. For example, the thorough observation of a facility may take longer when using remote methods compared to when the assessor is onsite. Additional time may also be needed in the event of unforeseen delays caused by technical issues or scheduling conflicts.

Activities that support an efficient assessment process include:

- Reviewing floor plans, schematics, data-flow diagrams, and network diagrams in advance, to gain an understanding of remote location layouts and identify the specific physical areas and locations of data that will need to be reviewed.
- Setting up any shared storage repositories, access accounts and credentials, and the necessary security protocols for assessor and entity personnel to securely access and share material during the assessment.
- Scheduling interview and meeting times well in advance and tracking acceptances to meeting requests.
- Scheduling assessment activities at appropriate times and durations to avoid “screen fatigue” during personnel interactions.
- Providing entity and assessor personnel with dedicated and controlled workspaces to minimize background noise and interruptions.
- Performing checks on the remote technologies prior to their use to confirm connectivity and audio/visual quality.
- Ensuring that assessor and entity personnel are trained and comfortable in the use of the remote technologies.

## 2.4 Use of Technologies for Remote Assessments

While much of the planning and processes involved in a remote assessment are similar to an onsite assessment, there is a greater reliance on technology for verifying objective evidence when the testing is performed remotely. The technologies and methods used for a remote assessment should be appropriate to support effective completion of the assessment in a manner that:

- Minimizes the security impact of the remote assessment to the entity's environment and any sensitive areas.
- Maximizes confidence in the integrity and assurance of the assessment result.
- Maximizes confidence in the security, accuracy, and reliability of collected evidence.
- Considers human factors in their use.

Section *3* identifies remote testing methods and includes detailed guidelines for their use.

The entity should not disable its security procedures and requirements, or allow them to be bypassed, for the purposes of a remote assessment. Where a remote assessment would require a breach of the entity's security rules, an onsite assessment should be performed.

Once it is confirmed that technologies, competencies, and resources are available to support a thorough remote assessment, the assessor and entity will need to agree on the appropriate use of the technologies before the remote assessment can commence. This includes:

- Agreeing on the remote access tools, protocols, devices, and software to be used to conduct the assessment.
- Agreeing on the security protocols to be followed before, during, and after the assessment process, including secure access to the entity's environment, secure methods for the access, collection, storage, and deletion of data, and protections for personnel security and privacy.
- Holding practice sessions for access and assessment methods to resolve any technical issues.
- Defining contingency plans in the event of a technology failure—for example, whether alternative technologies are available.

## 2.5 Data Confidentiality and Security Requirements

Remote assessments have additional considerations related to the confidentiality and security of the assessment process and the integrity and protection of the associated information and data. Some of these considerations include:

- Identification of any business, legal, and regulatory requirements that could affect how the remote assessment is conducted—for example, restrictions on the use of video and audio recordings and capturing images of personnel.
- Securing remote connections and transmissions of images and data. The mechanisms for sharing documentation and other information should be managed using secure systems and protocols—for example, using a secure portal that requires multi-factor authentication and strong cryptography to protect the transmission.
- Securing and controlling all logical access to systems and data. Assessors should not request or attempt to access systems or data beyond that which has been identified for the scope of the assessment. Remote access to the entity's systems and data should be provided only when needed to complete the relevant assessment activities. Upon completion of the assessment, the entity should remove or disable the assessor's access to systems and data repositories that were used to share information during the assessment.
- Defining security and retention requirements for the collection and storage of documentation, data, and other digital evidence. Assessors should retain data only as required for their work papers as agreed to by the entity.

- Responding to potential security incidents. If a security incident is suspected or confirmed while the remote assessment is underway, the assessor and entity should review the situation and agree on next steps and actions to be taken, including whether to halt, reschedule, or continue with the assessment.

As part of the assessment planning process, the assessor and entity should agree on the methods, controls, and protections that will be followed throughout the assessment to ensure that confidentiality, security, and integrity requirements are maintained. These methods should be communicated to and acknowledged by all persons participating in the assessment. The assessor and entity should each aim to ensure the methods are effectively implemented and followed by their participants at all times during the assessment.

There may be a greater likelihood that data not relevant to the assessment is captured when the assessment is using video and other recordings. Care should be taken to avoid collection of information or data that is outside of the assessment scope. Where out-of-scope information or data is provided together with in-scope information, the security and data protections required for the out-of-scope information should be determined.

Assessors and entities should take all necessary steps to ensure that payment card account data is not inadvertently included in the evidence being retained. Procedures for dealing with the accidental capture of account data—for example, communication to affected entities and secure deletion methods—should be defined and agreed to during the planning phase.

### *2.5.1 Recordings and Screenshots*

The use of recordings and screenshots should be clearly defined and agreed upon in advance and adhered to throughout the assessment. General principles to be followed include:

- No video or audio recording of entity personnel should take place without the express permission of the entity and the individual.
- Personal interactions that are not relevant to the assessment should not be recorded or documented.
- Recording of any other transmissions—for example, data or images that are shared using screen-sharing tools—should be previously agreed to by the entity.
- Screenshots of personnel during video calls should not be taken without the express permission of the entity and the individual.
- Screenshots or photo captures of documents, live data, or other evidence should be previously agreed to by the entity.
- Recordings and screenshots of assessors by entity personnel should not take place without the permission of the assessor.

Assessors and entities should be aware of any legal or regulatory requirements that apply to the capture of personal data.

## 2.6 Verifying Information Received During Remote Assessments

Assessors should take practical steps to determine whether the information collected during the assessment provides sufficient objective evidence to demonstrate that a requirement has been met, including whether the information is:[4]

- Complete (all expected content is contained in the documented information).
- Correct (the content conforms to other reliable sources).
- Consistent (the documented information is consistent within itself and with related documents).
- Current (the content is up to date).

The assessor should have a high degree of confidence that the information relied on to reach a finding meets these four criteria. Where evidence or data is provided in a way that varies from the approach previously agreed—for example, generated on a different system or by different personnel—additional verification of the integrity of the evidence may need to be considered.

## 2.7 Determining Assessment Results

The assessor is ultimately responsible for determining whether the remote testing has provided the level of reliability and assurance needed to document a finding. Assessors should use sound professional judgment and an unbiased evaluation of the effectiveness of the remote testing methods used, including how the use of such methods could have affected the integrity and reliability of the assessment result. Considerations for determining the assessor's level of assurance in the testing results include:

- How the remote testing differed from onsite testing, and how those differences affected the reliability and assurance achieved during the testing.
- The effectiveness of controls used to verify the accuracy and integrity of the evidence received.
- The effectiveness of any additional testing and/or collection of additional evidence that was performed to address reliability and assurance gaps.

When evaluating the level of assurance provided by a particular testing result, assessors should consider all aspects of the test that was performed, including the specific scenario being tested and the testing methods used. The cumulative effect that the remote testing has on assurance for different requirements and for the assessment overall also needs to be considered. An assessor should be confident that their findings are defendable and supported by objective evidence, and that a group of their peers would have reached the same finding, before documenting the finding in a ROC or ROV.

Examples of testing results with resultant level of assurance and impact on assessment findings is shown in Table 3.

[4] ISO 19011:2018(E) Guidelines for auditing management systems

**Table 3. Example Descriptions of Testing Results with Corresponding Assurance and Assessment Findings**

| Example Descriptions of Testing Results and Resultant Level of Assurance | | Impact on Assessment Findings |
|---|---|---|
| **High** | The testing results and evidence received confirm all the entity's assertions about the implemented controls, the testing was able to be completed in full, and the testing and evidence fully cover the scope of the environment and the implemented controls. The assessor has a high degree of assurance in the evidence received and testing results and is highly confident in attesting to a finding for the requirement. | The assessor can determine a finding for the requirement |
| **Medium** | The testing results and evidence received indicate that the implemented controls meet some aspects of the requirement, or that the requirement is implemented for some components. However, there are irregularities within the testing results or the evidence, or full testing could not be completed, or the testing and evidence do not fully cover the scope of the implemented controls. The assessor does not have a sufficiently high level of confidence to attest to a finding for the requirement. | The assessor cannot determine a finding for the requirement and the assessment is considered incomplete |
| **Low** | The testing results and evidence received are not sufficient for the assessor to form an opinion about whether the requirement has been met. The assessor cannot with any confidence determine a finding for the requirement. | |

Findings should be recorded in a ROC or ROV only when the assessor has a high degree of confidence in the coverage and scope of testing performed, the reliability and accuracy of the testing results and the evidence received, and that the level of assurance achieved is equivalent with performing the assessment onsite.

If the assessor does not have a high level of confidence and assurance in the initial testing results, they should work with the entity to determine if additional testing could be performed that could further support the assessor's ability to reach a finding.

If after the completion of all feasible testing the assessor cannot with confidence reach a finding, they must document in the ROC or ROV that testing for that requirement could not be completed. Requirements for which testing cannot be completed are considered incomplete and non-compliant. Details for how to report incomplete findings is provided in *Appendix A, Addendum for ROC/ROV: Remote Assessments*.

## 2.8 Consideration for Previous Assessment Results

Assessors that have previously completed an onsite assessment of an entity's location might be inclined to rely on the information gathered during the onsite assessment as supporting evidence for a current remote assessment. However, environments, technologies, people, and processes are constantly changing, and it should never be assumed that characteristics that were present during a prior assessment are still in place today.

There may also be scenarios where extraordinary circumstances have resulted in significant changes to an entity's environment since its last assessment. For example, an entity could have completely rearchitected their technologies and processes to migrate from an onsite work environment to a remote working model. In this scenario, the assessor would not be able to rely on previous assessment findings, as the current environment would be substantially different than what was previously assessed.

Conversely, there may be scenarios where the assessor can use their findings from a previous onsite assessment as part of a current remote assessment. For example, where a testing procedure requires observation of a physical environment characteristic that remains constant over a long period of time, such as the thickness and structure of a building wall. In cases where the assessor has previously verified the building's wall structure during an onsite assessment, the assessor may determine that additional testing—such as interviews and data evidence that confirm the structure has not changed since the onsite assessment—contributes to their level of assurance that the requirement is still being met.

Where the assessor has previously performed an onsite assessment at a particular location, it is critical that the assessor carefully consider any preconceptions they have from the previous assessment. An assessor with preconceptions of an entity's compliance, either positive or negative, due to a previous assessment finding, could be lacking objectivity and produce an assessment result that does not represent the entity's current environment. Assessors should take the necessary steps to ensure that any preconceptions do not compromise their objectivity during the assessment.

# 3 Use of Remote Testing Methods

## 3.1 Remote Testing Methods

Table 4 identifies common methods that can support remote assessment activities. Each method is considered for potential use as a synchronous or asynchronous method.

- "Synchronous" describes activities involving simultaneous interaction between the assessor and the entity.
- "Asynchronous" describes activities performed independently by the assessor without simultaneous interaction with the entity.

**Table 4. Remote Testing Methods[5]**

| Remote Testing Method | Potential Use | Examples | Logistical Considerations |
|---|---|---|---|
| **Documentation review (synchronous)** | Guided review of documentation provided by entity personnel through online collaboration tool. Often combined with video call. | Entity personnel uses screen sharing to navigate assessor to an internal document, system, or file. | • Scheduling and time zone challenges.<br>• Potential delays in responding to documentation requests.<br>• Entity personnel controls what the assessor can view.<br>• Potentially time-consuming due to interviewee interaction.<br>• Reliance on entity personnel access permissions and ability to navigate to the defined documentation. |
| **Documentation review (asynchronous)** | Assessor review of documentation without active participation of entity personnel. | Assessor downloads or navigates to online repository to review documentation placed there by the entity. | • Potentially time-consuming for entity to set up document repository for remote access and for assessor navigating to relevant files.<br>• Entity personnel controls what the assessor can view.<br>• Lack of interaction with entity personnel inhibits ability to clarify information during document review. |

[5] Adapted from ISO 9001 Auditing Practices Group Guidance on Remote Audits

| Remote Testing Method | Potential Use | Examples | Logistical Considerations |
|---|---|---|---|
| **Audio/Video call (synchronous)** | Interviewing entity personnel in real time with assessor and interviewee in different locations. | Assessor and entity personnel communicate by telephone or use online collaboration or video meeting tools to conduct live interviews. | • Scheduling and time zone challenges.<br>• Authentication of interviewee identification.<br>• Low quality of communication interfering with audio or visual transmission.<br>• The ability to observe reactions from interviewees may be reduced. |
| **Data review (synchronous)** | Guided review of data or other evidence provided by entity personnel through online collaboration tool. Often combined with video call. | Entity personnel uses screen sharing to allow assessor to observe data being generated or function or process being performed on a system. | • Scheduling and time zone challenges.<br>• Delays in responding to requests to view data on a particular system.<br>• Entity personnel controls what the assessor can view.<br>• Potentially time-consuming due to interviewee interaction.<br>• Reliance on entity personnel access permissions and ability to navigate to the defined systems and data. |
| **Data review (asynchronous)** | Assessor review of data or other evidence without active participation of entity personnel. | Assessor downloads or navigates to online repository to review data placed there by the entity. | • Potentially time-consuming for entity to set up document repository for remote access and for assessor navigating to relevant files.<br>• Entity personnel controls what the assessor can view.<br>• Lack of interaction with entity personnel inhibits ability to clarify information during data review.<br>• Reduced visibility into how data was generated. |
| **Video (synchronous)** | Guided site tour, witnessing the performance of tasks or processes as they occur, observing physical and structural characteristics of the environment as they are now. | Entity uses portable device to transmit a live video stream that the assessor views in real time. May also include live streaming of process simulations performed outside of the location where process usually occurs. | • Scheduling and time zone challenges.<br>• Entity personnel control what the assessor sees.<br>• Reduced ability for assessor to receive a full appreciation of the environment or process being observed.<br>• Use of portable equipment or live transmissions may not be possible in all areas.<br>• Potential for manipulation of data. |

| Remote Testing Method | Potential Use | Examples | Logistical Considerations |
|---|---|---|---|
| **Video (asynchronous)** | Observing a task or process that had been previously performed, or physical and structural characteristics that were previously captured or recorded. | Entity provides excerpts from surveillance footage or recordings of activities that have already been performed for the assessor to review. | • Entity personnel control what the assessor sees.<br>• Reduced ability for assessor to receive a full appreciation of the environment or process being observed.<br>• Use of recording equipment may not be possible in all areas.<br>• Activities and events not observed in real time.<br>• Potential inaccuracies in date/time stamps of recorded video.<br>• Potential for manipulation of data. |

## 3.2 Applying Remote Testing Methods to PCI SSC Testing Activities

Each PCI SSC standard specifies the testing activities that assessors are expected to perform when determining whether a requirement has been met. These testing activities may be referred to in different standards as “testing procedures”, “test procedures”, “test requirements” or “validation methods”. For the purposes of this document, the term “testing activity” encompasses all testing methods defined in PCI SSC standards, irrespective of the terminology used within each standard.

Table 5. Summary of Remote Testing Methods for Use with PCI SSC Testing ActivitiesTable 5 identifies testing activities that are common across PCI SSC standards, some examples of each, and the remote testing methods that can be considered for each testing activity.

Table 5 also defines a baseline hierarchy for the use of remote testing methods as alternatives to onsite testing.

## Table 5. Summary of Remote Testing Methods for Use with PCI SSC Testing Activities

| PCI SSC Testing Activity | Example | Remote Testing Methods[6] | Baseline for Determining Use of Remote Testing Methods as Alternatives to Onsite Testing |
|---|---|---|---|
| **Examine documentation** | Reviewing materials such as policies and procedures, vendor documentation, training materials, and implementation manuals. Documentation may be electronic or physical (paper). | • Documentation review (synchronous)<br>• Documentation review (asynchronous) | • When performed properly, either method provides an acceptable alternative to onsite testing.<br>• A combination of methods can also be used—for example, guided remote navigation to the document location, with documentation then provided to assessor for offline review. |
| **Interview personnel** | Conversing with participants to determine understanding of the entity's policies and procedures, describe how an activity is performed, or confirm personnel knowledge of a security principle. | • Audio/Video call (synchronous) | • When performed properly, this method provides an acceptable alternative to onsite testing. |
| **Examine/observe live data** | Inspecting network, system, or software configuration settings, audit logs, change control records, source code, testing results, access controls, and system process outputs. | • Data review (synchronous)<br>• Data review (asynchronous) | • Onsite observation should be performed where feasible.<br>• If onsite observation is not feasible, synchronous data review should be considered.<br>• If neither onsite observation nor synchronous data review are feasible, asynchronous data review with additional steps to ensure the origin and integrity of data sources may be considered. |
| **Observe process being performed** | Watching personnel or systems perform activities and functions in real time, such as authentication procedures, system administration tasks, response procedures, software updates, and key-management procedures. Observation may be of a "live" process or, if the process can only be performed under specific conditions that are not present during the assessment, a demonstration of the process (process simulation). | • Video (synchronous)<br>• Video (asynchronous) | • Onsite observation should be performed wherever feasible.<br>• If onsite observation is not feasible, synchronous video observation should be considered.<br>• If neither onsite observation nor synchronous video observation are feasible, asynchronous video observation with additional steps to ensure the origin and integrity of video data, as well as additional detailed interviews and supporting evidence that confirm all steps of the process may be considered. |

[6] As described in Table 4.

| PCI SSC Testing Activity | Example | Remote Testing Methods[6] | Baseline for Determining Use of Remote Testing Methods as Alternatives to Onsite Testing |
|---|---|---|---|
| **Observe physical environment** | Viewing physical aspects of a location in real time, such as structural aspects of a building, placement of devices within a facility, layout of a secure room, and personnel interacting with physical security controls. | • Video (synchronous)<br>• Video (asynchronous) | • Onsite observation should be performed wherever feasible.<br>• If onsite observation is not feasible, synchronous video observation should be considered.<br>• If neither onsite observation nor synchronous video observation are feasible, asynchronous video observation with additional steps to ensure the origin and integrity of video data, as well as additional detailed interviews and supporting evidence that confirms all required aspects of the physical environment may be considered. |
| **Perform Interactive testing** | Performing hands-on testing activities on an entity-provided asset (for example, hardware or software), such as installing and configuring software in accordance with defined instructions, performing test transactions and evaluating the output, and using forensic tools or methods on a sample implementation. This activity also encompasses the use of security-testing tools and techniques—for example, to conduct a penetration test or to perform static or dynamic analyses on a piece of software. | • Combined video (synchronous) and data review (synchronous) | • Onsite or offsite[7] testing should be performed wherever feasible.<br>• If neither onsite nor offsite testing are feasible, testing by combined synchronous video and data review, with additional interviews and supporting evidence that confirm the integrity and accuracy of the testing process and testing results, may be considered. |

[7] Offsite testing is where the assets and data being tested are sent to an assessor-controlled testing environment or lab.

## 3.3 Detailed Guidelines for the Use of Remote Testing Methods

This section defines further detail around the use of remote testing methods for each type of PCI SSC testing activity. The following information has been defined for each type of testing activity:

- An initial risk ranking associated with performing the testing activity remotely compared to onsite testing. This ranking considers the potential impact to evidence reliability and level of assurance when the testing activity is performed using remote methods. The ranking is intended as guidance, to identify where additional effort and testing may be needed to complete the testing activity and achieve sufficient assurance.
- The remote testing methods (as defined in Table 4) that can be used for this testing activity as alternatives to onsite testing.
- Factors affecting evidence reliability and assessment assurance when a testing activity is performed remotely.
- Examples of additional testing activities to help mitigate reliability/assurance gaps.
- Potential scenarios where remote testing might not be feasible.
- Additional guidelines and best practices for effective use of the remote testing methods.

### *3.3.1 Examining Documentation*

| Examining Documentation | |
|---|---|
| Potential risk to evidence reliability and assessment assurance when performing the testing activity remotely: | • Low |
| Remote testing methods as alternative to onsite testing: | • Documentation review (synchronous)<br>• Documentation review (asynchronous) |
| Factors affecting evidence reliability and assurance when testing is performed remotely: | • Reduced assurance that personnel are aware of the documentation, its location and how to access.<br>• Reduced assurance that documentation was not modified while being prepared to send to assessor. |
| Examples of additional testing activities that may help to mitigate risks to reliability and assurance: | • Additional interviews and/or remote observation to confirm location of documentation, personnel knowledge and awareness, and integrity of documentation provided. |
| Scenarios where remote testing might not be feasible: | • Remote examination of documentation containing confidential or proprietary information may not be possible where such access would violate the entity's security policies or protocols—for example, where such data is not permitted to leave the entity's premises. In such cases, the assessor may need to be onsite at the entity's designated location to review the documentation in accordance with the entity's security requirements. |

| Examining Documentation |
|---|
| Additional Guidelines and Best Practices: |
| All documentation should be shared by a secure method that is protected with strong cryptography, such as a secure portal or encrypted transmission channel. Examining documentation file storage information, document properties, or other metadata may help confirm that creation and modification dates are consistent with the entity's defined process for keeping documentation up to date. |

### *3.3.2 Interviewing Personnel*

| Interviewing Personnel | |
|---|---|
| Potential risk to evidence reliability and assessment assurance when performing the testing activity remotely: | • Low – Medium |
| Remote testing methods as alternative to onsite testing: | • Audio/Video call (synchronous) |
| Factors affecting evidence reliability and assurance when testing is performed remotely: | • Missed visual cues from interviewees that could indicate uncertainty or an incomplete response.<br>• Reduced ability to integrate interviews with guided walkthrough of processes or facility.<br>• Heavy reliance on the quality of the video/audio transmission, availability of required entity and assessor personnel, and the assessor's interpersonal and interviewing skills. |
| Examples of additional testing activities that may help to mitigate risks to reliability and assurance: | • Additional and more in-depth interviews, including follow-up questions to confirm interviewee statements. |
| Scenarios where remote testing might not be feasible: | • Remote interviews can take place only if entity personnel have access to a reliable audio or video connection. If a connection is not available, alternative and/or additional testing may be needed. |
| Additional Guidelines and Best Practices: | |
| Interviews are an essential means of collecting information and typically play a significant part in an assessment. Barring technical difficulties, a remote interview should not take more time than an onsite interview; however, the assessor may need more time to prepare for interviews when they are conducted remotely.<br><br>Interview areas should be comfortable, safe environments that allow the interview to be conducted without interruption. Setting the right atmosphere encourages the interviewee to speak openly and frankly and helps all participants to remain attentive for the duration of the interview. | |

## Interviewing Personnel

To facilitate interview effectiveness, protocols and procedures defining how the interviews will be conducted should be communicated for all participants to follow. Protocols should include mechanisms that allow for open discussions and avoid situations where individuals are inadvertently talking over one another.

The purpose and objectives of an interview should be clearly defined and communicated. Assessors should attend interviews with questions and discussion points prepared in advance, and actively observe interviewees throughout the interview to ensure all participants are engaged.

Interview participants should be provided sufficient notice of interview schedules, and all participants should confirm that they are able to attend. Interview times, including breaks, should be scheduled such that participants are not required to attend hours-long draining sessions or be present at interviews that are not relevant to their job function.

Time zone differences should be considered. Interviews should be conducted during normal working hours whenever possible.

Video cameras should be set so the assessor can clearly see all interview participants, confirm which individual is responding, and engage in active communication. Where practical, keep microphones on to encourage open conversation. If background noise is affecting audio quality, consider moving the participant to a more suitable location.

Reasonable and reliable methods for confirming the identity of personnel being interviewed should be defined. Verifying interviewee identity allows the assessor to confirm the role of the individual they are talking to and whether the individual is the appropriate person to discuss the control or process being assessed.

The assessor should clearly communicate how and what notes will be taken during the interview.

Interviewee privacy should be respected at all times. This includes muting microphones and pausing cameras during scheduled breaks.

Considerations for recording of interviews include:

- The approach toward recording interviews should be the same as if the interview were being conducted onsite. If an onsite interview would be documented through the assessor's notes instead of being recorded, there is no reason for the interview to be recorded when it is performed remotely.
- Any recording of interviews should be in accordance with the approach agreed to by the assessor and entity during the assessment planning phase. All parties should be made aware about whether any recording will take place during the interview.
- If the interview is recorded, the recording should be protected to the same level of security as the information being conveyed during the interview.

### 3.3.3 Examining/Observing Live Data

| Examining/Observing Live Data | |
|---|---|
| Potential risk to evidence reliability and assessment assurance when performing the testing activity remotely: | • Medium |
| Remote testing methods as alternative to onsite testing: | • Data review (synchronous)<br>• Data review (asynchronous) |
| Factors affecting evidence reliability and assurance when testing is performed remotely: | • Reduced ability to confirm origin of evidence–for example, which system generated the evidence and when it was generated.<br>• Reduced ability to confirm how the evidence was generated and by whom (for example, that correct access controls were in place).<br>• Heavy reliance on the assessor's ability to achieve a detailed understanding of the environment and clearly define what they need to view on which systems. |
| Examples of additional testing activities that may help to mitigate risks to reliability and assurance: | • Remote observation of evidence being generated to confirm source.<br>• Additional interviews to confirm who, what, where, when, and how the evidence was generated.<br>• Increased sample size and/or collection of additional evidence that confirms how the evidence was generated. |
| Scenarios where remote testing might not be feasible: | • Remote examination of data evidence that contains confidential or proprietary information may not be possible where such access would violate the entity's security policies or protocols—for example, where such data is not permitted to leave the entity's premises. In such cases, the assessor may need to be onsite at the entity's designated location to review the data in accordance with the entity's security requirements. |

Additional Guidelines and Best Practices:

Assessors should aim to have a thorough understanding of the entity's people, processes, and technologies prior to initiating synchronous data reviews. The use of asynchronous reviews and interviews prior to the commencement of a synchronous review may help to facilitate the synchronous review process.

The specific data and system components to be reviewed should be identified in advance whenever possible, and clearly communicated at the start of the review. Where sampling is used, assessors should always select the data and system components to be included in the sample.

When using synchronous review methods, assessors should actively direct entity personnel to navigate to the systems and data that have been identified by the assessor for review.

Entity personnel who are facilitating the synchronous review should be confirmed as possessing the access permissions necessary for the systems and data to be accessed. Personnel should be provided sufficient notice of the review schedule to ensure that the requisite personnel are available.

| Examining/Observing Live Data |
|---|
| Reasonable and reliable methods should be in place for confirming the system or source of the data being observed. Synchronous reviews should allow the assessor to begin observation prior to the entity personnel accessing the target data or system, so the assessor can be sure which system or data store they are observing and how it is being accessed.<br><br>The capture of screenshot images and recordings should be in accordance with the approach agreed to by the assessor and entity during the assessment planning phase. The assessor should identify how and what screenshots or recordings will be taken during the review. All screenshots and recordings should be protected to the same level of security as the information being captured.<br><br>Live data associated with high security areas should be reviewed synchronously and not be recorded or distributed outside of the assessed entity.<br><br>While data is being observed or captured, entity personnel should take care not to disclose any sensitive information on their screens that is not relevant to the assessment—for example, proprietary or other confidential data. |

### *3.3.4 Observing Processes*

| Observing Processes | |
|---|---|
| Potential risk to evidence reliability and assessment assurance when performing the testing activity remotely: | • High |
| Remote testing methods as alternative to onsite testing: | • Video (synchronous)<br>• Video (asynchronous) |
| Factors affecting evidence reliability and assurance when testing is performed remotely: | • Missed visual cues from being unable to view the entire environment, resulting in incomplete observation.<br>• Reduced visibility of personnel interaction with environment.<br>• May not be possible to witness some operations “live” as they occur. |
| Examples of additional testing activities that may help to mitigate risks to reliability and assurance: | Additional interviews and collection of additional data and evidence to support observation. For example,<br>• More in-depth interviews and simulated demonstrations of the process, including detailed walkthroughs and descriptions of each step of the process.<br>• Additional evidence that verifies the steps performed, how the process was completed, the outcome of the process, and all inputs, outputs, and interactions during the process.<br>• Additional evidence that verifies the functions performed by a physical control, including the inputs, outputs, and interactions associated with the control. |

| Observing Processes | |
|---|---|
| Scenarios where remote testing might not be feasible: | • Remote observation of locations where sensitive processes are performed may not be possible where such access would violate the entity's security policies or protocols. Where remote observation of a sensitive process does not conform to an entity's security policy, the process must be observed onsite, and the assessment considered incomplete until the onsite observation is performed. |

Additional Guidelines and Best Practices:

Testing that requires observations of processes is among the most challenging to complete remotely. A thorough understanding of the process or activity being observed is critical for assessors to gain assurance from remote observations. Being onsite and actively observing a process in action may be the only way for an assessor to make an accurate determination about whether the process meets the applicable requirements.

When relying on video for observation, consideration is needed for whether the images being observed are real-time (synchronous) or pre-recorded (asynchronous). A pre-recording may provide "one-off" evidence that a process or activity is being conducted in a certain way. However, pre-recordings do not provide a means for the assessor to interact with personnel or ask questions during the process, which may prevent the assessor from gaining a sufficient level of understanding about what is being observed.

Planning for remote video observations should include discussion and agreement between the entity and assessor about which processes are to be observed at which locations. Both parties should also agree that the assessor is leading the virtual observation and will be directing cameras and questioning personnel throughout to replicate the experience of an in-person observation.

During the video observation, the assessor should take charge of what the camera is looking at, guiding entity personnel on where to point the camera throughout the process enactment. In this role, entity personnel are serving as the "remote eyes" of the assessor. The objective is to allow the assessor to direct the video to capture all aspects of the process and surrounding environment that they would be able to see if they were physically onsite at the location. This includes covering areas that would normally be seen in the assessor's peripheral vision, directing the camera to pan from side to side as well as forward, and focusing on areas that the assessor would be examining if they were onsite.

Remote observation of a process or activity should be accompanied by in-depth and detailed verbal walkthroughs of each step of the process activity as it is performed. Additional data evidence (such as photos, logs, and records of process output) may also be required to attain assurance.

If synchronous video (live streaming) is not feasible—for example, due to a lack of network connectivity at the facility—the assessor may consider whether pre-recorded, or asynchronous, video would be able to provide the requisite information. Where entity personnel will be video recording a process asynchronously, the assessor should provide clear instructions on where the camera needs to be pointed to view all process steps as they occur, as well as any environmental aspects that could interact with or affect how a process step is performed.

For pre-recorded video footage, mechanisms should be in place that verify the date and time the recording was made, as well as the location where the footage was taken. The mechanisms used should provide assurance that the footage is current, has not been altered, and was taken at the date, time, and location requested. Video metadata containing date/time stamps and GPS coordinates can assist with verification if the integrity of the metadata can be confirmed.

**Observing Processes**

Whether synchronous or asynchronous, the assessor should ensure that the images being captured cover all applicable aspects of process, and not rely on entity personnel to select which aspects are included. The resultant observation should provide the same level of visibility and perspective that the assessor would have gained had they had been onsite at the location.

Assessors should also be prepared for the possibility of "unknown unknowns,"[8] both within the process or at the location where the process is performed, which may not be immediately apparent during a remote observation. Additional evidence and interviews with entity personnel will likely be required for the assessor to attain sufficient understanding of all aspects of the process and fill in any gaps that could not be seen during a remote observation.

During observations of sensitive processes and of processes in sensitive areas, entity and assessor personnel should ensure that confidential information is not disclosed unnecessarily—for example, the assessor should not be able to determine what passcode was entered on a keypad, or view confidential data that is not relevant to the assessment.

All recordings should be protected to the same level of security as the processes and information captured in the recording.

***Process Simulations***

Some areas—such as a key-loading room or other designated high security area—are highly sensitive and may have physical and logical security restrictions that prevent the use of video and photo capture. These restrictions may render it infeasible to remotely observe certain processes in the "live" environment—for example, processes for generating and loading cryptographic keys, or the performance of HSM administration functions. Additional considerations for assessing high security areas are provided in Section *3.4*.

In circumstances where it is not possible to remotely observe a process taking place in the live environment, it might be feasible for demonstrations of the process to take place in a simulated environment in a manner that produces a detailed, structured walk-through of the process. Process simulations should be supported by detailed discussions and verbal walkthroughs of each process step, as well as process documentation and data evidence resulting from the process. The assessor will need to make a judgment on whether a remote observation of a process simulation supported by additional data evidence is sufficient to reach a finding.

If process simulations are being considered, details of how and where the process will be simulated will need to be examined. Any deviation in the simulation from the original process or activity should be identified, documented, and considered for impact on the resulting assurance. The assessor will therefore need to be familiar with the steps and objectives of the process being simulated. Without detailed understanding and planning, the simulation will likely not produce a sufficient level of assurance in the result.

[8] ISACA: General guidance on IT Audit Technology Risk: Knowns and Unknowns

### 3.3.5 Observing Physical Environment

| Observing Physical Environment | |
|---|---|
| Potential risk to evidence reliability and assessment assurance when performing the testing activity remotely: | • High |
| Remote testing methods as alternative to onsite testing: | • Video (synchronous)<br>• Video (asynchronous) |
| Factors affecting evidence reliability and assurance when testing is performed remotely: | • Missed visual cues from being unable to view the entire environment, resulting in incomplete observation.<br>• Reduced visibility of personnel interaction with environment.<br>• May not be possible to witness some operations "live" as they occur. |
| Examples of additional testing activities that may help to mitigate risks to reliability and assurance: | Additional interviews and collection of additional data and evidence to support observation. For example,<br>• More in-depth interviews and simulated demonstrations of the physical control or environmental characteristic.<br>• Additional evidence that verifies the details of a physical control or environmental characteristic. |
| Scenarios where remote testing might not be feasible: | • Remote observations of a physical environment may not be possible where such access would violate the entity's security policies or protocols. Where remote observation of an environment does not conform to an entity's security policy, the environment will need to be observed onsite and the assessment considered incomplete until the onsite observation is performed. |
| Additional Guidelines and Best Practices: | |

Testing that requires observations of physical security controls and environmental characteristics is among the most challenging to complete remotely. A thorough understanding of the physical control or environment being observed is critical for assessors to be able to gain assurance from remote observations. Being onsite and actively observing the physical space and how people interact with it may be the only way for an assessor to make an accurate determination about whether the applicable requirements are met.

When relying on video for observation, consideration is needed for whether the images being observed are real time (synchronous) or pre-recorded (asynchronous). A pre-recording may provide "one-off" evidence that an environmental characteristic is present or a physical control is being used in a certain way. However, pre-recordings do not provide a means for the assessor to interact with the environment and could prevent the assessor from gaining a sufficient level of understanding about what is being observed.

Planning for remote video observations should include discussion and agreement between the entity and assessor about which areas are to be observed. Both parties should also agree that the assessor is leading the virtual walkthrough and will be directing cameras and questioning personnel throughout to replicate the experience of an in-person walkthrough.

## Observing Physical Environment

During the video walkthrough, the assessor should take charge of what the camera is pointing toward, guiding entity personnel on where to walk and where to point the camera. In this role, entity personnel are serving as the "remote eyes" of the assessor. The objective is to allow the assessor to direct the video to capture all aspects of the environment that they would be able to see if they were physically onsite at the location. This includes covering areas that would normally be seen in the assessor's peripheral vision, directing the camera to pan from side to side as well as forward, and focusing on areas that the assessor would be examining if they were onsite.

If synchronous video (live streaming) is not feasible—for example, due to a lack of network connectivity at the facility—the assessor may consider whether pre-recorded, or asynchronous, video would be able to provide the requisite information. Where entity personnel will be video recording the environment asynchronously, the assessor should map out the paths to be walked for each area and provide clear instructions on where the camera needs to be pointed to view the area as a whole and any specific aspects that the assessor needs to focus on.

For pre-recorded video footage, mechanisms should be in place that verify the date and time the recording was made, as well as the location where the footage was taken. The mechanisms used should provide assurance that the footage is current, has not been altered, and was taken at the date, time, and location requested. Video metadata containing date/time stamps and GPS coordinates can assist with verification if the integrity of the metadata can be confirmed.

It is critical that the areas to be included in the walkthrough are fully understood and agreed upon by both the entity and the assessor. Once there is agreement on the specific areas to be observed, any deviation from these areas could result in an incomplete assessment. If the entity refuses to follow the assessor's direction or attempts to obfuscate the assessor's view, this could indicate the presence of a characteristic or activity that, if viewed by the assessor, would negatively impact the assessor's findings.

Whether synchronous or asynchronous, the assessor should ensure that the captured images cover all applicable aspects of the environment being observed, and not rely on entity personnel to select which aspects are included. The resultant observation should provide the same level of visibility and perspective that the assessor would have gained had they had been onsite at the location.

During observations of sensitive areas, entity and assessor personnel should ensure that confidential information is not disclosed unnecessarily—for example, the assessor should not be able to determine what passcode was entered on a keypad, or view confidential data that is not relevant to the assessment.

Some areas—such as a key-loading room or other designated high security area—are highly sensitive and may have physical and logical security restrictions that prevent the use of video and photo capture. These restrictions may render it infeasible to remotely observe certain environments in any capacity. Additional considerations for assessing high security areas are provided in Section *3.4*.

### 3.3.6 Performing Interactive Testing

| Performing Interactive Testing | |
|---|---|
| Potential risk to evidence reliability and assessment assurance when performing the testing activity remotely: | • Medium – High |
| Remote testing methods as alternative to onsite testing: | • Combined video (synchronous) and data review (synchronous) |
| Factors affecting evidence reliability and assurance when testing is performed remotely: | • Reduced visibility over interactions between the asset being tested and the test environment.<br>• Reduced ability to confirm origin of evidence–for example, which system generated the evidence and when it was generated.<br>• Reduced ability to confirm how the evidence was generated and by whom (for example, that correct access controls were in place).<br>• Some assets might not be accessible for testing with remote methods. |
| Examples of additional testing activities that may help to mitigate risks to reliability and assurance: | • Remote instruction and observation of each step of the testing with detailed walkthroughs of each step performed and observation of the resulting evidence as it is generated.<br>• Additional interviews and collection of additional evidence to confirm who, what, where, when, and how the test was performed, and the results generated.<br>• Additional evidence to confirm the test platform/environment. |
| Scenarios where remote testing might not be feasible: | • Performing interactive testing with remote methods may not be possible where such access would violate the entity's security policies or protocols—for example, where access to the asset or data being tested is not permitted outside of the entity's premises. In such cases, the assessor may need to be onsite at the entity's location to complete the interactive testing and determine a finding. |
| Additional Guidelines and Best Practices: | |
| While other testing activities require assessors to examine artifacts, interview people, or observe environments and processes, interactive testing requires assessors to actively interact with and perform actions on the entity's assets. Depending on the type of test and sensitivity of the data or asset being tested, interactive testing is often performed either onsite at the entity's location or offsite at an assessor-controlled location, such as within a designated testing environment or laboratory.<br>Where the environment used for testing is not under the assessor's control—for example, testing takes place within the entity's test environment—additional preparation and walkthroughs of the test environment and systems, including operating system details, installation date, installed software, user permissions, services, programs, security settings, and so on, will be needed. The assessor will also need to ensure that the test environment reflects a real-world implementation and is sanitized such that the outcomes and results of testing are accurate and reliable. | |

## Performing Interactive Testing

Where the assets or data to be tested remain at the entity's location and onsite testing is not possible, the options for remote testing include:

- Approach 1: The assessor is granted an appropriate level of remote access to the entity's networks and systems that allows the assessor to directly interact with and conduct testing on the target systems or data.
- Approach 2: The assessor remotely observes and directs entity personnel to conduct each step of the testing on the assessor's behalf.

In the first approach, the assessor is provided with account credentials that provide access to the requisite systems and data as well as the privileges needed to perform the testing activities. In this option, the assessor has direct control over the keystrokes and commands that are transmitted to and entered into the test components within the entity's environment.

The second approach has all the risk and assurance considerations of the "examine/observe live data" and "observe processes" testing activities. Consequently, the best practices for using video (synchronous) and data review (synchronous) testing methods are also applicable for interactive testing.

Where testing is to be performed by entity personnel, additional considerations include:

- Both parties should agree that the assessor is leading the testing activity and will be directing entity personnel on what to do for each step, including questioning personnel throughout to replicate the experience of an onsite test.
- In this role, entity personnel are serving as the "remote hands" and "remote eyes" of the assessor, allowing the assessor to direct what actions are taken and what is observed. The objective is that the assessor controls each aspect of the testing activity as it occurs and can verify the results of each activity to the same level of assurance as if they were performing the test themselves.
- The synchronous observation should begin prior to the entity personnel accessing the data or asset being tested, so the assessor can be sure of what they are observing and how it is being accessed.
- Synchronous observation of an interactive testing activity often requires at least two concurrent views—for example, one view that shows the steps being performed by the entity personnel, and one that simultaneously shows the outcome of those steps on the asset/data being tested.
- Remote observation of an interactive testing activity should be accompanied by in-depth and detailed verbal walkthroughs of each step as it is performed. Additional data evidence (such as photos, logs, and records of output) may also need to be collected and correlated to attain assurance.
- Details of the type of account and associated access permissions used by entity personnel to perform the testing activity should be confirmed.
- Increased interviews and meetings should be scheduled to support communication needed for successful completion of testing.
- Where the testing requires installation of an application or software, details of the platform on which the installation will occur should be verified prior to the installation commencing.

Irrespective of the method used, all testing activities and samples are to be collected and tested per the assessor's instructions.

## 3.4 High Security Areas

Some environments may have tighter restrictions on the presence, storage, and use of portable electronic devices within particular zones or areas—for example, secure rooms for key-injection and areas designated as high security areas.

While the use of alternative remote testing methods—for example, process simulations—may be able to provide the assessor with sufficient assurance to reach a finding in some instances, the observation of processes, systems, or materials within these areas is often required. In such instances, portable electronic devices could provide a means to observe a process or environmental characteristic that cannot be replicated outside of the secure area.

Live streaming with recording disabled (synchronous video) is preferred over recording and asynchronous video review. Where live streaming is not possible—for example, due to lack of connectivity to the secure area—recording of the process for remote observation by the assessor should be facilitated. The recording should be stored only on the entity's system and streamed to the assessor for observation. Transfer of recorded material outside of the entity's systems presents a higher level of risk and should be avoided.

The use of portable electronic devices in secure areas requires in-depth consultation with the entity, including consideration for their security policies and risk appetite, as well as confirmation that such usage would not be in violation of applicable security requirements. Where the use of portable electronic devices does not conform to the entity's security policy, the secure area will need to be observed onsite and the assessment considered incomplete until the onsite observation is performed. The feasibility of remote observation for secure areas and processes should be discussed during the pre-planning process.

### *3.4.1 Guidance on the Use of Portable Electronic Devices*

A portable electronic device is described as any device, including personal computers, tablet devices, mobile telephones, smart watches, cameras, and any other device, that can connect to the internet, transmit frequency (such as traditional radio transmission, Bluetooth, Wi-Fi, or any other transmission protocol), or has a visual or audio recording and/or storage or GPS capability.

Policies and procedures governing the use of portable electronic devices during remote assessments should be agreed to by the entity and assessor.

The following controls should be considered whenever portable electronic devices are to be used.

- The use of a portable electronic device should be clearly defined and fit for purpose. Devices should have only the capability needed for the defined task, with all other functions disabled.
- The device should be assigned to, accounted for, and operated by a designated entity custodian. The custodian should have the appropriate security clearances for operation in the area within which the device will be used.
- Once the device has entered a secure area, it should be treated in a commensurate manner to the highest classification of assets processed or stored in that area.
- When not in use, the device and any removable storage should be stored outside of the secure area, in a manner commensurate with the highest classification of the information or asset processed or stored in the area—for example in an appropriate security container or in the custody of a designated custodian.

- The device should be inspected by a supervisor before introduction to the secure area. The inspection should include a check of the device serial number and removable storage memory, and a visual inspection for tampering or damage.
- The process, system, or material to be observed should be clearly identified. The immediate area should be sanitized, and other individuals in the secure zone warned of the remote observation so as not to expose other processes, information, or systems. This could include the cessation of other processes, or "close-up" recording of the process so as not to compromise other assets, information, or processes.
- The device should be active only for the minimum amount of time required to provide assurance. The device should be turned on, used to observe the process or asset, and then be turned off (as opposed to standby).
- The device should be configured to apply strong cryptography for the protection of all transmissions.

In addition to the above, if synchronous observation is not possible and the entity is capturing a recording for the assessor to observe at a later time:

- Where possible, the recording device should use removable storage memory (for example, memory card) that is accounted for and destroyed in a manner commensurate to the highest classification asset or level of information that it has accessed.
- Upon completion of the recording, it should be immediately transferred to a secure system in preparation for remote observation by the assessor.
- Following observation of the recording, the removable storage memory should be wiped. Once the assessment activity has been completed, the removable storage memory should be destroyed in an accountable manner that is commensurate to the highest classification information or asset processed or stored in the secure area(s) to which it was introduced. The device should be accounted for and stored for future use in remote assessments at that site and not used for any other purpose.
- In the event the device does not have a removable storage capability, it is preferable that the device be destroyed in the same manner as removable storage memory. If this is not possible, the memory should be securely wiped to ensure the recording cannot be recovered. The device should be accounted for, stored, and audited in a manner commensurate to the highest classification of information or asset processed or stored in the secure area(s) to which it was introduced.

# 4 Assessor Responsibilities

PCI SSC qualifies assessors to validate adherence to specific PCI SSC standards in accordance with applicable program requirements. In addition to requirements defined in Qualification Requirements and Program Guides, the following guidance applies to PCI SSC assessors when conducting remote assessment activities.

- Remote assessment activities are to be performed to the same rigor of quality and accuracy as onsite assessments. As much as possible, assessors should use testing methods and approaches that replicate an onsite assessment, such that the result of a remote assessment is commensurate with that which would have resulted from an onsite assessment. This includes:
  - Taking all necessary steps to ensure that the integrity of the assessment result is not negatively affected by the use of remote testing methods. For example, assessors should ensure that the personnel being interviewed and systems being examined are the same as if the assessor were onsite. Additional controls may also be needed when observing implementations and collecting evidence to confirm the source of evidence being viewed.
  - Maintaining control of all assessment activities. For example, where a live video stream is being used to show evidence or a physical location, it is for the assessor to determine where the video camera should point, not the person holding the camera. Similarly, the selection of system components, sites, and personnel for inclusion in the assessment should be chosen by the assessor, not the entity.
- Assessors should clearly document within the ROC or ROV why onsite testing was not performed, how the remote testing was performed, and to what extent the remote testing provided assurance in the finding. Refer to *Appendix A, Addendum for ROC/ROV: Remote Assessments* for details.
- A requirement can only be identified as "in place"[9] in a ROC or ROV if the testing performed produces the necessary assurance that the controls are properly implemented and the requirement has been met.
- The use of remote assessment activities and associated quality assurance (QA) requirements should be accounted for in the assessor company's QA Program and documented in their QA Manual.
- Assessors must not capture or retain highly sensitive evidence that would not have been captured if the assessor had been onsite. For example, video footage of sensitive processes or high security areas should be observed in real-time wherever possible, and any recordings be securely deleted immediately once the assessor has reviewed and verified the recording.
- During remote interviews and observations, assessors must ensure that their work environment prevents unauthorized observation of the video or material being observed.
- All relevant evidence should be retained as part of the assessor's workpapers. The assessor company's Workpaper Retention Policy and procedures should define what evidence is necessary to retain in workpapers and the required retention time, assign the appropriate security classification for protection of the data, and enforce a secure destruction method when retention period is reached.
- Policies and procedures for maintaining confidentiality and integrity of information gathered during the assessment must include consideration for the types of information collected from remote assessment activities.

[9] Or equivalent terminology as used to indicate that a requirement has been met

## 4.1 Sampling

The process for selecting samples for remote testing should be consistent with the rationale and criteria used for onsite testing. When selecting samples, assessors should always ensure that the chosen samples are representative of the entirety of the environment being assessed.

Where there are multiple similar locations included in the assessment and the assessor can successfully complete onsite assessments at a representative sample of locations, the proper use of remote testing methods can help facilitate assessment of the additional locations.

The availability of remote testing methods can also provide opportunities to expand the sample size if deemed necessary—for example, where additional assurance is needed to confirm that a particular requirement is being consistently met in different locations.

In all cases, the samples chosen should be selected by the assessor, not by the entity, and documented in the applicable ROC/ROV.

## 4.2 Competencies and Experience

An assessor's experience should be carefully evaluated before being assigned to a remote assessment. For example, it is recommended that experienced assessors who have performed multiple onsite assessments to the applicable standard be considered to lead a remote assessment.

As well as having a designated lead assessor, effective remote assessments will often use one or more assessors to provide support for the various testing activities. Newer assessors and those with less onsite assessment experience should be assigned a supporting role for one or more remote assessments before being assigned to lead an assessment. Assessors may also require additional direction on the use of remote assessment processes for their first two or three remote assessments.

In addition to the skills and competencies required for onsite assessments, assessors must be technically proficient in the technologies used for a remote assessment to ensure their secure and proper use. Assessor company personnel who support the assessment process—for example, personnel responsible for setting up and scheduling meetings over secure channels, or for configuring and communicating on the use of secure document repositories—must also be technically proficient and ensure the secure and proper use of the technologies.

## 4.3 Regional Considerations

The increased ability to assess over a larger geographic area using remote assessment techniques does not supersede Servicing Markets limitations. Assessors are required to honor the geographical limits of the Servicing Markets they are approved to assess.

## 4.4 Subcontracting to Qualified Assessors

For assessor programs that permit subcontracting,[10] assessor companies that are not able to support travel to an entity's location may subcontract some or all of the onsite assessment work to another qualified assessor company that is based in or near the entity's location. Outsourcing onsite assessment work to an approved subcontractor allows for independent assessment to be completed and for a qualified assessor to observe environments firsthand. All subcontracting engagements are to be handled in accordance with the applicable assessor program requirements.

[10] As defined in the applicable assessor program Qualification Requirements and Program Guides.

# Appendix A Addendum for ROC/ROV: Remote Assessments

This Addendum documents the use of remote testing methods to complete an assessment to a PCI SSC standard. Completion of this Addendum is defined by the applicable PCI SSC program or payment brand compliance program requirements.

## *Assessment Details*

| | |
|---|---|
| PCI SSC standard and version used for the assessment: | |
| Company name of the entity being assessed: | |
| Name of solution, application, or product being assessed, if applicable: | |
| Date of completion of Assessment (as stated in section 3.x of the AOC/AOV): | |

## *Overview of Remote Testing Activity*

| | |
|---|---|
| To what extent were remote testing methods used for this assessment? | ☐ A combination of onsite and remote testing methods was used<br>☐ 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. | |

## *Use of Subcontractors*

| | | |
|---|---|---|
| Were any aspects of the assessment subcontracted to another Assessor Company?[11] | ☐ Yes | ☐ No |
| If yes, identify the Assessor Company(s) utilized during the assessment. | | |

[11] The use of subcontractors must conform with the requirements defined in the applicable assessor program Qualification Requirements and Program Guides.

### *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 | | |
| Interview personnel | ☐ Yes | ☐ No | | |
| Examine/observe live data | ☐ Yes | ☐ No | | |
| Observe process being performed | ☐ Yes | ☐ No | | |
| Observe physical environment | ☐ Yes | ☐ No | | |
| Interactive testing | ☐ Yes | ☐ No | | |

### *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 PCI SSC Remote Assessment Guidelines? | ☐ 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 |

### *Requirements That Could Not be Fully Verified*

| | | |
|---|---|---|
| Were any requirements unable to be fully tested, or was the assessor otherwise unable to reach a finding for any requirement, due to an inability to perform onsite testing?<br>If yes, complete the following table. | ☐ Yes | ☐ No |

| Requirement number | Was any testing able to be completed for this requirement? | | Describe what (if any) aspects of the requirement could be verified | Describe what aspects of the requirement could not be verified |
|---|---|---|---|---|
| | ☐ Yes | ☐ No | | |
| | ☐ Yes | ☐ No | | |
| | ☐ Yes | ☐ No | | |

### *Assessor Attestation*

| | |
|---|---|
| *Signature of Lead Assessor* | *Date:* |
| *Lead Assessor Name:* | *Assessor Company Name:* |

### *Findings and Observations*

The assessor should document any additional information related to the use of remote assessment activities that is relevant to the finding for a requirement in the Findings and Observations section of the applicable ROC/ROV, including:

- How the assessor confirmed the authenticity and completeness of evidence collected
- Details of any additional and alternative testing performed to resolve reliability or assurance gaps

Assessors may only document a finding of "in place"[12] for a requirement if they have reached a high degree of confidence in the coverage and scope of testing performed, the reliability and accuracy of the testing results and the evidence received, and that the level of assurance achieved is equivalent with performing the assessment onsite.

If a requirement was unable to be fully tested or the assessor does not have a high level of confidence in the testing result, the assessor cannot confirm a finding for the requirement. For requirements where a finding could not be reached, the only option is to identify the requirement as "not in place."[13] In this scenario, the assessor should provide details of testing that could not be completed or that otherwise did not produce the assurance needed to reach a finding.

A summary of how incomplete findings are to be documented for each PCI SSC standard is provided in Table 6.

[12] Or equivalent terminology as used in the ROC/ROV to indicate that a requirement has been met
[13] Or equivalent terminology as used in the ROC/ROV to indicate that a requirement has not been met

**Table 6. How to document incomplete findings for each PCI SSC standard**

| Standard Program | How to document incomplete findings within the ROC/ROV Findings and Observations section |
|---|---|
| Card Production and Provisioning – Logical | Identify as “New” (for the first incomplete finding) or “Open” (for subsequent incomplete findings) in the ROC |
| Card Production and Provisioning – Physical | Identify as “New” (for the first incomplete finding) or “Open” (for subsequent incomplete findings) in the ROC |
| CPoC | Identify as “Not Verified” in the Evaluation Report |
| P2PE | Identify as “Not in Place” in the applicable P-ROV |
| PA-DSS | Identify as “Not in Place” in the ROV |
| PCI 3DS Core | Identify as “Not in Place” in the ROC |
| PCI DSS | Identify as “Not in Place” in the ROC or SAQ |
| PCI PIN | Identify as “Not in Place” in the ROC |
| Secure SLC | Identify as “Not in Place” in the ROC |
| Secure Software | Identify as “Not in Place” in the ROV |
| SPoC | Identify as “Not Verified” in the Evaluation Report |
| TSP | Identify as “Not in Place” in the ROC |

For assessments associated with a PCI SSC validation program, incomplete assessments are not eligible for submission to PCI SSC.

For assessments associated with a payment brand compliance program, the acceptance of incomplete assessments is determined by the compliance-accepting entity.

# Appendix B References

*Environmental, Health & Safety Knowledge Brief: Remote Auditing for COVID-19 and Beyond*, Roy Litzenberg and Carrie F. Ramirez, The Institute of Internal Auditors

*General guidance on IT Audit Technology Risk: Knowns and Unknowns*, Robin Lyons, ISACA, December 2020

*GMP Auditing and COVID-19: A Guide to Remote Auditing and Workforce Recovery*, the FDA Group LLC, 2020

*Guidelines for Conducting Remote Audits*, Rainforest Alliance, April 2020

*IAF Informative Document Principles on Remote Assessment Issue 1*, IAF ID 12:2015 International Accreditation Forum, Inc

*IAF Mandatory Document for the Use of Information and Communication Technology (ICT) for Auditing/Assessment Purposes*, Issue 2 IAF MD 4:2018, July 2018, International Accreditation Forum

*IATF Global Waivers and Measures In Response to the Coronavirus Pandemic (COVID-19) - Revision 5*, International Automotive Task Force, October 2020

*ISO 9001 Auditing Practices Group Guidance on Remote Audits Editon1 2020-04-16*, International Organization for Standardization, International Accreditation Forum

*ISO 19011:2018(E) Guidelines for Auditing Management Systems*, International Organization for Standardization

*Making Remote Work*, Lance B. Coleman Sr, Quality Progress, ASQ, September 2020