Payment Card Industry (PCI)
Data Security Standard
Approved Scanning Vendors

Program Guide

Version 3.1

July 2018

Document Changes

Date	Version	Description
February 2010	1.0	Approved Scanning Vendors (ASV) Program Guide Reference Document 1.0 of the PCI (DSS) 1.2: this is the first release of the ASV Program Guide. Constructed by the ASV Taskforce and finalized by PCI SSC's Technical Working Group (TWG) and approved by the PCI SSC Executive Committee.
May 2013	2.0	ASV Program Guide updated to provide a number of minor clarifications in response to feedback from the ASV and scanning community, including clarification on resolving inconclusive scans due to scan interference. Changes to formatting, punctuation and grammar also made throughout the document. This document is intended for use with PCI DSS version 2.0.
February 2017	3.0	Updated to align with PCI DSS v3.2 and other PCI SSC program documents and provide clarification in response to feedback from ASV, merchant/service provider and acquirer communities. Added new scan components: ▪ Anonymous (non-authenticated) key-exchange protocols ▪ Embedded links from out-of-scope domains ▪ Insecure Services ▪ Unknown Services ▪ Virtualization Components Added guidance for aggregating multiple failing scan reports to total one passing scan report. Increased scan-report retention period from two years to three years to align with *ASV Qualification Requirements* evidence retention period. Updated reporting requirements and templates: ▪ Clarification of passing scan report being the initial scan or the result of multiple failing scans in Appendix A: Attestation of Scan Compliance. ▪ Allow ASVs to omit Low severity/non-compliance impacting vulnerabilities from Appendix B: ASV Scan Report Summary. ▪ Require ASVs to report all detected/open ports and services in Appendix C: Scan Report Vulnerability Details. Added Appendix D: ASV Scan Report Summary Example. Removed Appendix E: Remote Access Security Features.
July 2018	3.1	Removed requirement to report components no longer used/owned by the scan customer for an additional quarter (section 5.5.3) Removed requirement to report information leakage as an automatic failure (Table 1) Updated requirements related to SSL/early TLS to aslign with PCI DSS v3.2.1 (Table 1) Clarified details in Scan Report Summary Example (Appendix D)

Table of Contents

Program Guide Version 3.1 ..... **1**
Document Changes **1**
1 Introduction **3**
1.1 Related Publications 3
1.2 Updates to Documents and Security Requirements 3
2 About PCI SSC **4**
2.1 PCI DSS Initiative and Overview 4
3 Terminology **5**
4 Roles and Responsibilities **7**
4.1 Participating Payment Brands 7
4.2 PCI SSC 7
4.3 Approved Scanning Vendors 7
4.4 ASV Validation Lab 8
4.5 Qualified Security Assessors (QSAs) 8
4.6 Scan Customers 9
5 Scan Process Overview **11**
5.1 PCI DSS Requirement 11.2 12
5.2 Can a Merchant or Service Provider Perform its own External Vulnerability Scanning? 13
5.3 ASV Testing and Approval Process 14
5.4 Fees for ASV Testing and Approval Process 15
5.5 ASV Scan Scope Definition 15
5.6 ASV Scan Interference 17
6 ASV Scan Solution – Required Components **20**
6.1 General Characteristics 20
6.2 Vulnerability Reporting 30
6.3 Compliance Determination – Overall and by Component 31
7 Scan Reporting **33**
7.1 Generating, Reading, and Interpreting Scan Reports 33
7.2 Special Notes 35
7.3 Scan Customer and ASV Attestations 35
7.4 ASV Scan Finalization 36
7.5 Resolving Failing ASV Scans 36
7.6 Resolving Inconclusive Scans 37
7.7 Managing False Positives and Other Disputes 38
7.8 Addressing Vulnerabilities with Compensating Controls 39
7.9 Compliance Reporting 39
7.10 Report Delivery and Integrity 39
8 Quality Assurance **40**
8.1 ASV's Internal Quality Assurance Program 40
8.2 PCI SSC's Quality Assurance Program for ASVs 40
8.3 Remediation 41
8.4 Revocation 41
Figure 1: Overview of ASV Scan Processes **42**
Appendix A: ASV Scan Report Attestation of Scan Compliance **43**
Appendix B: ASV Scan Report Summary **45**
Appendix C: ASV Scan Report Vulnerability Details **48**
Appendix D: ASV Scan Report Summary Example **49**

1 Introduction

This *Approved Scanning Vendor (ASV) Program Guide* explains the purpose and scope of PCI DSS external vulnerability scans for merchants and service providers undergoing scans as part of validating compliance with PCI DSS Requirement 11.2.2, and also provides guidance and requirements for ASVs who perform these scans.

The requirements in this document apply specifically to the quarterly EXTERNAL vulnerability scans required by PCI DSS Requirement 11.2.2. PCI SSC recommends, but does not require, that scan customers use this document for other vulnerability scanning required by PCI DSS Requirement 11.2, including internal vulnerability scanning, scanning performed after a significant change to the network or applications, and any scanning performed in addition to the required quarterly external scans/rescans.

1.1 Related Publications

Requirement 11.2.2 of the PCI DSS requires quarterly external vulnerability scans by an Approved Scanning Vendor (ASV) approved by PCI SSC. The PCI DSS provides the foundation for this and all other PCI DSS-related requirements and procedures.

In regard to the ASV Program, the following additional documents are used in conjunction with the PCI DSS:

- *Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard Glossary of Terms, Abbreviations, and Acronyms*
- *Payment Card Industry (PCI) Qualification Requirements for Approved Scanning Vendors (ASV)*

Note: *The PCI DSS provides the specific technical requirements and assessment procedures used by merchants and service providers to validate PCI DSS compliance and document the assessment. PCI DSS Requirement 11.2.2 specifically requires quarterly external vulnerability scans that must be performed by an ASV. The* ASV Qualification Requirements *define the requirements that must be met by an ASV in order to perform PCI DSS quarterly external vulnerability scans for ASV Program purposes.*

All ASV Program-related documents are available in electronic form on www.pcisecuritystandards.org.

1.2 Updates to Documents and Security Requirements

PCI SSC updates PCI DSS requirements in accordance with a standards lifecycle management process. The *ASV Program Guide* may be updated when threats evolve, or as necessary to reflect changes to the PCI DSS.

PCI SSC reserves the right to change, amend, or withdraw the PCI DSS and/or ASV Requirements at any time, and works closely with its community of Participating Organizations regarding such changes.

The final published version of this document supersedes *ASV Program Guide v3.0.*

ASVs may begin using this document and the included report templates immediately, and must implement the requirements set forth in this document effective 1 July, 2018.

2 About PCI SSC

PCI SSC reflects a desire among constituents at all levels of the Payment Card Industry to standardize security requirements, security assessment procedures, and processes for external vulnerability scans and validation of ASV scan solutions. The ASV Program documents and PCI DSS together define a common security assessment framework that is currently recognized by each Participating Payment Brand.

All stakeholders in the payments value chain can benefit from the standardized requirements:

- Scan customers benefit from a broad selection of ASVs and gain assurance that if they use ASV scan solutions, those solutions have been validated by an ASV Validation Lab as satisfying applicable PCI DSS requirements.
- Consumers gain assurance that merchants and service providers are receiving vulnerability scans from validated ASV scan solutions.
- Acquiring banks and Participating Payment Brands receive consistent reports to help demonstrate merchant and service provider compliance with applicable PCI DSS requirements.

For more information regarding PCI SSC, see the Website.

2.1 PCI DSS Initiative and Overview

PCI DSS Requirement 11.2.2 requires that external vulnerability scanning be performed at least quarterly by an ASV qualified by PCI SSC. The *ASV Program Guide* sets forth a standard set of:

- Technical requirements for ASV scan solutions
- Reporting requirements for ASV scan solutions
- Processes for determining scan customers' compliance with PCI DSS external vulnerability scanning requirements using an ASV scan solution
- ASV testing and approval processes
- Quality assurance processes for ASVs
- Scan requirements and guidance for scan customers

Note:
The ASV prepares scan reports in accordance with Section 7, "Scan Reporting," and submits those reports to the scan customer. The scan customer then submits those reports to its acquirers or Participating Payment Brands as directed by the Participating Payment Brands.

3 Terminology

Throughout this document, the following terms shall have the meanings below.

Term	Meaning
ASV	Acronym for "Approved Scanning Vendor." Refers to a company qualified by PCI SSC for ASV Program purposes to conduct external vulnerability scanning services in accordance with PCI DSS Requirement 11.2.2.
ASV Agreement	The then-current version of (or successor document to) the PCI ASV Compliance Test Agreement, the current version of which is attached as Appendix A to the *ASV Qualification Requirements*.
ASV Program	The Approved Scanning Vendor Program managed and operated by PCI SSC (the "ASV Program").
ASV Qualification Requirements	The then-current version of (or successor documents to) the *Payment Card Industry (PCI) Qualification Requirements for Approved Scanning Vendors (ASV)*, as from time to time amended and made available on the Website.
ASV Portal	The then-current PCI SSC Assessor Portal (and its accompanying web pages), which is currently available at https://programs.pcissc.org.
ASV scan (or ASV scanning)	The external vulnerability scanning services performed by an ASV using an ASV scan solution to validate the compliance of a scan customer with PCI DSS Requirement 11.2.2 for ASV Program purposes.
ASV scan solution (or scan solution)	A set of security services, tool and processes offered by an ASV to validate the compliance of a scan customer in accordance with PCI DSS Requirement 11.2.2 and that at the time of such validation appears on the list of Approved Scanning Vendors on the Website. ASV scan solutions include the tools, methods, procedures, associated scan reports, processes for exchanging information between the ASV and the scan customer, and the processes used by ASV Employees to: ▪ Operate the ASV scan solution. ▪ Work with scan customer to coordinate and resolve matters. ▪ Review and interpret scan results, as needed. ▪ Generate the scan report. ▪ Submit the scan report to the scan customer.
ASV Validation Lab	Defined in the *ASV Qualification Requirements.*
CDE	Acronym for "cardholder data environment." The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.
CVE (Common Vulnerabilities and Exposures)	A publicly available and free-to-use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.
CVSS (Common Vulnerability Scoring System)	A vendor-agnostic, industry open standard designed to convey the severity of computer system security vulnerabilities and help determine urgency and priority of response.

Term	Meaning
External scan	A vulnerability scan conducted from outside the logical network perimeter on all Internet-facing hosts that are within or provide a path to an entity's cardholder data environment (CDE).
Internal scan	A vulnerability scan conducted from inside the logical network perimeter on all internal-facing hosts that are within or provide a path to an entity's cardholder data environment (CDE).
NVD (National Vulnerability Database)	The U.S. government repository of standards-based vulnerability management data. NVD includes databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics.
Participating Payment Brand	Defined in the ASV Agreement.
PCI DSS	Acronym for "Payment Card Industry Data Security Standard." Refers to the then-current version of (or successor documents to) the *Payment Card Industry (PCI) Data Security Standard and Security Assessment Procedures,* as from time to time amended and made available on the Website.
PCI SSC	Acronym for "Payment Card Industry Security Standards Council" that refers to PCI Security Standards Council, LLC.
QSA	Acronym for "Qualified Security Assessor." QSAs are companies qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the *Payment Card Industry (PCI) Qualification Requirements for Qualified Security Assessors (QSA)* for details about requirements for "QSA Companies" and "QSA Employees."
Scan customer	A merchant or service provider that is required to undergo a quarterly external vulnerability scan via an ASV for ASV Program purposes.
Scan interference	Interference, including but not limited to, active protection systems blocking, filtering, dropping or modifying network packets in response to scan traffic, such that the view of the environment would be changed and the ASV scan solution would no longer see what an attacker would see.
Test Bed (or ASV test bed)	A simulated network environment containing a baseline of intentionally vulnerable hosts and network devices against which all candidate and validated ASV scan solutions are tested to demonstrate their capability to detect, accurately identify, and report a baseline of technical vulnerabilities for ASV Program purposes.
Website (or PCI SSC Website)	The then-current PCI SSC web site (and its accompanying web pages) currently available at www.pcisecuritystandards.org.

4 Roles and Responsibilities

There are several stakeholder groups in the payment community. Some of these stakeholders—ASVs, QSAs, and PCI SSC—participate more directly in the PCI DSS assessment process. Stakeholders that are not directly involved with the assessment process should nonetheless be aware of the overall process to facilitate associated business decisions.

The following describes the high-level roles and responsibilities of the stakeholders in the payment community as they relate to the PCI DSS and ASV Program.

4.1 Participating Payment Brands

The Participating Payment Brands develop and enforce their respective programs related to compliance with PCI standards, including, but not limited to, the following:

- Requirements, mandates, or dates for PCI DSS compliance
- Fines or penalties for non-compliance

4.2 PCI SSC

PCI SSC maintains various payment card industry standards, supporting programs, and related documentation in accordance with a standards lifecycle management process. In relation to the ASV Program, PCI SSC:

- Maintains the *ASV Program Guide* and *ASV Qualification Requirements* (including the ASV Agreement)
- Provides training for ASV Companies and ASV Employees
- Evaluates ASV Company and ASV Employee qualifications to perform external vulnerability scans in accordance with PCI DSS and ASV Program requirements
- Maintains the List of Approved Scanning Vendors on the Website
- Maintains a quality assurance program for ASVs

4.3 Approved Scanning Vendors

An ASV is an organization with an ASV scan solution (i.e., a set of security services and tools) used to validate adherence to the external scanning requirements of PCI DSS Requirement 11.2.2. The ASV's ASV scan solution must be tested by an ASV Validation Lab and approved by PCI SSC before that ASV is added to the list of Approved Scanning Vendors.

ASVs are responsible for the following:

- Performing external vulnerability scans in accordance with PCI DSS Requirement 11.2.2, this document and other supplemental guidance published by PCI SSC.
- Maintaining the security and integrity of systems and tools used to perform such scans.
- Ensuring that such scans:
  - Do not impact the normal operation of the scan customer environment.
  - Do not penetrate or intentionally alter the scan customer environment.

- Scanning all IP address ranges, domains, components, etc. provided by the scan customer to identify active components and services.
- Consulting with the scan customer to determine whether components found, but not provided by the scan customer, should be included in the scope of the scan.
- Providing a determination as to whether the scan customer's components have met the scanning requirements.
- Providing adequate documentation within the scan report to demonstrate the compliance or non-compliance of the scan customer's components with the scanning requirements.
- Submitting (to the scan customer) the ASV Scan Report Attestation of Scan Compliance cover sheet (an "Attestation of Scan Compliance") and the scan report in accordance with the instructions of the scan customer's acquirer(s) and/or Participating Payment Brand(s).
- Including required scan customer and ASV Company attestations in the scan report in accordance with this document and applicable ASV Program requirements.
- Retaining scan reports and related work papers and work product for three (3) years, as required by the *ASV Qualification Requirements*.
- Providing the scan customer with a means for disputing findings of scan reports.
- Maintaining an internal quality assurance process for its ASV Program-related efforts in accordance with this document and applicable ASV Program requirements.

4.4 ASV Validation Lab

ASV Validation Labs (defined in the *ASV Qualification Requirements*) are PCI-recognized laboratories that host a simulated network environment ("Test Bed") containing a baseline of intentionally vulnerable hosts and network devices against which all ASV scan solutions are tested to demonstrate their capability to detect, identify, and report a baseline of technical vulnerabilities contained within the ASV Validation Lab.

ASV Validation Labs are responsible for the following:

- Configuring and maintaining their ASV testing laboratory environment and Test Bed in accordance with PCI SSC coordination and instructions.
- Assessing and scoring scan test reports submitted by scanning vendors upon completion of the scan test for the vendor's candidate or approved ASV scan solution.
- Conducting debriefing sessions with the scanning vendor to provide the test results and feedback on the scan solution's performance.

4.5 Qualified Security Assessors (QSAs)

QSAs, while performing onsite assessments, are responsible for the following:

- Performing PCI DSS Assessments in accordance with the PCI DSS, which includes confirming that PCI DSS Requirement 11.2.2 is "in place" and that the ASV and ASV scan solution were both on the list of Approved Scanning Vendors on the date when the respective scans were performed.
- Providing an opinion about whether the assessed entity meets applicable PCI DSS requirements in accordance with QSA Program requirements.
- Providing adequate documentation within the Report on Compliance (ROC) to demonstrate the assessed entity's compliance with the PCI DSS.

- Submitting the ROC and the Attestation of Validation (signed by the QSA and in some cases, the assessed entity).
- Maintaining an internal quality assurance process for its QSA program-related efforts.

It is the QSA's responsibility to attest to the entity's compliance with PCI DSS. PCI SSC does not approve ROCs from a technical perspective, but performs QA reviews on ROCs to help ensure that the documentation of test procedures performed is sufficient to demonstrate compliance.

4.6 Scan Customers

Scan customers are responsible for the following:

- Maintaining compliance with the PCI DSS at all times, which includes properly maintaining the security of their Internet-facing systems.
- Selecting an ASV from the list of Approved Scanning Vendors from the Website to conduct quarterly external vulnerability scanning in accordance with PCI DSS Requirement 11.2.2 and this document using an ASV scan solution.
- Performing due diligence in its ASV selection process, per the scan customer's due-diligence processes, to obtain assurance as to the ASV's qualification, capability, experience, and level of trust in performing scanning services required by the PCI DSS.
- To the degree deemed appropriate by the scan customer, monitoring Internet-facing systems, active protection systems, and network traffic during the scan, to assure an acceptable level of trust is maintained.
- Defining the scope of external vulnerability scanning, which includes:
  - Providing the IP addresses and/or domain names of all Internet-facing systems to the ASV so the ASV can properly conduct a full scan.
  - Implementing proper network segmentation for any external-facing components excluded from the scope.

  See Section 5.5, "ASV Scan Scope Definition," for more information.
- Ensuring that devices do not interfere with the ASV scan, including:
  - Configuring active protection systems so they do not interfere with the ASV's scan, as required by this document. See Section 5.6, "ASV Scan Interference."
  - Coordinating with the ASV if the scan customer has load balancers in use. See "Account for Load Balancers" in Section 6.1.
- Coordinating with the scan customer's Internet service provider (ISP) and/or hosting providers to allow ASV scans. See Section 5.5.2, "Internet Service Providers and Hosting Providers."
- Attesting to proper scoping and network segmentation (if IP addresses or other components are excluded from scan scope) within the ASV scan solution. See Section 7.3, "Scan Customer and ASV Attestations."
- Providing sufficient documentation to the ASV to fully enable the ASV's investigation and resolution of disputed findings, such as suspected false positives, and providing related attestation. See Section 7.7, "Managing False Positives and Other Disputes."

- Providing sufficient documentation to the ASV to fully enable the ASV's evaluation of any compensating controls implemented or maintained by the scan customer. See Section 7.8, "Addressing Vulnerabilities with Compensating Controls."
- Reviewing the scan report and correcting any noted vulnerabilities that result in a non-compliant scan.
- Arranging with the ASV to re-scan any non-compliant systems to verify that all "High" and "Medium" severity vulnerabilities have been resolved, to obtain a passing quarterly scan. See Table 2 of Section 6, "Vulnerability Severity Levels Based on the NVD and CVSS."
- Submitting the completed ASV scan report to the scan customer's acquirer(s) and/or Participating Payment Brand(s), as directed by the Participating Payment Brands.
- Providing feedback on ASV performance in accordance with the ASV Feedback Form (available on the Website).

Note: *Fees and dates for the ASV's scanning services are typically established between the ASV and the scan customer. The scan customer typically either pays these fees directly to the ASV, or to the scan customer's acquirer or other aggregating entity (if the acquirer or other aggregating entity has a contract with the ASV on behalf of a group of merchants).*

5 Scan Process Overview

To demonstrate compliance with the PCI DSS, merchants and service providers may be required by applicable Participating Payment Brands to conduct periodic PCI DSS vulnerability scans, in accordance with PCI DSS Requirement 11.2.

PCI DSS external vulnerability scans are conducted over the Internet by an ASV, as a remote service that requires scanning from a source external to the scan customer's network and does not require onsite presence to execute. PCI DSS external vulnerability scans are an indispensable tool to be used in conjunction with a vulnerability management program. Vulnerability scans help identify vulnerabilities and misconfigurations of websites, applications, and other information technology infrastructures with Internet-facing IP addresses.

Vulnerability scan results provide valuable information that supports efficient patch management and other security measures that help improve protection against Internet attacks.

PCI DSS external vulnerability scans may apply to any merchant or service provider with external/ Internet-facing components. Even if an entity does not offer Internet-based transactions, other services may make systems Internet accessible. Basic functions such as email and user Internet access will result in the Internet-accessibility of a company's network. Such seemingly insignificant paths to and from the Internet can provide unprotected pathways into scan customer systems and potentially expose cardholder data if not properly controlled.

Vulnerability scanning companies interested in providing vulnerability scanning services for ASV Program purposes must comply with the requirements set forth in this document as well as the *ASV Qualification Requirements* and related ASV Program requirements, and must successfully complete the PCI SSC Security Scanning Vendor Testing and Approval Process. See Section 5.3, "ASV Testing and Approval Process."

Note: *To be considered compliant with the external vulnerability scanning requirement of PCI DSS Requirement 11.2.2, the scan customer infrastructure must be tested and shown to be compliant, in accordance with this document and applicable ASV Program requirements. Compliance with this external vulnerability scanning requirement only represents compliance with PCI DSS Requirement 11.2.2, and does not represent or indicate compliance with any other PCI DSS requirement or component.*

Refer to Figure 1 for an overview of the major phases of the scanning process for both scan customers and ASVs, and for a summary of the flow of activities during these phases. The main phases of the scanning process consist of:

- Scoping
- Scanning
- Reporting/remediation
- Dispute Resolution
- Rescan (as needed)
- Final reporting

5.1 PCI DSS Requirement 11.2

PCI DSS Requirements	Testing Procedures
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred..*	**11.2** Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed as follows:
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	**11.2.1.a** Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.
	11.2.1.b Review the scan reports and verify that all "high risk" vulnerabilities are addressed and the scan process includes rescans to verify that the "high risk" vulnerabilities (as defined in PCI DSS Requirement 6.1) are resolved.
	11.2.1.c Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).

PCI DSS Requirements	Testing Procedures
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).* *Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*	**11.2.2.a** Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period.
	11.2.2.b Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures).
	11.2.2.c Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	**11.2.3.a** Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned.
	11.2.3.b Review scan reports and verify that the scan process includes rescans until: ▪ For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. ▪ For internal scans, all "high risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved.
	11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).

5.2 Can a Merchant or Service Provider Perform its own External Vulnerability Scanning?

Pursuant to the PCI DSS, merchants and service providers must use only ASVs to perform the quarterly external vulnerability scans required by PCI DSS Requirement 11.2.2, and the ASV scan solution must be managed by the ASV. Some ASV scan solutions may, while still under the control and management of the ASV, be started remotely by a scan customer (for example, via an ASV's web portal and/or ASV's scan solution) to allow a scan customer to select the best times to scan their cardholder data environment and define which of the customer's components are to be scanned. However, only authorized ASV Employees are permitted to configure any settings (for example, modify or disable any vulnerability checks, assign severity levels, alter scan parameters, etc.), or modify the output of the scan. Additionally, the ASV scan solution must not provide the ability for anyone other than an authorized ASV Employee to alter or edit any reports, or revise any results.

While scan customers may seek assistance from external security consultants, including QSAs, to help them understand their scan results and coordinate on their behalf with the ASV, QSA Companies are bound to the QSA Agreement, which includes specific organizational independence requirements. Therefore, an ASV that is also a QSA Company must have controls in place to assure separation of duties between functions in order to ensure independence and avoid any conflicts of interest. Refer to the *QSA Qualification Requirements* and the QSA Agreement for more details.

Additionally, the Scan Customer Attestation of Scan Compliance (*ASV Program Guide* Appendix A) must be completed by the scan customer and may not be outsourced to a third party. If the scan customer receives assistance producing or submitting dispute-supporting evidence to the ASV, the scan customer is still required to review the evidence prior to submittal, and attest to its completeness and accuracy prior to the ASV generating the final report.

5.3 ASV Testing and Approval Process

As part of the initial ASV qualification process, and annually thereafter as outlined in the *ASV Qualification Requirements*, each submitted scan solution is tested in an ASV Validation Lab to ensure that it performs in accordance with this document and applicable ASV Program requirements.

Note: *ASVs may have more than one validated scan solution listed on the Website.*

The specific version(s) of the ASV's full ASV scan solution(s), as tested, approved, and listed in accordance with the ASV Program as part of PCI SSC's scanning vendor testing and approval process, is the ONLY version of the scan solution that the ASV is approved to use to perform external vulnerability scans in accordance with PCI DSS Requirement 11.2.2 for ASV Program purposes. While significant modifications to the tested and approved ASV scan solution (without undergoing another ASV Validation Lab test) are prohibited, minor modifications that enhance or improve the quality of the scan solution are acceptable. These minor improvements (which do not require another ASV Validation Lab test) fall into categories of vulnerability coverage and product maintenance:

Category	Allowed Changes
Vulnerability Coverage	Addition of new vulnerability signatures
	Improvements to the reliability and accuracy of existing vulnerability signatures (including removing individual faulty vulnerability checks for repair)
Product Maintenance	Maintenance and patching of systems comprising the scan solution
	Minor updates to the underlying software and UI, including bug fixes
	Addition of capacity or fault tolerance (scan engines, data center expansion, etc.)

For more information about qualifying as an ASV Company or ASV Employee, refer to the *Qualification Requirements for Approved Scanning Vendors (ASVs)* (i.e., *ASV Qualification Requirements*) located on the Website.

5.4 Fees for ASV Testing and Approval Process

PCI SSC charges fees for the various testing stages for candidate and/or approved ASV scan solutions, in accordance with the *PCI SSC Programs Fee Schedule* (available on the Website).

5.5 ASV Scan Scope Definition

For the purpose of ASV scanning, the PCI DSS requires quarterly vulnerability scanning of all externally accessible (Internet-facing) system components owned or utilized by the scan customer that are part of the cardholder data environment (CDE), as well as any externally facing system component that may provide access to the CDE.

In addition to providing the ASV with all external-facing IP addresses, the scan customer must also supply all fully qualified domain names (FQDN) and other unique entryways into system components for the entire in-scope infrastructure including, but not limited to:

- Domains for web servers
- Domains for mail servers
- Domains used in name-based virtual hosting
- Web server URLs to "hidden" directories that cannot be reached by crawling the website from the home page
- Any other public-facing hosts, virtual hosts, domains or domain aliases

The scan customer must define and attest to its scan scope prior to the ASV finalizing the scan report. The scan customer is ultimately responsible for defining the appropriate scope of the external vulnerability scan and must provide all Internet-facing components, IP addresses and/or ranges to the ASV. If an account data compromise occurs via an externally-facing system component *not* included in the scan scope, the scan customer is responsible.

Note: *The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment (CDE). The CDE is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data. "System components" include network devices, servers, computing devices, and applications. Examples of system components include but are not limited to the following:*

- *Systems that provide security services (for example, authentication servers) facilitate segmentation (for example, internal firewalls) or may impact the security of (for example, name-resolution or web-redirection servers) the CDE.*
- *Virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.*
- *Network components including but not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.*
- *Server types including but not limited to web, application, database, authentication, mail, proxy, Network Time Protocol (NTP), and Domain Name System (DNS).*
- *Applications including all purchased and custom applications, including internal and external (for example, Internet) applications.*
- *Any other component or device located within or connected to the CDE.*

5.5.1 Network Segmentation

Network segmentation—also referred to as "segmentation" or "isolation"—isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the CDE and thus reduce the scope of the PCI DSS Assessment. See the section titled "Network Segmentation" in the *PCI DSS Requirements and Security Assessment Procedures* for guidance on using network segmentation. Network segmentation is not a PCI DSS requirement.

In general, the following segmentation methods may be used to reduce the scope of the ASV scan:

- Provide physical segmentation between the system components that store, process, or transmit cardholder data and systems that do not.
- Employ appropriate logical segmentation where traffic is prohibited between the segment or network handling cardholder data and other networks or segments.

5.5.2 Internet Service Providers and Hosting Providers

This section applies to the scan customer's Internet service provider (ISP) or hosting provider (if used by scan customers to host part or all of their CDE).

Scan customers must coordinate with their ISPs to allow the ASV scan to be performed without interference from active protection systems. For more details, see Section 5.6, "ASV Scan Interference."

In a shared hosting environment, the scan customer shares the environment with the hosting provider's other customers. This could lead to the scan customer's environment being compromised through security weaknesses in other customers' environments at the hosting provider.

There are two options for ASV scanning of hosting providers that host scan customer infrastructures or components:

1. The hosting provider can undergo ASV scans on its own and provide evidence to its customers to demonstrate their compliant scans; or
2. The hosting provider can undergo ASV scans as part of each of its customers' ASV scans.

In either case, it is the responsibility of the scan customer to ensure that their hosted environment receives a passing score from an ASV scan.

Note: *If the hosting provider has all Internet-facing IP ranges AND all scan customers' domains, etc. scanned as part of the hosting provider's own ASV scans, and provides proof of passing scans to scan customers, the domains do not have to be included in the scan customers' ASV scans.*

5.5.3 ASV "Discovery" and Scope Validation

ASVs must, at a minimum, perform the below actions to identify whether any scoping discrepancies exist in the information provided by the scan customer. Information about any scoping discrepancies must be indicated on the Attestation of Scan Compliance (see Appendix A) under A.3, "Scan Status" (Number of components found by ASV but not scanned because scan customer confirmed components were out of scope). Although this information must be reported as noted above, the ASV should disregard this information in making its PCI DSS compliance determination:

- Include any IP address or domain previously provided to the ASV and still owned or used by the scan customer that has been removed at the request of the scan customer.
- For each domain provided, look up the IP address of the domain to determine whether it was already provided by the scan customer.
- For each domain provided, perform DNS forward and reverse lookups of common host names—such as "www," "mail," etc.—that were not provided by the scan customer.
- Identify any IP addresses found during MX record DNS lookup.
- Identify any IP addresses outside of scope reached via web redirects from in-scope web servers (includes all forms of redirect including: JavaScript, Meta redirect and HTTP 30x codes).
- Match domains found during crawling to user-supplied domains to find undocumented domains belonging to the scan customer.

5.6 ASV Scan Interference

If an ASV detects that an active protection system has actively blocked or filtered a scan, then the ASV is required to handle it in accordance with Section 7.6, "Resolving Inconclusive Scans." In order to ensure that reliable scans can be conducted, the ASV scan solution must be allowed to perform scanning without interference from active protection systems, where "active" denotes security systems that dynamically modify their behavior based on information gathered from non-attack network traffic patterns. Non-attack traffic refers to potentially legitimate network traffic patterns that do not indicate malformed or malicious traffic, whereas attack traffic includes, for example, malicious network traffic patterns or patterns that match known attack signatures, malware, or packets exceeding the maximum permitted IP packet size.

Examples of active protection systems that dynamically modify their behavior include, but are not limited to:

- Intrusion prevention systems (IPS) that drop non-malicious packets based on previous behavior from originating IP address (for example, blocking all traffic from the originating IP address for a period of time because it detected one or more systems being scanned from the same IP address)
- Web application firewalls (WAF) that block all traffic from an IP address based on the number of events exceeding a defined threshold (for example, more than three requests to a login page per second)
- Firewalls that shun/block an IP address upon detection of a port scan from that IP address

- Next generation firewalls (NGF) that shun/block IP address ranges because an attack was perceived based on previous network traffic patterns
- Quality of Service (QoS) devices that limit certain traffic based on traffic volume anomalies (for example, blocking DNS traffic because DNS traffic exceeded a defined threshold)
- Spam filters that blacklist a sending IP address based on certain previous SMTP commands originating from that address

Such systems may react differently to an automated scanning solution than they would react to a targeted hacker attack, which could cause inaccuracies in the scan report.

Systems that consistently block attack traffic, while consistently allowing non-attack traffic to pass (even if the non-attack traffic follows directly after attack traffic) typically do not cause ASV scan interference. Examples of these security systems (that do not dynamically modify their behavior, rather, they maintain consistent, static behavior based on rules or signatures) include, but are not limited to:

- Intrusion detection systems (IDS) that log events, track context or have a multifaceted approach to detecting attacks, but action is limited to alerting (there is no intervention).
- Web application firewalls (WAF) that detect and block SQL injections, but let non-attack traffic from the same source pass.
- Intrusion prevention systems (IPS) that drop all occurrences of a certain attack, but let non-attack traffic from the same source pass.
- Firewalls that are configured to always block certain ports, but always keep other ports open.
- VPN servers that reject entities with invalid credentials but permit entities with valid credentials.
- Antivirus software that blocks, quarantines, or deletes all known malware based on a database of defined “signatures” but permits all other perceived clean content.
- Logging/monitoring systems, event and log aggregators, reporting engines, etc.

If the ASV scan cannot detect vulnerabilities on Internet-facing systems because the ASV scan is blocked by an active protection system, those vulnerabilities will remain uncorrected and may be exploited by an attacker whose attack patterns don't trigger the active protection mechanism.

All ASV scans must either be validated by the ASV to ensure they have not been blocked or filtered by an active protection system, or resolved in accordance with Section 7.6, “Resolving Inconclusive Scans.”

Temporary configuration changes may need to be made by the scan customer to remove interference during an ASV scan.

Due to the remote nature of external vulnerability scans and the need mentioned previously to conduct an ASV scan without interference from active protection systems, certain temporary configuration changes to the scan customer's network devices may be necessary to obtain a scan that accurately assesses the scan customer's external security posture. *Note, per above, that temporary configuration changes are not required for systems that consistently block attack traffic, while consistently allowing non-attack traffic to pass (even if the non-attack traffic follows directly after attack traffic)*.

The changes in this section are considered **temporary** and are only required for the duration of the ASV scan, and only apply to external-facing components in scope for quarterly external vulnerability scans required by PCI DSS Requirement 11.2.2. Scan customers are encouraged to work with the ASV to perform secure quarterly scans that do not unnecessarily expose the scan customer's network—but also do not limit the final results of the ASV scans—as follows:

- Agree on a time for the ASV scan window to minimize how long changed configurations are in place.
- Conduct the ASV scan during a maintenance window under the scan customer's standard change control processes, with full monitoring during the ASV scan.
- Configure the active protection systems to either:
  - Monitor and log, but not to act against, the originating IP address(es) of the ASV, or
  - Allow non-attack traffic to pass consistently (even if the non-attack traffic immediately follows attack traffic)
- Reapply the previous configurations as soon as the ASV scan is complete.

Note: *The intent of these temporary configuration changes is to ensure that an active protection system, such as an IPS reacting dynamically to traffic patterns, does not interfere with the ASV scan in a manner that would provide the ASV scan solution with a different view of the environment than the view an attacker would have. ASV scans tend to be "noisy" as they generate a lot of traffic in a short period of time. This is generally to ensure that an ASV scan can be completed as quickly as possible. However, this type of approach can also lead to a high rate of reaction by active intrusion-prevention systems. An attacker will generally attempt to restrict the volume of their scans so they are stealthier and less likely to trigger an event that may be noticed. Thus, the high-volume scans typically performed by ASVs are significantly more likely to trigger an active protection mechanism than those of an attacker.*

Temporary configuration changes do not require that the scan customer "white list" or provide the ASV a higher level of network access. Rather, the scan customer must ensure that any triggers, such as volume-based or correlated IP address thresholds, are not activated by the ASV scan and the ASV scan is allowed to complete. The intent is that the ASV be provided the same network level view through the duration of the ASV scan as an actual attacker.

6 ASV Scan Solution – Required Components

6.1 General Characteristics

The ASV scan solution must have the following characteristics:

- **Be Non-disruptive**

  The ASV scan solution must not be configured with disruptive testing methods enabled that would result in a system crash or reboot, or interfere with or change Domain Name System (DNS) servers, routing, switching, or address resolution. Software (such as root kits) must not be installed unless part of the scan solution and pre-approved by the scan customer.

  The following are examples of some of the tests that are **not** permitted:

  - Denial of service (DoS)
  - Buffer overflow exploit
  - Brute-force attack resulting in an account lockout or password reset
  - Excessive usage of available communication bandwidth

- **Perform Host Discovery**

  The ASV scan solution must make a reasonable attempt to identify live systems, including live systems that do not respond to ICMP echo ("ping") requests.

- **Perform Service Discovery**

  The ASV scan solution must perform a port scan on all Transmission Control Protocol (TCP) ports and common User Datagram Protocol (UDP) ports, including UDP ports related to the following services:

  - Authentication services such as RADIUS and Kerberos
  - Backdoors and remote access applications
  - Backup applications
  - Database servers
  - DNS (Domain Name System)
  - NetBIOS and CIFS
  - NFS (Network File System)
  - NTP (Network Time Protocol)
  - P2P (peer-to-peer), chat or instant messaging applications
  - Routing protocols, including RIP (Routing Information Protocol)
  - RPC (Remote Procedure Call) and RPC endpoint mapping
  - SNMP (Simple Network Management Protocol) and SNMP trap
  - Syslog
  - TFTP (Trivial File Transfer Protocol)
  - VPNs (Virtual Private Networks), including ISAKMP, L2TP, and NAT-T
  - Other common UDP ports that may expose the scan customer to vulnerabilities, including ports associated with malicious activity

- **Perform OS and Service Fingerprinting**

  Fingerprinting can reduce the load on the scan customer environment by eliminating tests that are not relevant to the particular environment. Additionally, accurate operating system and service version identification can help scan customers understand their risks and prioritize remediation activities.

  The ASV scan solution should, where possible, identify the operating system running on each live system. The ASV scan solution should also, where possible, determine the protocol and service/application and version running on each open port. Since services may sometimes run on non-standard ports, the ASV scan solution should, where possible, not rely solely on a well-known port number to determine which protocol or service is running on a given port.

- **Have Platform Independence**

  Customer platforms are diverse and each platform has strengths and weaknesses. The ASV scan solution must cover all commonly used platforms.

- **Be Accurate**

  In addition to confirmed vulnerabilities, ASVs must report all occurrences of vulnerabilities that have a reasonable level of identification certainty. *When the presence of a vulnerability cannot be determined with certainty, the potential vulnerability must be reported as such*. Potential vulnerabilities must be scored the same as confirmed vulnerabilities and must have the same effects on compliance determination.

- **Account for Load Balancers**

  If a scan customer has deployed load balancers, the scan may only see part of the configuration beyond the load balancer. In these cases, the following applies:

  - Localized Load Balancers: The ASV must obtain documented assurance from the scan customer that the infrastructure behind the load balancer(s) is synchronized in terms of configuration.

    If the scan customer is unable to validate a synchronized environment behind their load balancers, the ASV must disclose the inconsistency with the following Special Note[1] on the scan report:

    > ***Note to customer:*** *As you were unable to validate that the configuration of the environment behind your load balancers is synchronized, it is your responsibility to ensure that the environment is scanned as part of the internal vulnerability scans required by the PCI DSS.*

  - External Load Balancing Services: The ASV must take into account the use of load balancing services external to the scan customer's environment that direct traffic globally or regionally based upon source IP address location. Depending on implementation, external load balancing services may direct the ASV scan solution to only a regional subsection of a scan customer's environment. Thus, the ASV scan solution must accommodate external load balancing scenarios to ensure that all IP addresses and ranges provided by the scan customer are successfully scanned.

  The use of load balancers, the configuration, and the customer's assurance must be clearly documented in the scan report.

[1] Special Notes do not cause a scan failure or supersede any established CVSS scoring.

Table 1: Required Components for PCI DSS Vulnerability Scanning

Following is a non-exhaustive list of services, devices, and operating systems that must be tested.

Note: *Scan customers may use the dispute-resolution process documented in this guide if a noted failure is mitigated by compensating controls.*

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
Firewalls and Routers	Firewalls and routers, which control traffic between the company's network and external untrusted networks (for example, the Internet), have known vulnerabilities for which patches are periodically released. Another common problem with firewalls and routers is inadequate configuration. To ensure firewalls and routers are protected against these vulnerabilities and are able to protect the network effectively, it is important to apply the patches as soon as possible.	The ASV must scan all network devices such as firewalls and external routers. If a firewall or router is used to establish a demilitarized zone (DMZ), these devices must be included. The ASV scan solution must test for known vulnerabilities and determine whether the firewall or router is adequately patched.
Operating Systems	An operating system (OS) sits between hardware and applications. Malicious individuals exploit OS vulnerabilities to gain access to applications and internal databases that potentially store, process or manage access to cardholder data. New exploits are discovered routinely for OSs, and security patches are released for these flaws. To protect operating systems against these exploits and vulnerabilities, it is important to apply vendor patches as soon as possible.	The ASV scan solution must be able to verify that the operating system is patched for known exploits. The ASV scan solution must also be able to determine the version of the operating system and whether it is a version no longer supported by the vendor, in which case it must be marked as an automatic **failure** by the ASV.
Database Servers	Database servers store and manage access to cardholder data. Malicious individuals exploit vulnerabilities in these servers to gain access to cardholder data. New vulnerabilities and exploits are discovered routinely for databases, and security patches are released for these flaws. To protect against these exploits and vulnerabilities, it is important to apply the patches as soon as possible.	The ASV scan solution must be able to detect open access to databases from the Internet. This configuration is a violation of PCI DSS Requirement 1.3.6, and must be marked as an automatic **failure** by the ASV. The ASV scan solution must also be able to detect and report on known database exploits and vulnerabilities.

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
Web Servers	Web servers allow Internet users to view web pages, interact with web merchants, and conduct online web transactions. Malicious individuals exploit vulnerabilities in these servers and their scripts to gain access to applications and internal databases that potentially store, process or manage access to cardholder data. Permitting directory browsing on a web server increases security risk; for example, it may expose file system contents or provide unintended access to sensitive data. Because these servers are accessible from the public Internet, scanning for vulnerabilities is essential.	The ASV scan solution must be able to test for all known vulnerabilities and configuration issues on web servers. The ASV scan solution must also be able to scan the website and verify that directory browsing is not possible on the server. Positive identification of directory browsing must be reported and disclosed with the following Special Note: ***Note to scan customer:*** *Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Consult your ASV if you have questions about this Special Note.*
Application Servers	Application servers act as the interface between web servers and other systems, such as back-end databases. For example, when cardholders share account numbers with merchants or service providers, the application server may provide the functionality to transport data in and out of the secured network. Malicious individuals exploit vulnerabilities in these servers and scripts to gain access to applications or internal databases that potentially store, process or manage access to cardholder data. Website configurations that do not include application servers (i.e., the web server itself is configured to act as an application server) are called web application servers.	The ASV scan solution must be able to detect the presence of application servers and/or web application servers and detect known vulnerabilities and configuration issues.
Common Web Scripts	Common web scripts enable servers to respond to client-side requests (for example, to enable an e-commerce web server to respond to requests from customers' web browsers).	The ASV scan solution must be able to detect commonly found scripts such as common gateway interface (CGI) scripts, e-commerce related scripts (for example, shopping carts and CRM scripts), ASPs, PHPs, etc. and detect any known vulnerabilities.

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
Built-in Accounts	Built-in, or default accounts and passwords, are commonly used by hardware and software vendors to allow the customer initial access to the product. These accounts may have no password or have passwords assigned by the vendor. These default accounts and passwords are often published by the vendors, are well known in hacker communities, and their continued presence leaves systems highly vulnerable to attack. These accounts should be assigned strong passwords or should be disabled or removed if not needed. ***Note:*** *PCI DSS Requirement 2.1 stipulates that vendor-supplied defaults, including vendor accounts and passwords, are changed and disabled or removed before installing a system on a network.*	For testing and reporting on built-in or default accounts in routers, firewalls, operating systems, web servers, database servers, applications, point-of-sale (POS) systems, or other components, the ASV scan solution must do the following: ▪ Detect the presence of built-in or default accounts and passwords, not by using brute-force or dictionary attacks, but rather by concentrating on known built-in or default accounts using default passwords—for example, as published by software vendors or vulnerability reference sources. Any such vulnerability must be marked as an automatic **failure** by the ASV. ▪ Report on services that are available without authentication—for example, services that require a username but do not require a password.
DNS Servers	DNS servers are used to locate resources on the Internet by resolving domain names to their respective IP address. Merchants or service providers may use their own DNS server or may use a DNS service provided by their ISP. If DNS servers are vulnerable, malicious individuals can masquerade as—or redirect traffic from—a merchant's or service provider's web page and collect cardholder data.	The ASV scan solution must be able to detect the presence of DNS servers, perform forward *and* reverse DNS lookups, and detect any known vulnerability and configuration issues, including unrestricted DNS zone transfer (which must be marked as an automatic **failure** by the ASV).
Mail Servers	Mail servers typically exist in the DMZ and can be vulnerable to attacks by malicious individuals. They are a critical element to maintaining overall security of the technology infrastructure.	The ASV scan solution must be able to detect the presence of mail servers and detect any known vulnerabilities and configuration issues.
Virtualization components	Virtualization components may include virtual hosts, virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. Just like physical system components, an internet-facing virtualized component that connects (or provides a path) to the cardholder data environment is a potential target of attack and is therefore subject to scanning under PCI DSS Requirement 11.2.2.	The ASV scan solution must be able to detect and identify vulnerabilities in any accessible hypervisor as well as known vulnerabilities and configuration issues with virtualized components.

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
Web Applications	Web applications typically reside on web or application servers and interface with the back-end databases and other systems. Web applications may process or transmit cardholder data as part of the customer's online transaction, or store such data in a database server. Malicious individuals exploit web application vulnerabilities to gain access to applications or internal databases that may process, store, or manage access to cardholder data. See OWASP Top 10 Project[2] for additional information on current web application vulnerabilities. While only *unauthenticated* web application testing is required, *authenticated* testing is more thorough since user interaction and functionality (such as conducting payment transactions) can be more accurately simulated. Some authenticated scan tests may simulate attacks that could cause account lockouts or other negative impact to the systems or applications being tested, so it is important for scan customers to work with their ASVs to determine whether authenticated web application scan testing is right for their particular environment, the type and depth of testing to perform, etc. Merchants should also work with their acquiring banks or the payment brands to determine whether authenticated vulnerability scans should be performed as part of their vulnerability management program.	The ASV scan solution must be able to detect via automated or manual means current vulnerabilities and configuration issues (for example, OWASP [2] Top 10, SANS CWE Top 25, etc.) including the following web application vulnerabilities and configuration issues: ▪ Unvalidated parameters that lead to SQL injection attacks (which must be marked as an automatic **failure**) ▪ Cross-site scripting (XSS) flaws (which must be marked as an automatic **failure**) ▪ Directory traversal vulnerabilities (which must be marked as an automatic **failure**) ▪ HTTP response splitting/header injection (which must be marked as an automatic **failure**) ▪ Information leakage, including: • Detailed application error messages • Backup script files (for example, home.asp.bak, index.jsp.old, etc.) • Include file source code disclosure • Insecure HTTP methods enabled • WebDAV or FrontPage extensions enabled • Default web server files • Testing and diagnostics pages (for example, phpinfo.html, test-cgi, etc.) ***Note:*** *ASV scan solutions must be capable of detecting vulnerabilities in custom web applications. While performing authenticated web application testing is not required, certain web application vulnerabilities exist which may only be identified by means of authenticated testing, which (in addition to the required unauthenticated web application scans) may help the ASV provide a more comprehensive scan report. ASVs should work with scan customers to determine whether authenticated scans are appropriate for the particular environment.*
Other Applications	Other applications, such as those for streaming media, RSS feeds, proxy servers, media content, etc. may be exploited by malicious individuals to gain access to cardholder data that may be processed or accessed by these applications.	The ASV scan solution must be able to detect and report the presence of other applications and to detect any known vulnerability and configuration issues.

[2] https://www.owasp.org

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
Common Services	Many common services such as file and print services, email, name resolution, file transfer, etc. (often present on servers by default) have known vulnerabilities which malicious individuals can exploit to gain access to the network. These common services should either be disabled, securely configured, or patched to properly protect the systems.	The ASV scan solution must be able to detect and report common services known to have vulnerabilities.
Wireless Access Points	Wireless networks, if not securely configured, allow malicious individuals an easy way to eavesdrop on or tamper with network traffic, capture data and passwords, and gain access to a network from remote and inconspicuous locations, such as a parking lot or adjacent room or building. Wireless vulnerabilities and security misconfigurations must be identified and corrected.	The ASV scan solution must scan detected wireless access points visible from the Internet (over the wire) and detect and report known vulnerabilities and configuration issues.
Backdoors/ Malware	A backdoor is malicious software that allows an unauthorized user to bypass normal authentication while remaining undetected. Malicious software (malware) must be identified and eliminated.	The ASV scan solution must detect and report all known, remotely-detectable backdoor applications. The presence of any such malware, including rootkits, backdoors, and Trojan horse programs must be marked as an automatic **failure** by the ASV.

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
SSL/TLS	The SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols were designed to provide encryption and integrity for data during transit over a network. There are well-known and easily exploitable vulnerabilities affecting SSL and early versions of TLS, which allow for interception or modification of encrypted data during transit. There are also vulnerabilities ("forced downgrade" attacks such as CVE-2014-3566) which can trick an unsuspecting client into downgrading to insecure versions of the protocol when both client and server support newer, more secure versions along with less secure versions for backwards compatibility reasons. Per PCI DSS, strong cryptography and security protocols must be deployed—see the *PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms* (available on the Website) for additional details on "Strong Cryptography." Also refer to industry best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 rev 1 and SP 800-57, OWASP, etc.) ***Note:*** *SSL and early TLS are not considered strong cryptography and cannot be used as a security control for PCI DSS, except by POS POI terminals that are verified as not being susceptible to known SSL/early TLS exploits and the termination points to which they connect. Refer to PCI DSS Appendix A2 for details.* *See the Information Supplements "Use of SSL/Early TLS and Impact on ASV Scans" and "Use of SSL/Early TLS for POS POI Terminal Connections" on the Website for additional guidance on the use of SSL/early TLS.*	The ASV scan solution must: ▪ Detect the presence and versions of cryptographic protocols on a component or service ▪ Detect the encryption algorithms and encryption key strengths used in all cryptographic protocols for each component or service ▪ Detect the signature-signing algorithms used for all server certificates ▪ Detect and report on certificate validity, authenticity and expiration date ▪ Detect and report on whether the certificate Common Name or wildcard matches the server hostname. ***Note:*** *When scanning systems by IP address, it may not always be possible for an ASV scan solution to determine whether the server hostname matches a certificate Common Name or wildcard.* A component must be considered non-compliant and marked as an automatic **failure** by the ASV: ▪ If it supports SSL or early versions of TLS, OR ▪ If strong cryptography is supported in conjunction with SSL or early versions of TLS (due to the risk of "forced downgrade" attacks). ***Note:*** *Entities that have not completely migrated away from SSL/early TLS will need to follow the "Managing False Positives and Other Disputes" and/or "Addressing Vulnerabilities with Compensating Controls" processes to verify the affected system is not susceptible to the particular vulnerabilities. For example, where SSL/early TLS is present but is not being used as a security control—e.g., is not being used to protect confidentiality of the communication.*

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
Anonymous (non-authenticated) key-agreement protocols	Cryptographic services which allow anonymous or non-authenticated key exchange—for example, Anonymous Diffie-Hellman (ADH)—provide encryption but do not provide server authentication. Since use of such cipher suites may increase the risk of "man in the middle" attacks, it must not be used for sensitive transmissions or network communications where server authentication is required.	The ASV scan solution must be able to detect the presence of cryptographic protocols or services which allow anonymous/non-authenticated cipher suites. In addition to reporting any identified anonymous/non-authenticated cipher suites in the cardholder data environment, the ASV scan solution must note the presence of such services with the following Special Note: ***Note to scan customer:*** *Due to increased risk of "man in the middle" attacks when anonymous (non-authenticated) key-agreement protocols are used, 1) justify the business need for this protocol or service to the ASV, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.*
Remote Access	Remote access software is often visible to the Internet and not configured securely. In some cases, software vendors, service providers, integrators, or resellers use remote access tools to provide support, while sometimes remote access is not needed for business purposes or may not be known to the scan customer. Remote access software is a path frequently used for cardholder data compromises. Without strong authentication and authorization controls, remote access software increases risk to the cardholder data environment by allowing unauthorized individuals easy access into a scan customer's environment.	The ASV scan solution must be able to detect the presence of remote access software and detect any known vulnerability or configuration issues. Remote access software includes, but is not limited to: VPN (IPSec, PPTP), applications such as LogMeIn, GoToMyPC, pcAnywhere and VNC, Terminal Server, remote web-based administration, SSH, and Telnet. In addition to reporting any identified vulnerability or configuration issues in the remote access software, the ASV scan solution must note the presence of remote access software with the following Special Note: ***Note to scan customer:*** *Due to increased risk to the cardholder data environment when remote access software is present, 1) justify the business need for this software to the ASV and confirm it is implemented securely, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.*

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
Point-of-sale (POS) Software	POS software that is visible from the Internet increases risk to the cardholder data environment. Well-known default passwords and publicized weaknesses for POS software are frequently used for cardholder data compromises.	If the ASV scan solution detects point-of-sale (POS) software, the following note must be included in the Special Notes section of the scan report: ***Note to scan customer:*** *Due to increased risk to the cardholder data environment when a point-of-sale system is visible on the Internet, 1) confirm that this system needs to be visible on the Internet, that the system is implemented securely, and that original default passwords have been changed to complex passwords, or 2) confirm that the system has been reconfigured and is no longer visible to the Internet. Consult your ASV if you have questions about this Special Note.*
Embedded links or code from out-of-scope domains	Embedded code – such as code used for search engine statistics-gathering or web traffic analytics – may redirect traffic to distribution centers or malicious sites where malware can be embedded into the code, or from code that is fetched from a third party and loaded to the visitor's browser. Evidence of such attack may not be evident to the scan customer; scan customers are encouraged to first receive the code from the third party, perform a code review, and post it to the web server only after verifying its functionality and integrity. Scan customers are also encouraged to refrain from permitting banner ads on payment pages or other web pages that are susceptible to higher risk of attack.	If the ASV scan solution detects embedded code from (or links to) domains or sources outside of the scan customer's scope, the following must be included in the Special Notes section of the scan report: ***Note to scan customer:*** *Due to increased risk to the cardholder data environment when embedded links redirect traffic to domains outside the merchant's CDE scope, 1) confirm that this code is obtained from a trusted source, that the embedded links redirect to a trusted source, and that the code is implemented securely, or 2) confirm that the code has been removed. Consult your ASV if you have questions about this Special Note.*
Insecure Services / industry-deprecated protocols	Industry-deprecated protocols (such as SHA-1) and/or services that transmit username and passwords as clear text (without encryption) are considered "insecure" as it makes it very easy to intercept usernames and passwords in transit. PCI DSS Requirement 1.1.6 (under PCI DSS Requirement 1.1: Establish and implement firewall and router configuration standards...) states: *Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.*	If the ASV scan solution detects insecure services or industry-deprecated protocols, the following must be included in the Special Notes section of the scan report: ***Note to scan customer:*** *Insecure services and industry-deprecated protocols can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, 1) justify the business need for this service and confirm additional controls are in place to secure use of the service, or 2) confirm that it is disabled. Consult your ASV if you have questions about this Special Note.*

Scan Component	For Scan Customers: Why must it be scanned?	For ASVs: ASV scan solution must:
Unknown services	Ports, protocols and services that cannot be remotely identified by the ASV may indicate a less common but safe protocol or an in-house developed application using a proprietary protocol, but they may also indicate malicious activity such as backdoors, malware, rootkits, etc.	If the ASV scan solution detects a service that cannot be identified, the following note must be included in the Special Notes section of the scan report: ***Note to scan customer:*** *Unidentified services have been detected. Due to increased risk to the cardholder data environment, identify the service, then either 1) justify the business need for this service and confirm it is securely implemented, or 2) identify the service and confirm that it is disabled. Consult your ASV if you have questions about this Special Note.*

6.2 Vulnerability Reporting

To demonstrate compliance with PCI DSS Requirement 11.2.2, a scan report must not contain "High" or "Medium" severity vulnerabilities (see Table 2 below), or any vulnerability that indicates features or configurations that are in violation of PCI DSS. If such vulnerabilities exist, the ASV must consult with the scan customer to determine whether these are, in fact, PCI DSS violations and therefore warrant a non-compliant scan report.

ASVs must determine compliance based on the following requirements.

6.2.1 Vulnerability Categorization

To assist scan customers in prioritizing the solution or mitigating identified issues, ASVs must assign a severity level to each identified vulnerability or misconfiguration as defined in Table 2.

Whenever possible, ASVs must use two tools to categorize and rank vulnerabilities, and determine PCI DSS scan compliance:

1. The Common Vulnerability Scoring System (CVSS) version 2.0, which provides a common framework for communicating the characteristics and impact of IT vulnerabilities. The CVSS scoring algorithm utilizes a Base Metric Group, which describes both the complexity and impact of a vulnerability to produce a Base Score, which ranges between 0 and 10. The CVSS Base Score must, where available, be used by ASVs in computing PCI DSS compliance scoring.
2. The National Vulnerability Database (NVD), which is maintained by the National Institute of Standards and Technology (NIST). The NVD contains details of known vulnerabilities based on the Common Vulnerabilities and Exposures (CVE) dictionary. The NVD has adopted the CVSS and publishes CVSS Base Scores for each vulnerability. ASVs should use the CVSS scores whenever they are available.

The use of the CVSS and CVE standards in conjunction with the NVD is intended to provide consistency across ASVs.

With a few exceptions (see Section 6.3, "Compliance Determination – Overall and by Component" for details), any vulnerability with a CVSS base score of 4.0 or higher will result in a non-compliant scan report, and all such vulnerabilities must be remediated by the scan customer. To assist customers in prioritizing the solution or mitigating identified issues, ASVs must assign a severity level to each identified vulnerability or misconfiguration.

Table 2: Vulnerability Severity Levels Based on the NVD and CVSS

Table 2 describes how an ASV scan solution categorizes vulnerabilities and risks that are considered High or Medium severity.

CVSS Score	Severity Level	ASV Scan Result	Guidance
7.0 through 10.0	High Severity	**Fail**	To achieve a passing ASV scan, these vulnerabilities must be corrected and the affected systems must be re-scanned after the corrections (with a report(s) that shows a passing ASV scan).
4.0 through 6.9	Medium Severity	**Fail**	Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical, until all vulnerabilities rated 4.0 through 10.0 are corrected.
0.0 through 3.9	Low Severity	**Pass**	While passing ASV scan results can be achieved with vulnerabilities rated 0.0 through 3.9, organizations are encouraged, but not required, to correct these vulnerabilities.

6.3 Compliance Determination – Overall and by Component

Reports must indicate compliance determination at two levels: by component level, and for the overall customer level. The following statements provide the necessary guidance to ASVs to determine compliance at component level and customer level.

6.3.1 Overall Compliance Determination

For a scan customer to be considered compliant, all components within the customer's cardholder data environment must be compliant. The cardholder data environment includes the entire network infrastructure unless physical or logical network segmentation is in place.

6.3.2 Component Compliance Determination

Generally, to be considered compliant, a component must not contain any vulnerability that has been assigned a CVSS base score equal to or higher than 4.0.

If the NVD does not have a CVSS base score for a vulnerability identified in the component, the scoring of that vulnerability should be performed in accordance with Section 6.3.3 below, "Exceptions to Scoring Vulnerabilities with the NVD."

6.3.3 Exceptions to Scoring Vulnerabilities with the NVD

There are four exceptions to the NVD scoring guidance described in Section 6.3.2 above, "Component Compliance Determination." Only these exceptions may supersede any established CVSS scores. These exceptions must be documented under "Exceptions, False Positives, or Compensating Controls" as noted in Appendix B: ASV Scan Report Summary.

1. **The vulnerability is not included in the NVD.**
   In this case, the ASV must provide its own risk score using the CVSS Calculator and include, where possible, references to other external sources of information about the vulnerability.

2. **The ASV disagrees with the CVSS score noted in the NVD.**
   In this case, the ASV must provide (in addition to all the other required reporting elements for vulnerabilities) the following information:
   - The NVD rating of the vulnerability
   - The ASV's rating of the vulnerability
   - Description of why the ASV disagrees with the NVD rating

   Note: *When re-ranking a vulnerability's risk assignment, ASVs are encouraged to utilize industry-recognized resources (such as the CVSS v3.0 Calculator), rather than arbitrarily or subjectively assigning numbers to vulnerabilities.*

3. **The vulnerability is purely a denial-of-service (DoS) vulnerability.**
   In the case of DoS vulnerabilities (e.g., where the vulnerability has both a CVSS Confidentiality Impact of "None" and a CVSS Integrity Impact of "None"), the vulnerability must not be ranked as a failure.

4. **The vulnerability violates PCI DSS and may be a higher risk than noted in NVD.**
   In this case, the ASV must score the presence of certain types of vulnerabilities as **automatic failures** due to the risk of the vulnerability and the possibility to exploit the cardholder data environment. See Table 1: Required Components for PCI DSS Vulnerability Scanning for examples of vulnerabilities that are considered violations of the PCI DSS and must therefore be scored as **automatic failures**.

7 Scan Reporting

ASVs produce a scan report based on the results of the ASV scan. The scan report describes the type of vulnerabilities or risks, diagnoses the associated issues, and provides guidance on how to fix or patch vulnerabilities. The scan report will assign ratings for vulnerabilities identified in the ASV scan process and must report results in accordance with the PCI DSS external vulnerability scanning requirements and this *ASV Program Guide*.

7.1 Generating, Reading, and Interpreting Scan Reports

The scan report must have the following three sections:

1. **Attestation of Scan Compliance**
2. **ASV Scan Report Summary**
3. **ASV Scan Vulnerability Details**

The Attestation of Scan Compliance and the ASV Scan Report Summary must follow the format in the templates provided in Appendices A and B of this *ASV Program Guide*.

- All of the data elements and supporting text will exactly match that provided in the templates;
- The required information will be presented in an order that exactly matches the provided templates;
- The presentation of information is similar to that which is provided in the templates; and
- All variables (for example, "Customer Name" or "Date") and all fields and check boxes will be completed by the ASV.

There is no required template or format for the ASV Scan Vulnerability Details report. ASVs are permitted to design their own format for this report as long as all content specified in Appendix C of this *ASV Program Guide* is included.

Further detail on the requirements of each section is set out below:

1. Attestation of Scan Compliance

This is the overall summary that shows whether the scan customer's infrastructure met the scan requirements and received a passing scan.

The Attestation of Scan Compliance can be submitted alone – without the ASV Scan Report Summary or ASV Scan Vulnerability Details – or is also the mandatory cover sheet for the ASV Scan Report Summary and/or ASV Scan Vulnerability Details, at acquirer's or Participating Payment Brand's discretion.

Report Customization: *Note that while the use of Appendices A and B are mandatory as templates for the Attestation of Scan Compliance and the ASV Scan Report Summary, some customization of these documents is allowed, such as:*

- *Page orientation of the report (landscape or portrait)*
- *Addition of the ASV's logo*
- *Addition of ASV-specific clauses as long as the added language does not contradict or replace other Appendix A or B language or language within the ASV Program Guide*
- *Font style, sizes, and colors, and page spacing*
- *Placement of information*

While the compliance status indicators (e.g., radio button, checkbox, etc.) must show as green for "pass" and red for "fail," they may be shown as a single button revealing only the relevant compliance status for that item.

2. ASV Scan Report Summary

This section of the scan report lists vulnerabilities by component (IP address, hosts/virtual hosts, domains, FQDN, etc.) and shows whether each component scanned received a passing score and met the scan requirement. This section shows, at minimum, all compliance-impacting vulnerabilities noted for a given component, with one line per vulnerability noted. For example, a component will show one line when only one vulnerability is noted, but will have five lines if five vulnerabilities are noted, etc.

Note: *Unless otherwise specified by the scan customer or the acquirer or Participating Payment Brand, the ASV may choose to omit vulnerabilities that do not impact PCI DSS compliance (for example, Low severity vulnerabilities) from the Summary. However, all compliance-affecting vulnerabilities (for example, automatic failures, Medium and High severity vulnerabilities)—including 1) all failing vulnerabilities that have been fixed, rescanned and validated as passing upon rescan, and 2) failing vulnerabilities that have been changed to "pass" via exceptions or after remediation/rescan—must always be listed in the Summary.*

Consolidated solution/correction plan, provided as a separate line item for each component

- The ASV must provide a high-level description of the remediation that needs to be performed on a particular system—for example, "Apply available patches" or "Update to a vendor-supported OS version." ASVs are permitted to include pointers/links to specific remediation information and guidance that may exist in either a) an appendix to the ASV Scan Report Summary, or b) in the main body of or an appendix to the ASV Scan Report Vulnerability Details.

3. ASV Scan Report Vulnerability Details

This section of the scan report is the overall listing of vulnerabilities that shows compliance status (pass/fail) and details for *all* vulnerabilities detected during the scan.

Vulnerability Details generation and submission

- The ASV Scan Vulnerability Details must be submitted with the Attestation of Scan Compliance cover sheet, and can optionally be submitted with the ASV Scan Report Summary at acquirer's or Participating Payment Brand's discretion.

Vulnerability Detail content – See Appendix C: ASV Scan Report Vulnerability Details for optional template.

- Customer and ASV names (Full contact information does not need to be included here since it is included on the Attestation of Scan Compliance cover sheet.)
- For each vulnerability, all affected components including severity and scoring, industry reference numbers, vulnerability compliance status (pass/fail), detailed explanation, and other information about the vulnerability that the ASV may choose to add.
- List of all detected open ports and, where possible, the service/protocol identified by the ASV.

7.2 Special Notes

Special Notes are to be used to disclose the presence of certain software or configurations that may pose a risk to the scan customer's environment due to insecure implementation rather than an exploitable vulnerability. The requirement for an ASV to utilize a Special Note is identified where applicable in this document. The ASV must complete all fields listed in Appendix B: ASV Scan Report Summary, Part 3b: Special Notes, including the documentation of:

- The scan customer's declared business need for the software.
- The scan customer's declaration that the software is implemented with strong security controls, as well as the details that comprise those controls.
- Actions taken by the scan customer—including removal—to secure the software, as well as the details that comprise those controls.

Note: *The ASV must ensure that an applicable and relevant scan customer declaration is provided for* ***each*** *Special Note before issuing a passing scan report. The ASV must declare a report as FAILED until all applicable scan customer declarations have been obtained and reviewed by the ASV.*

The use of a Special Note does not result in an automatic failure on the scan report, nor does it override any CVSS scoring.

7.3 Scan Customer and ASV Attestations

Before completion of the scan results and generation of the scan report, each ASV must provide a mechanism within its ASV scan solution to capture the following attestations from both the scan customer and the ASV. These attestations (once completed by the scan customer and ASV) are included on the *Attestation of Scan Compliance* cover sheet. ASVs may not use the same *Attestation of Scan Compliance* for multiple quarters. The scan customer attestation must be generated each quarter for the scan(s) identified in the scan report, and must be completed before each scan report is finalized.

Note: *If multiple, failed scans are aggregated to represent one overall passing scan*, an additional Attestation of Scan Compliance cover sheet with a Scan Status of "Pass" may be included by the ASV as a "cover sheet" to represent all partial/failed scans (and each accompanying partial/failed scan's respective Attestation of Scan Compliance cover sheets) for that quarterly period. This would be acceptable as long as each report includes 1) all failing vulnerabilities that have been fixed, rescanned, and validated as passing upon rescan, and 2) all respective failing vulnerabilities that have been changed to "pass" via exceptions or after remediation/rescan.*

* *An example of aggregation would be instead of having a single, environment-wide scan report, the entity may verify it has met the scanning requirements through a collection of scan results, which together show that all required scans are being performed and that all applicable vulnerabilities are being identified and addressed on a quarterly basis—see FAQ 1152 on the Website for additional information.*

The scan customer's attestation includes the following elements:

- Scan customer is responsible for proper scoping of the scans and has included all components in the scan that should be included in the PCI DSS scope.
- Scan customer has implemented network segmentation if any components are excluded from PCI DSS scope.

- Scan customer has provided accurate and complete evidence to support any disputes over scan results.
- Acknowledgement that ASV scan results only indicate whether scanned systems are compliant with the external quarterly vulnerability scan requirement (PCI DSS 11.2.2) and are not an indication of overall compliance with any other PCI DSS requirements.

The ASV's attestation includes the following elements:

- The *ASV Program Guide* and other supplemental guidance from PCI SSC was followed for this scan.
- ASV's practices for this scan included a Quality Assurance process that:
  - Reviews scan customer scoping practices.
  - Detects incorrect, incomplete, inconclusive or corrupt scans.
  - Detects obvious inconsistencies in findings.
  - Reviews and corrects connectivity issues between the scan solution and scan customer.
  - ASV reviewed this scan report and any/all exceptions reported.

7.4 ASV Scan Finalization

A completed ASV scan has one of the following results:

- A passing scan
  - Scan customers only submit passing scan reports (which may be comprised of multiple failed scans to demonstrate all vulnerabilities reported in the initial scan for that quarterly period were addressed).
  - Scan customers submit passing scan reports according to Section 7.9, "Compliance Reporting."
- A failing scan for which the scan customer disputes the results
  - The scan customer and ASV resolve any scan disputes or exceptions according to Section 7.7, "Managing False Positives and Other Disputes."
- A failing scan that the scan customer does not dispute
  - The scan customer resolves failing vulnerabilities according to Section 7.5, "Resolving Failing Scans."
- A failing scan due to scan interference
  - The scan customer and ASV resolve such scan failures according to Section 7.6, "Resolving Inconclusive Scans."

7.5 Resolving Failing ASV Scans

For failing ASV scans, the scan customer uses the following general process until all failing vulnerabilities are corrected and a passing scan is achieved:

- Scan customer corrects noted failing vulnerabilities.
  - Scan customer may seek help from the ASV or other security professional as needed to determine proper corrective actions.

- Scan customer contacts ASV to initiate another scan.
  - If a passing scan is achieved, the scan customer submits results according to Section 7.9, “Compliance Reporting.”
  - For failing scans, scan customer repeats this “Resolving Failing ASV Scans” section.

(See Section 7.3 for more information on aggregating multiple failing scans into a passing scan report.)

7.6 Resolving Inconclusive Scans

For ASV scans that cannot be completed due to scan interference, the scan customer may work with the ASV to implement one or more of the following options until a complete scan is achieved. An inconclusive scan that is left unresolved must be reported by the ASV as a **failed** scan:

1. Scan customer makes proper temporary configuration changes to remove interference during an ASV scan; the scan customer may seek help from a trusted security professional as needed to determine proper temporary configuration changes to be made. Scan customer then contacts ASV to initiate another scan.
2. Scan customer provides the ASV with sufficient written supporting evidence to support their assertion that the scan was not actively blocked. Scan customer and ASV work together to resolve scanning issues and schedule additional scan(s), as necessary, in order for the scans to cover all ports on all applicable systems. Note that if the ASV agrees that a scan was not actively blocked, the ASV may determine that all ports on all applicable systems have been scanned and that additional scans are not necessary.
3. Scan customer and ASV agree on a method that allows the ASV scan solution to complete a scan of all in-scope components without interference. *This method must be operated and managed by the ASV in accordance with all ASV Program requirements*. For example, a secure connection (such as an IPsec VPN tunnel) could be implemented between the ASV and scan customer, or the lab-validated ASV scan solution[3] (such as an appliance or agent) could be installed at the scan customer’s site.

The ASV scan solution must complete a full ASV scan of all external interfaces of the in-scope system components, in accordance with all ASV Program requirements, in order for the scan to be considered complete.

***Note**: Where resolution of inconclusive scans involves ASV personnel, the personnel must be ASV Employees qualified by PCI SSC per Section 3.2, "ASV Employee – Skills and Experience" of the* ASV Qualification Requirements.

If the ASV scan cannot be completed due to scan interference, the ASV must record the ASV scan result as a **failure**, and clearly describe the conditions resulting in an inconclusive ASV scan in the report under “Exceptions, False Positives, or Compensating Controls” as noted in Appendix B: ASV Scan Report Summary.

[3] The ASV scan solution must be the same lab-validated scan solution tested and approved by the PCI SSC for the ASV.

7.7 Managing False Positives and Other Disputes

The scan customer may dispute the findings in the ASV scan report including, but not limited to:

- Vulnerabilities that are incorrectly reported (false positives)
- Vulnerabilities that have a disputed CVSS Base score
- Vulnerabilities for which a compensating control is in place (See Section 7.8, "Addressing Vulnerabilities with Compensating Controls")
- Exceptions in the scan report
- Conclusions of the scan report
- List of components designated by scan customer as segmented from the CDE
- Inconclusive ASV scans or ASV scans that cannot be completed due to scan interference

Note: *Missing security patches that are available to address High or Medium severity vulnerabilities must be installed (or have sufficient compensating controls to mitigate the threat) before a component or scan report can be marked as passing. Lack of an available security patch is not in itself an exception or false positive; High or Medium severity vulnerabilities without an available patch must be secured with compensating control(s) before the component or scan report can be marked as passing.*

The ASV must have a written procedure in place for handling disputes, and the scan customer must be clearly informed on how to report a dispute to the ASV, including how to appeal the findings of the dispute investigation with the ASV. The ASV must explicitly inform the scan customer that disputes in scan results are NOT to be submitted to the PCI SSC.

- The ASV is REQUIRED to investigate false positives with a CVSS Base score at or above 4.0 (failing score).
- The ASV is ENCOURAGED to investigate false positives with a CVSS Base score at or below 3.9 (passing score).
- The ASV is REQUIRED to investigate inconclusive scans disputed by the scan customer.

During dispute investigation the scan customer must:

- Provide written supporting evidence for disputed findings. Scan customers should submit system-generated evidence such as screen captures, configuration files, system versions, file versions, list of installed patches, etc. Such system-generated evidence must be accompanied by a description of when, where and how they were obtained (chain of evidence)
- Attest within the ASV scan solution that the evidence is accurate and complete.

During the dispute investigation the ASV must:

- Determine whether the dispute can be validated remotely (from the ASV) and:
  - If remotely validated, update the scan report.
  - If remote validation is not possible, then the ASV must determine whether the submitted written evidence is sufficient to resolve the dispute. This includes examining the scan customer's evidence for relevance and accuracy. If evidence is sufficient, the ASV updates the scan report accordingly.

- Document the ASV's conclusion and either clearly describe, reference or include the supporting evidence in the report under "Exceptions, False Positives, or Compensating Controls" as noted in Appendix B: ASV Scan Report Summary.
- Not remove disputes from a scan report.
- Not allow the scan customer to edit the scan report.
- Not carry dispute findings forward from one quarterly scan to the next by the ASV. Dispute evidence must be verified and resubmitted by the scan customer, and evaluated again by the ASV, for each quarterly scan.
- Allow evaluation of disputes only by ASV Employees who have been qualified by PCI SSC per Section 3.2, "ASV Employee – Skills and Experience" in the document *Qualification Requirements for Approved Scanning Vendors (ASVs)*.
- Include the name of the ASV Employee who handled each exception within the scan report.

7.8 Addressing Vulnerabilities with Compensating Controls

The scan customer may dispute the results of an ASV scan by stating they have compensating controls in place to reduce or eliminate the risk of a vulnerability identified in the scan report. In this case, the following is required:

- The ASV must assess the relevance and applicability of the compensating controls to meet the risk presented by the vulnerability.
- The ASV's conclusion must be documented in the scan report under "Exceptions, False Positives, or Compensating Controls" as noted in Appendix B: ASV Scan Report Summary.
- The scan customer must not be permitted to edit the scan report.
- The ASV scan must not reduce the search space of any scan by discarding vulnerabilities resolved by compensating controls.

7.9 Compliance Reporting

Scan customers must follow each Participating Payment Brand's respective compliance reporting requirements to ensure each Participating Payment Brand acknowledges an entity's compliance status. Scan reports must be submitted according to each Participating Payment Brand's requirements. Scan customers should contact their acquiring bank or each Participating Payment Brand to determine to whom results should be submitted.

7.10 Report Delivery and Integrity

The ASV scan solution's final scan report must be submitted or delivered in a secure fashion ensuring report integrity with clear demonstration that controls are in place to prevent interception or alteration to the final reports. Scan customers must not have the ability to change or alter the final report.

ASVs must at all times handle scan reports and all associated documentation in accordance with the *ASV Qualification Requirements* section titled "Protection of Confidential and Sensitive Information."

8 Quality Assurance

8.1 ASV's Internal Quality Assurance Program

The ASV must have a Quality Assurance (QA) process to analyze ASV scan results for inconsistencies, verify false positives, record the reporting attestations, and to review the final report before a scan report is submitted to the scan customer.

The ASV must include contact information in each report for inquiries relating to integrity of the specific report. This can be either a generic corporate contact or a named individual per the ASV's discretion. In either case, the individual responsible for responding to inquiries, whether identified as a generic contact or a named individual, must (when so identified and responding) be qualified by PCI SSC per Section 3.2, "ASV Employee – Skills and Experience," of the *ASV Qualification Requirements*.

The ASV must implement a QA process that is designed to detect incomplete, inconclusive or corrupted ASV scans. The ASV's QA process must include at minimum the following features:

- The QA process may be performed automatically or manually. Automatic QA processes must include random sampling of reports for manual review on a regular basis.
- The QA process must detect potential connectivity issues between the scan solution and the target network, including those resulting from link failure or active security measures such as those implemented in active protection systems.
- The QA process must perform basic sanity tests to detect obvious inconsistencies in findings.

8.2 PCI SSC's Quality Assurance Program for ASVs

In accordance with the *ASV Qualification Requirements,* PCI SSC reviews work associated with ASV scan reports for quality assurance purposes. As stated in the *ASV Qualification Requirements* and the ASV Agreement, ASVs are required to meet quality assurance standards set by PCI SSC.

The quality assurance of ASV services and reporting includes annual validation via the ASV Validation Labs Test Bed. Additionally, the ASV may be validated by reviewing the results of scan reports developed for scan customers; PCI SSC may request the results of such scan reports at any time.

PCI SSC has determined that the occurrence of various "Violations" (defined in the ASV Agreement and further described in the *ASV Qualification Requirements*) may warrant (and is grounds for) immediate remediation or revocation of ASV qualification. The list of Violations includes, but is not limited to:

- Intentionally deciding not to scan relevant components.
- Operating a different scan solution or methodology than what was validated during the ASV lab scan test.
- Failure to maintain (and provide evidence to PCI SSC) specified insurance requirements.
- Unqualified professionals operating the ASV scan solution and/or reviewing results.
- Failure to successfully complete annual validation against the ASV Validation Labs Test Bed.

- Misrepresentation of the PCI DSS or supporting documentation to sell products or services, to mislead scan customers or potential clients, to discredit a competitor, or for any other purpose.
- Removing components or applications from scope that may impact cardholder data.
- Independent forensic investigations performed by reputable, qualified experts conclusively demonstrating that cardholder data was compromised, the breach occurred on systems or by system components evaluated by the ASV, and the breach occurred as a direct result of the ASV's failure to properly scan or report the systems or system components.

Refer to the *ASV Qualification Requirements* for additional Violations and requirements.

8.3 Remediation

During remediation, ASVs are still permitted to conduct ASV scans, but scan reports and ASV scanning activity may be monitored by PCI SSC to determine whether the issues under remediation have been mitigated. ASVs are charged remediation fees and may be charged additional fees to cover the costs of monitoring.

The ASV may also be required to submit a remediation plan to PCI SSC detailing how the ASV plans to improve the quality of its performance or ASV scan solution. PCI SSC may also require onsite visits with the ASV to audit the ASV's QA program, at the expense of the ASV.

The ASV qualification of an ASV that remains in remediation without substantial and demonstrable progress on its remediation plan for more than 90 days past its requalification date will be automatically revoked.

See the *ASV Qualification Requirements* for additional details on Remediation.

8.4 Revocation

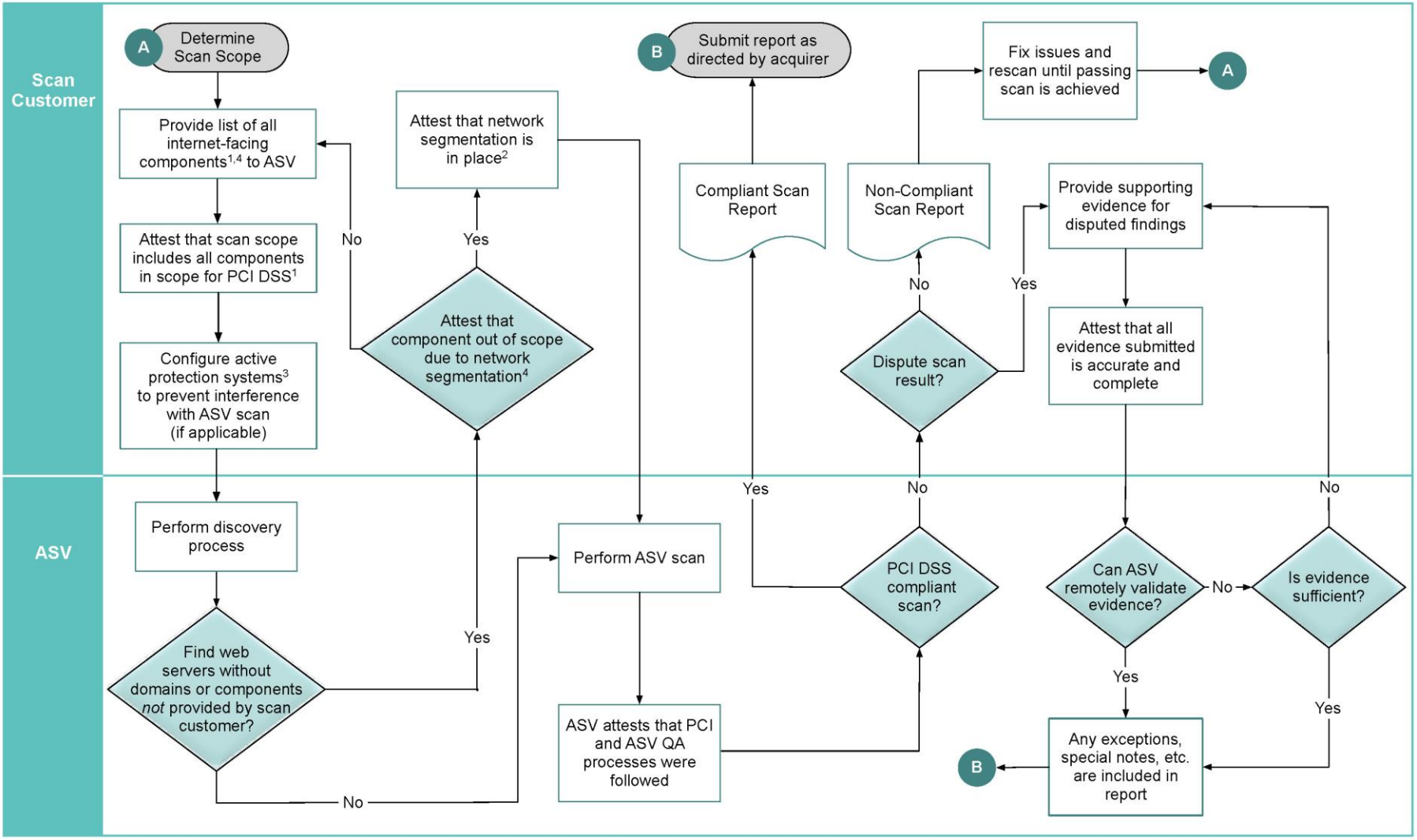
When ASV qualification is revoked, the vendor is removed from the PCI SSC list of Approved Scanning Vendors. Once ASV qualification is revoked, the vendor is no longer authorized to perform scans for the purpose of validating compliance with PCI DSS Requirement 11.2.2 as part of the ASV Program. Vendors may appeal revocation decisions per the ASV Agreement within 30 days of revocation notice, but must meet all ASV Program requirements prior to reinstatement as an ASV.

After a revocation period of at least six (6) months, a vendor can reapply to become an ASV according to the process and fees detailed in Sections 5.3, "ASV Testing and Approval Process" and 5.4 "Fees for ASV Testing and Approval Process" of this document, and the *ASV Qualification Requirements*.

PCI SSC reserves the right to remove a vendor from the list of Approved Scanning Vendors if the ASV is not performing services in accordance with the *ASV Qualification Requirements* or *ASV Program Guide* or otherwise is not in compliance with applicable ASV Program requirements. A revoked ASV will be notified by PCI SSC in accordance with the ASV Agreement.

See the *ASV Qualification Requirements* for additional details on Revocation.

Figure 1: Overview of ASV Scan Processes



1 Scan customers are ultimately responsible for defining the scan scope, though they may seek expertise from QSAs and guidance from ASVs. If an account data compromise occurs via a component not included in the scan, the scan customer is accountable.

2 To reduce the scope of the scan, network segmentation must be in place to isolate system components that store, process, or transmit cardholder data from systems that do not. ASV still reports these components as not scanned due to scan customer attestation that they're out of scope.

3 Active protection systems: Systems that block, filter, drop, or modify network packets in response to scan traffic that is allowed through the firewall—for example, intrusion-prevention systems.

4 Component: IP address, domain, FQDN, web server domain, etc.

Appendix A: ASV Scan Report Attestation of Scan Compliance

A.1 Scan Customer Information		
Company:		
Contact Name:		
Job Title:		
Telephone:	E-mail:	
Business Address:		
City:	State/Province:	ZIP/postal code:
Country:		
Website / URL:		

A.2 Approved Scanning Vendor Information		
Company:		
Contact Name:		
Job Title:		
Telephone:	E-mail:	
Business Address:		
City:	State/Province:	ZIP/postal code:
Country:		
Website / URL:		

A.3 Scan Status			
Date scan completed:		Scan expiration date (90 days from date scan completed):	
Compliance status:	☐ **Pass** ☐ **Fail**	Scan report type:	☐ Full scan ☐ Partial scan or rescan
Number of unique in-scope components[4] scanned:			
Number of identified failing vulnerabilities:			
Number of components found by ASV but not scanned because scan customer confirmed they were out of scope:			

[4] A component includes any host, virtual host, IP address, domain, FQDN or unique vector into a system or cardholder data environment.

A.4 Scan Customer Attestation

(Scan customer name) attests on (date) that this scan (either by itself or combined with multiple, partial, or failed scans/rescans, as indicated in the above Section A.3, "Scan Status") includes all components which should be in scope for PCI DSS, any component considered out of scope for this scan is properly segmented from my cardholder data environment, and any evidence submitted to the ASV to resolve scan exceptions—including compensating controls if applicable—is accurate and complete. (Scan customer name) also acknowledges 1) accurate and complete scoping of this external scan is my responsibility, and 2) this scan result only indicates whether or not my scanned systems are compliant with the external vulnerability scan requirement of PCI DSS; this scan result does not represent my overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

A.5 ASV Attestation

This scan and report was prepared and conducted by (ASV name) under certificate number (insert number), according to internal processes that meet PCI DSS Requirement 11.2.2 and the ASV Program Guide.

(ASV name) attests that the PCI DSS scan process was followed, including a manual or automated Quality Assurance process with customer boarding and scoping practices, review of results for anomalies, and review and correction of 1) disputed or incomplete results, 2) false positives, 3) compensating controls (if applicable), and 4) active scan interference. This report and any exceptions were reviewed by (ASV reviewer name).

Appendix B: ASV Scan Report Summary

Appendix B must be used to create the ASV Scan Report Summary. The ASV Scan Report Summary must be submitted with the Attestation of Scan Compliance cover sheet and can optionally be submitted with the ASV Scan Vulnerability Details at acquirer's or Participating Payment Brand's discretion. See Section 7.1, "Generating, Reading, and Interpreting Scan Reports" for more details.

Part 1. Scan Information			
Scan customer company:		ASV Company:	
Date scan was completed:		Scan expiration date:	

Part 2. Component [4] Compliance Summary			
Component:		**Pass** ☐	**Fail** ☐
Component:		**Pass** ☐	**Fail** ☐
Component:		**Pass** ☐	**Fail** ☐

Part 3a. Vulnerabilities Noted for each Component [4]

ASV may choose to omit vulnerabilities that do not impact compliance from this section, however, failing vulnerabilities that have been changed to "pass" via exceptions or after remediation / rescan must always be listed.

Component	Vulnerabilities Noted per Component [5]	Severity Level [6]	CVSS Score [7]	Compliance Status		Exceptions, False Positives, or Compensating Controls [8] (Noted by the ASV for this vulnerability)
				Pass	Fail	
	Consolidated Solution/Correction Plan for above Component:					
				☐	☐	
	Consolidated Solution/Correction Plan for above Component:					
				☐	☐	

[4] A component includes any host, virtual host, IP address, domain, FQDN or unique vector into a system or cardholder data environment

[5] Include CVE identifier and title and rank in descending order by CVSS score.

[6] High, Medium or Low Severity in accordance with Table 2 of the *ASV Program Guide*.

[7] Common Vulnerability Scoring System (CVSS) base score, as indicated in the National Vulnerability Database (NVD), where available.

[8] Based on the information provided by scan customer, ASV agrees that the Compensating Control is relevant, applicable, and/or appropriate to address the vulnerability.

Part 3a. Vulnerabilities Noted for each Component [4]						
ASV may choose to omit vulnerabilities that do not impact compliance from this section, however, failing vulnerabilities that have been changed to "pass" via exceptions or after remediation / rescan must always be listed.						
Component	**Vulnerabilities Noted per Component [5]**	**Severity Level [6]**	**CVSS Score [7]**	**Compliance Status**		**Exceptions, False Positives, or Compensating Controls [8]** (Noted by the ASV for this vulnerability)
				Pass	**Fail**	
	Consolidated Solution/Correction Plan for above Component:					

Part 3b. Special Notes by Component [4]			
Component	**Special Note [9]**	**Item Noted [10]**	**Scan customer's description of action taken and declaration that software is either implemented securely or removed**

Part 3c. Special Notes – Full Text
Note

Part 4a. Scan Scope Submitted by Scan Customer for Discovery
IP Addresses/ranges/subnets, domains, URLs, etc.

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)
IP Addresses/ranges/subnets, domains, URLs, etc.

[9] Use appropriate text for each Special Note as outlined in Table 1.

[10] Use the appropriate scan component (for example, remote access software, POS software, etc.) as outlined in Table 1.

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)
IP Addresses/ranges/subnets, domains, URLs, etc.

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)
IP Addresses/ranges/subnets, domains, URLs, etc.

Appendix C: ASV Scan Report Vulnerability Details

Appendix C can optionally be used to create the ASV Scan Report Vulnerability Details. However, if the template is not used, each item included herein must be included in the ASV Scan Report Vulnerability Details.

The ASV Scan Vulnerability Details must be submitted with the *Attestation of Scan Compliance* cover sheet, and can optionally be submitted with the *ASV Scan Report Summary* at acquirer's or Participating Payment Brand's discretion. See Section 7.1, "Generating, Reading, and Interpreting Scan Reports," for more details.

Part 1. Scan Information			
Scan Customer Company:		ASV Company:	
Date scan was completed:		Scan expiration date:	

Part 2. Vulnerability Details								
Component [4]	**Detected Open Ports, Services/ Protocols**[11]	**Vulnerability**	**Severity Level** [6]	**CVE Number**	**CVSS Score** [7]	**Compliance Status**		**Details**
						Pass	**Fail**	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	
						☐	☐	

[11] The ASV must list *all detected open ports* and, where possible, the service/protocol identified by the ASV.

Appendix D: ASV Scan Report Summary Example

Appendix B must be used to create the ASV Scan Report Summary. The ASV Scan Report Summary must be submitted with the Attestation of Scan Compliance cover sheet and can optionally be submitted with the ASV Scan Vulnerability Details at acquirer's or Participating Payment Brand's discretion. See Section 7.1, "Generating, Reading, and Interpreting Scan Reports" for more details.

Part 1. Scan Information			
Scan Customer Company:	ABC Industries	ASV Company:	AwesomeScan
Date scan was completed:	1 March, 2018	Scan expiration date:	30 May, 2018

Part 2. Component [4] Compliance Summary		
Component: *w.x.y.*116	**Pass** ☐	**Fail** ☒
Component: *w.x.y.*117, www. company1.com	**Pass** ☒	**Fail** ☐
Component: *w.x.y.*118, www.company1.net	**Pass** ☒	**Fail** ☐
Component: *w.x.y.*119, vpn.company1.com	**Pass** ☒	**Fail** ☐
Component: *w.x.y.*119, remote.company1.com	**Pass** ☒	**Fail** ☐
Component: *w.x.y.*120, mail.company1.com	**Pass** ☒	**Fail** ☐

Part 3a. Vulnerabilities Noted for each Component [4]

ASV may choose to omit vulnerabilities that do not impact compliance from this section, however, failing vulnerabilities that have been changed to "pass" via exceptions or after remediation / rescan must always be listed.

Component	Vulnerabilities Noted per Component [5]	Severity Level [6]	CVSS Score [7]	Compliance Status		Exceptions, False Positives, or Compensating Controls [8] (Noted by the ASV for this vulnerability)
				Pass	Fail	
*w.x.y.*116	CVE-2008-1483 OpenSSH X Connections Session Hijacking Vulnerability	Medium	6.9	☐	☒	
*w.x.y.*116	MySql Detected	NA	NA	☐	☒	
*w.x.y.*116	CVE-2007-2010 bftpd GET/MGET Command File Transfer DoS	Medium	6.8	☒	☐	This is purely a denial-of-service (DoS) vulnerability with both a CVSS Confidentiality Impact of "None" and a CVSS Integrity Impact of "None"

Part 3a. Vulnerabilities Noted for each Component [4]

ASV may choose to omit vulnerabilities that do not impact compliance from this section, however, failing vulnerabilities that have been changed to "pass" via exceptions or after remediation / rescan must always be listed.

Component	Vulnerabilities Noted per Component [5]	Severity Level [6]	CVSS Score [7]	Compliance Status		Exceptions, False Positives, or Compensating Controls [8] (Noted by the ASV for this vulnerability)
				Pass	Fail	
	Consolidated Solution/Correction Plan for above IP Address: All openssh versions shipped in Red Hat Enterprise Linux 5 include the patch for this issue. This issue was fixed in Red Hat Enterprise Linux 4 via: https://rhn.redhat.com/errata/RHSA-2005-527.html Red Hat Enterprise Linux 3 is affected by this issue. The Red Hat Security Response Team has rated this issue as having low security impact. https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2008-1483. Recommend applying vendor patch or upgrading version. Automatic Failure: Open access to databases from the Internet. (Vulnerability is not included in the NVD). Restrict access to databases from the Internet. ASV recommends updating software to latest supported version; Apply all current vendor-issued security patches; Configure system security state (for example, per Center for Internet Security (CIS) Red Hat Enterprise Linux 6 Benchmark version X.Y.Z).					
vpn.company1.com remote.company1.com *w.x.y.*119	CVE-2008-1657 OpenSSH ForceCommand Command Execution Weakness	Medium	6.5	☒	☐	False Positive; RedHat RPL-2419 installed Screen capture provided by *[scan customer name]*, exception validated by *[ASV Employee name]*
	Consolidated Solution/Correction Plan for above Component: Compliance status updated from "fail" to "pass" per exception (false positive) noted above. No additional corrections required for this IP address to achieve a passing scan.					

Part 3b. Special Notes by Component

Component	Special Note [9]	Item Noted [10]	Scan customer's description of action taken and declaration that software is either implemented securely or removed
*w.x.y.*116	HTTP directory listing	Web Server	All HTTP directory listing capabilities have been disabled per vendor support documentation.
*w.x.y.*119	VPN detected	Remote Access Software	The VPN service is essential for conducting business and used to connect remote offices. The VPN service is securely implemented per vendor documentation and uses strong cryptography and authentication in accordance with PCI DSS Requirement 8. Validated by QSA in March 2018.

Part 3c. Special Notes – Full Text

Note

HTTP directory Listing

Note to scan customer: Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.

Part 3c. Special Notes – Full Text
VPN Detected *Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.*

Part 4a. Scope Submitted by Scan Customer for Discovery
IP Addresses/ranges/subnets, domains, URLs, etc.
IP Range: w.x.y.116 – w.x.y.128
Domain: company1.com
Domain: company1.net
URL: www.company1.com/payment

Part 4b. Scan Customer Designated "In-Scope" Components (Scanned)
IP Addresses/ranges/subnets, domains, URLs, etc.
w.x.y.116
w.x.y.117, www. company1.com
w.x.y.118, www.company1.net
w.x.y.119, vpn.company1.com, remote.company1.com
w.x.y.120, mail.company1.com

Part 4c. Scan Customer Designated "Out-of-Scope" Components (Not Scanned)
Requires description for each IP Address/range/subnet, domain, URL
w.x.y.121, artwork.company1.com – Scan customer attests to implementing segmentation via separate physical layer 2 switch with no connectivity to CDE.
w.x.y.122 (not active) – Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.
w.x.y.123 (not active) – Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.
w.x.y.124 (not active) – Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.
w.x.y.125 (not active) – Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.
w.x.y.126 (not active) – Scan customer attests that this IP address is not issued/assigned to any physical or virtual host. ASV confirmed it is nonresponsive.
w.x.y.127, test.company1.com – Scan customer attests to implementing segmentation via separate physical layer 2 switch with no connectivity to CDE.
w.x.y.128, beta.company1.net – Scan customer attests to implementing segmentation via separate physical layer 2 switch with no connectivity to CDE.