



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

Program Guide

Version 2.0

May 2013

Document Changes

Date	Version	Description
February 11, 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.

Table of Contents

Document Changes	2
Approved Scanning Vendor Program Guide – Introduction	4
Related Publications	4
Updates to Documents and Security Requirements	4
Terminology	5
About PCI SSC	6
PCI DSS Alignment Initiative and Overview	6
Roles and Responsibilities	6
Payment Brands	7
PCI SSC	7
Approved Scanning Vendors	7
Qualified Security Assessors (QSAs)	8
Scan Customers	8
Scan Process Overview	9
PCI DSS Requirement 11.2	10
Can a Merchant or Service Provider Perform Their Own External Vulnerability Scanning?	11
Fees	11
Scanning Vendor Testing and Approval Process	11
Fees for Scanning Vendor Testing and Approval Process	12
ASV Scan Scope Definition	12
Scope and Network Segmentation	12
Internet Service Providers and Hosting Providers	13
ASVs Confirm Scope and List Additional Components Identified During “Discovery”	13
ASV Scan Interference	14
ASV Scan Solution – Required Components	16
General Characteristics	16
Table 1: Required Components for PCI DSS Vulnerability Scanning	17
Vulnerability Reporting	22
Vulnerability Categorization	22
Table 2: Vulnerability Severity Levels Based on the NVD and CVSS Scoring	23
Compliance Determination – Overall and by Component	23
Scan Reporting	24
Special Notes	24
Generating, Reading, and Interpreting Scan Reports	24
Scan Customer and ASV Attestations	26
Scan Customer Attestation	27
ASV Attestation	27
Scan Finalization	27
Resolving Failing Scans	28
Resolving Inconclusive Scans	28
Managing False Positives and Other Disputes	28
Addressing Vulnerabilities with Compensating Controls	29
Compliance Reporting	30
Report Delivery and Integrity	30
Quality Assurance	31
ASV’s Internal Quality Assurance Program	31
PCI SSC’s Quality Assurance Program for ASVs	31
Remediation	32
Revocation	32
Figure 1: Overview of ASV Processes	33
Appendix A: ASV Scan Report Attestation of Scan Compliance	34
Appendix B: ASV Scan Report Executive Summary	35
Appendix C: ASV Scan Report Vulnerability Details	37
Appendix D: Remote Access Security Features	38

Approved Scanning Vendor Program Guide – Introduction

This Approved Scanning Vendor (ASV) Program Guide explains the purpose and scope of Payment Card Industry Data Security Standard (PCI DSS) external vulnerability scans for merchants and service providers undergoing scans as part of validating PCI DSS compliance, and also provides guidance and requirements for ASVs who perform these scans.

Note: *The requirements in this document apply specifically to the quarterly EXTERNAL vulnerability scans required by PCI DSS Requirement 11.2.2. The 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.*

Related Publications

Requirement 11.2 of the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures* requires quarterly external vulnerability scans, which must be performed by ASV. The PCI DSS provides the foundation for this and all other PCI DSS-related requirements and procedures.

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) Data Security Standard ASV Validation Requirements*

Note:

The PCI DSS Requirements and Security Assessment Procedures list the specific technical requirements and provide the assessment procedures and template used by merchants and service providers to validate PCI DSS compliance and document the review. PCI DSS Requirement 11.2.2 specifically requires quarterly external vulnerability scans that must be performed by an ASV. The ASV Validation Requirements defines the requirements that must be met by an ASV in order to perform PCI DSS quarterly external vulnerability scans.

All documents are available in electronic form on www.pcisecuritystandards.org.

Updates to Documents and Security Requirements

Security is a never-ending race against potential threats. As a result, it is necessary to regularly review, update and improve the PCI DSS. As such, PCI SSC will update PCI DSS requirements according to PCI SSC's defined three-year lifecycle process. The *ASV Program Guide* is expected to change when threats evolve or as necessary to incorporate changes in PCI DSS.

PCI SSC reserves the right to change, amend or withdraw PCI DSS and/or ASV requirements at any time, and will work closely with its community of Participating Organizations regarding such changes. The final published version of this document supersedes the following PCI DSS supporting documents:

- *ASV Program Guide 1.0*

ASVs must implement the requirements set forth in this document effective immediately since no changes in this document require changes to the ASVs' scanning solution.

Terminology

Note that throughout this document, the following terms shall have meanings shown in the chart below.

Term	Meaning
ASV (Approved Scanning Vendor)	Refers to a company that has been approved by PCI SSC to conduct external vulnerability scanning services in accordance with PCI DSS Requirement 11.2.2. Refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.
ASV scan solution	Refers to a set of security services and tool(s) offered by an ASV to validate compliance of a scan customer with the external vulnerability scanning requirement of PCI DSS Requirement 11.2.2. The scanning solution includes the scanning procedures, the scanning tool(s), the associated scanning report, the process for exchanging information between the scanning vendor and the scan customer, and the processes used by qualified ASV employees to: <ul style="list-style-type: none"> • Operate the ASV scan solution • Submit the scan report to the scan customer • Review and interpret scan results, as needed
CDE (Cardholder Data Environment)	Refers to the cardholder data environment as defined in the PCI DSS. Refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.
CVE (Common Vulnerabilities and Exposures)	Refers to a publicly available and free-to-use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.
CVSS (Common Vulnerability Scoring System)	Refers to the latest version of an open framework for communicating the characteristics and impacts of IT vulnerabilities.
External scan	Refers to 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	Refers to 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)	Refers to the National Institute of Standards and Technology (NIST) National Vulnerability Database for known vulnerabilities and vulnerability details.
Payment brands	Refers to the payment card brands that are statutory members of PCI SSC, currently American Express Travel Related Services Company, Inc., Discover Financial Services LLC, JCB Advanced Technologies, Inc., MasterCard International Incorporated, and Visa Holdings, Inc.
PCI DSS	Refers to the then-current version of the <i>Payment Card Industry (PCI) Data Security Standard</i> , as available through the Website (defined below).
PCI SSC	Refers to the PCI Security Standards Council, LLC.
QSA (Qualified Security Assessor)	Refers to an assessor company that has been qualified and trained by PCI SSC to perform PCI DSS assessments. Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.
Scan Customer	Refers to a merchant or service provider who undergoes a quarterly external vulnerability scan via an ASV, either through a relationship with an ASV, or through a relationship between a scan customer's acquirer and an ASV.

Term	Meaning
Scan interference	Refers to 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 scanning solution would no longer see what an attacker would see.

Both NVD and CVE are sponsored by the [National Cyber Security Division](#) of the [U.S. Department of Homeland Security](#).

About PCI SSC

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

All stakeholders in the payments value chain benefit from the aligned requirements:

- Customers benefit from a broad selection of ASVs.
- Customers are assured that they will be using ASV scan solutions that have met the required level of validation.

For more information regarding PCI SSC, see the PCI SSC’s website at www.pcisecuritystandards.org (“the Website”).

PCI DSS Alignment Initiative and Overview

The Payment Card Industry has initiated a collaborative effort to address common industry security requirements, including the security of merchants’ and service providers’ cardholder data environments. The creation of PCI DSS to secure cardholder data represents an effort to standardize security requirements relevant to protection of cardholder data environments used to store, process, or transmit cardholder data. PCI DSS Requirement 11.2.2 requires that external vulnerability scanning be performed quarterly by an ASV qualified by PCI SSC. The ASV Program Guide reflects an alignment of the payment brands’ requirements to a standard set of:

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

Note:

The ASV prepares scan reports according to the ASV Scan Report requirements and submits reports to the scan customer. The scan customer submits reports to their acquirers or payment brands as directed by the payment brands.

Roles and Responsibilities

There are several stakeholders in the payment community. Some of these stakeholders—ASVs, QSAs, and PCI SSC—have a more direct participation in the PCI DSS assessment process. Other stakeholders that are not directly involved with the assessment process should be aware of the overall process to facilitate their associated business decisions.

The following defines the roles and responsibilities of the stakeholders in the payment community. Those stakeholders that are involved in the assessment process have those related responsibilities listed.

Payment Brands

In relation to the PCI DSS, the payment brands develop and enforce 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

PCI SSC

PCI SSC maintains the PCI DSS and related PCI standards, including the PA-DSS. In relation to the ASV program, PCI SSC:

- Approves and trains ASVs to perform PCI DSS external vulnerability scans in accordance with PCI DSS and the PCI DSS Security Scanning Vendor Testing and Approval Processes, and qualifies, trains, and lists Approved Scanning Vendors on the Website
- Maintains and updates PCI DSS and related documentation (including this ASV Program Guide) according to a standards life cycle management process
- Maintains a quality assurance program for ASVs

Approved Scanning Vendors

An ASV is an organization with a set of security services and tools (“ASV scan solution”) to validate adherence to the external scanning requirement of PCI DSS Requirement 11.2.2. The scanning vendor’s ASV scan solution is tested and approved by PCI SSC before an ASV is added to PCI SSC’s *List of Approved Scanning Vendors*.

ASVs are responsible for the following:

- Performing external vulnerability scans in accordance with PCI DSS Requirement 11.2.2, and in accordance with this document and other supplemental guidance published by the PCI SSC
- Maintaining security and integrity of systems and tools used to perform scans
- Making reasonable efforts to ensure scans:
 - Do not impact the normal operation of the scan customer environment
 - Do not penetrate or intentionally alter the customer environment
- Scanning all IP ranges and domains provided by scan customer to identify active IP addresses and services
- Consulting with the scan customer to determine if IP addresses found, but not provided by the scan customer, should be included
- Providing a determination as to whether the scan customer’s components have met the scanning requirement
- 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 the ASV Scan Report Attestation of Scan Compliance cover sheet (called hereafter Attestation of Scan Compliance) and the scan report in accordance with the acquirer or payment brand instructions
 - Including required scan customer and ASV company attestations in the scan report as required by this document
- Retaining scan reports and related work products for 2 years, as required by the *Validation Requirements for Approved Scanning Vendors*
- Providing the scan customer with a means for disputing findings in the scan report

- Maintaining an internal quality assurance process for ASV efforts in accordance with this document and other supplemental guidance published by the PCI SSC

Qualified Security Assessors (QSAs)

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

- Performing PCI DSS assessments in accordance with the *PCI DSS Requirements and Security Assessment Procedures*, which includes confirming that PCI DSS Requirement 11.2 is “in place”
- Providing an opinion about whether the assessed entity meets PCI DSS requirements
- Providing adequate documentation within the Report on Compliance (ROC) to demonstrate the assessed entity’s compliance with 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 QSA efforts

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

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 Council’s website to conduct quarterly external vulnerability scanning according to PCI DSS Requirement 11.2.2 and this document
- Perform due diligence in the ASV selection process, per the scan customer’s due-diligence processes, to obtain assurance as to the ASV’s level of trust to perform scanning services
- To the degree deemed appropriate by the scan customer, monitor 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 conduct a full scan
 - Implementing proper network segmentation for any excluded external-facing IP addresses

See the section titled *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 the section entitled *ASV Scan Interference*.
 - Coordinating with the ASV if the scan customer has load balancers in use. See the section entitled *Account for Load Balancers*.
- Coordinating with the scan customer’s Internet service provider (ISP) and/or hosting providers to allow ASV scans. See the section entitled *Internet Service Providers and Hosting Providers*.
- Attesting to proper scoping and network segmentation (if IP addresses are excluded from scan scope) within the ASV solution
- Providing sufficient documentation to the ASV to aid the ASV’s investigation and resolution of disputed findings, such as suspected false positives, and providing related attestation within an ASV solution

- Reviewing the scan report and correcting any noted vulnerabilities that result in a non-compliant scan
- Arranging with ASV to re-scan any non-compliant systems to verify that all high severity and medium severity vulnerabilities have been resolved, to obtain a passing quarterly scan
- Submitting the completed ASV scan report to the scan customer's acquirer or payment brands, as directed by the payment brands
- Providing feedback on ASV performance in accordance with the ASV Feedback Form

Scan Process Overview

The PCI DSS details security requirements for merchants and service providers that store, process, or transmit cardholder data. To demonstrate compliance with the PCI DSS, merchants and service providers may be required to have periodic PCI DSS vulnerability scans conducted as defined by each payment brand, 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. Scans help identify vulnerabilities and misconfigurations of websites, applications, and information technology infrastructures with Internet-facing Internet protocol (IP) addresses.

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

PCI DSS external vulnerability scans may apply to all merchants and service providers with Internet-facing IP addresses. Even if an entity does not offer Internet-based transactions, other services may make systems Internet accessible. Basic functions such as Email and employee 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 in accordance with PCI DSS must comply with the requirements set forth in this document as well as the Validation Requirements for Approved Scanning Vendors (ASVs), and must successfully complete the PCI Security Scanning Vendor 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.*

Compliance with the 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.

Refer to the flowchart at 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

PCI DSS Requirement 11.2

PCI DSS Requirement	Testing Procedures
<p>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).</p> <p>Note: <i>It is not required that four passing quarterly scans must be completed for initial PCI DSS compliance 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. For subsequent years after the initial PCI DSS review, four passing quarterly scans must have occurred.</i></p>	<p>11.2 Verify that internal and external vulnerability scans are performed as follows:</p>
<p>11.2.1 Perform quarterly internal vulnerability scans.</p>	<p>11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period.</p> <p>11.2.1.b Review the scan reports and verify that the scan process includes rescans until passing results are obtained, or all “High” vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.</p> <p>11.2.1.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).</p>
<p>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).</p> <p>Note: <i>Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), qualified by the Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by internal staff.</i></p>	<p>11.2.2.a Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly scans occurred in the most recent 12-month period.</p> <p>11.2.2.b Review the results of each quarterly scan to ensure that they satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).</p> <p>11.2.2.c Review the scan reports to verify that the scans were completed by an Approved Scanning Vendor (ASV) approved by the PCI SSC.</p>
<p>11.2.3 Perform internal and external scans after any significant change.</p> <p>Note: <i>Scans conducted after changes may be performed by internal staff.</i></p>	<p>11.2.3.a Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.</p> <p>11.2.3.b Review scan reports and verify that the scan process includes rescans until:</p> <ul style="list-style-type: none"> • For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS, and • For internal scans, a passing result is obtained or no vulnerabilities exist ranked greater than “High” per PCI DSS Requirement 6.2 <p>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).</p>

Can a Merchant or Service Provider Perform Their Own External Vulnerability Scanning?

Merchants and service providers must use only PCI SSC Approved Scanning Vendors (ASVs) to perform the quarterly external vulnerability scans required by PCI DSS Requirement 11.2.2, and an ASV scan solution must be executed and 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 IP addresses are to be scanned. However, only an authorized ASV employee is 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 reinterpret any results.

Fees

All fees and dates related to the ASV's scanning services are typically negotiated between the ASV and the scan customer. The scan customer either pays all fees directly to the ASV, or may pay fees 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).

Scanning Vendor Testing and Approval Process

The ASV qualification process consists of three parts, which are conducted in the following order:

1. Qualification of the company
2. Qualification of the company's employees responsible for scanning services
3. Security Testing of the company's scanning solution

For more information about qualifying the company and the company's employees (Steps 1 and 2 above), refer to the *Validation Requirements for Approved Scanning Vendors (ASVs)* located at [the Council's website](#).

After completing the qualification process for the scanning company and employees responsible for scanning services, and each year thereafter, as outlined in the *Validation Requirements for Approved Scanning Vendors (ASVs)* found at the Council's website, the company's scanning solution is thoroughly tested in an ASV Validation Lab (the "ASV Test Bed") to ensure the scanning solution performs in accordance with this document. The steps for an ASV to prepare for Scanning Vendor Testing are as follows:

1. The scanning vendor ensures that the scanning solution meets all the requirements in this document, including the reporting requirements.
2. The scanning vendor notifies PCI SSC at asv@pcisecuritystandards.org that the scanning vendor is ready to be tested.
3. The PCI SSC notifies the scanning vendor to schedule the test, and provides the scanning vendor with instructions for the ASV Portal.
4. The scanning vendor submits a request for solution testing via the ASV Portal.
5. Once the submission is received by PCI SSC via the ASV Portal, PCI SSC will assign the scanning vendor to one of the ASV Validation Labs.
6. Once assigned to an ASV Validation Lab, the scanning vendor will receive notification directly from the ASV Validation Lab with the next steps in the process for scheduling the test.

Note: *Scanning Vendor Testing via the ASV Test Bed is an annual requirement.*

Note: *The full ASV scan solution tested and approved by the PCI SSC as part of the PCI DSS Security Scanning Vendor Testing and Approval Processes is the ONLY version that the ASV is allowed to use to*

perform external vulnerability scans. Significant modifications to the tested and approved ASV scan solution are prohibited. However, minor modifications that enhance or improve the quality of the scan solution are acceptable. These minor improvements 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 and fault tolerance (new scan engines, data center expansion)

Fees for Scanning Vendor Testing and Approval Process

Fees will be charged for the various testing stages in accordance with the PCI SSC Programs Fee Schedule. Please refer to the Council’s website for the current fee schedule.

ASV Scan Scope Definition

For the purpose of ASV scanning, the PCI DSS requires 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, as well as any externally facing system component that provides a path to the cardholder data environment.

The scan customer is ultimately responsible for defining the appropriate scope of the external vulnerability scan and must provide all Internet-facing 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, the scan customer is responsible.

Note: In the context of PCI DSS, “System components” are defined as any network component, server, or application that is included in or connected to the cardholder data environment. “System components” also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. The cardholder data environment is comprised of people, processes and technology that store, process or transmit cardholder data or sensitive authentication data. Network components include, but are not limited to: firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: web, application, database, authentication, mail, proxy, network time protocol (NTP), and Domain Name System (DNS). Applications include all purchased and custom applications, including internal and external (for example, Internet) applications.

Scope and Network Segmentation

Scan customers may use segmentation to reduce the scope of the ASV scanning. In general, the following segmentation methods can be used to reduce the scope of the ASV scan:

- Provide physical segmentation between the segment handling cardholder data and other segments
- Employ appropriate logical segmentation where traffic is prohibited between the segment or network handling cardholder data and other networks or segments

Note: The scan customer attests to their scan scope in the ASV Scan Tool prior to the ASV finalizing the scan report.

Scan Customers Provide Internet-facing IP Addresses and Domains

In addition to providing all external-facing IP addresses, the scan customer must also supply all fully qualified domain names (FQDN) and other unique entryways into applications for the entire in-scope infrastructure.

This includes, but is not limited to:

- Domains for all 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 domains or domain aliases

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).

For ISPs, scan customers need to coordinate with them to allow the ASV scan to be performed without interference from active protection systems. For more details, see the section entitled "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. Components commonly hosted by third-party providers include but are not limited to DNS servers, email and web servers, application servers, etc.

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

- 1) The hosting provider can undergo ASV scans on their own and provide evidence to their customers to demonstrate their compliant scans; or,
- 2) The hosting provider can undergo ASV scans as part of each of their 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 appropriate ASV scan.

Note: If the hosting provider has all Internet-facing IP ranges AND all scan customers' domains 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.

ASVs Confirm Scope and List Additional Components Identified During "Discovery"

ASVs must minimally perform the below actions to identify if any scoping discrepancies exist in the information provided by the customer. Information about any scoping discrepancies must be indicated on the Attestation of Scan Compliance cover sheet (see *Appendix A*) under heading "Number of components found by ASV but not scanned because scan customer confirmed components were out of scope." This information should NOT be factored into the compliance status:

- Include any IP address or domain previously provided to the ASV and still owned by the customer that has been removed at the request of the customer.
 - If the customer no longer owns or has custody of the IP address/domain, include that IP address or domain for at least one additional quarter after it was removed from scope or released by the customer.
- For each domain provided, look up the IP address of the domain to determine if it was already provided by the customer.
- For each domain provided, perform a DNS forward lookup of common host-names—such as "www," "mail," etc.—that were not provided by the customer.

- Identify any IPs found during MX record DNS lookup.
- Identify any IPs outside of scope reached via web redirects from in-scope web servers (includes all forms of redirect including: JavaScript, Meta redirect and HTTP codes 30x).
- Match domains found during crawling to user-supplied domains to find undocumented domains belonging to the customer.

ASV Scan Interference

If an ASV detects that an active protection system has blocked or filtered a scan, then the ASV is required to handle it in accordance with the *Resolving Inconclusive Scans* section of this document. 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.

Being able to detect all vulnerabilities is part of the “defense-in-depth” approach of PCI DSS. If the scan cannot detect vulnerabilities on Internet-facing systems because the 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 the *Resolving Inconclusive Scans* section of this document.

Temporary configuration changes may need to be made by the scan customer to remove interference during a scan

Due to the remote nature of external vulnerability scans and the need mentioned above to conduct a scan without interference from an active protection system, 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 that, per above, 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 IP addresses 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 scans—as follows:

- Agree on a time for the scan window each quarter to minimize how long changed configurations are in place.
- Conduct the 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 it comes right after attack traffic)
- Reapply the previous configurations as soon as the 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 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 a 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 a log 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 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 scan is allowed to complete. The intent is that the ASV be provided the same network level view as an actual attacker.*

ASV Scan Solution – Required Components

General Characteristics

The ASV scan solution must have the following characteristics:

- **Be Non-disruptive**

Solutions 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. Root-kits or other software must not be installed unless part of the solution and pre-approved by the 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 a password lockout
- 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. The ASV scan solution must also perform a port scan on 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) and chat 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 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 scanning solution should also, where possible, determine the protocol and service/application version running on each open port. Since services may sometimes run on non-standard ports, the ASV scanning 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. Each platform has strengths and weaknesses. The ASV 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 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.”

(Special Notes do not cause a scan failure or supersede any established CVSS scoring.)

- **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 tools 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.

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, etc.

Scan Components	For Scan Customers	For ASVs
	Why must it be scanned?	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	The ASV must scan all filtering devices such as firewalls and external routers (if used to filter traffic). If a firewall or router is used to establish a demilitarized zone (DMZ), these

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
	<p>which patches are periodically released.</p> <p>Another common problem with firewalls and routers is inadequate configuration.</p> <p>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.</p>	<p>devices must be included.</p> <p>The ASV scan solution must test for known vulnerabilities and determine whether the firewall or router is adequately patched.</p>
Operating Systems	<p>An operating system (OS) sits between hardware and applications.</p> <p>Malicious individuals exploit operating system vulnerabilities to gain access to applications and internal databases that potentially store, process or manage access to cardholder data.</p> <p>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.</p>	<p>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.</p>
Database Servers	<p>Database servers store and manage access to cardholder data.</p> <p>Malicious individuals exploit vulnerabilities in these servers to gain access to cardholder data.</p> <p>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.</p>	<p>The ASV scanning solution must be able to detect open access to databases from the Internet. This configuration is a violation of PCI DSS section 1.3.7, and must be marked as an automatic failure by the ASV. The ASV scanning solution must also be able to detect and report on known database exploits and vulnerabilities.</p>
Web Servers	<p>Web servers allow Internet users to view web pages, interact with web merchants, and conduct online web transactions.</p> <p>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.</p> <p>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.</p> <p>Because these servers are accessible from the public Internet, scanning for vulnerabilities is essential.</p>	<p>The ASV scanning solution must be able to test for all known vulnerabilities and configuration issues on web servers. New exploits are routinely discovered in web server products. The ASV scanning solution must be able to detect and report known vulnerabilities.</p> <p>The ASV scanning solution must be able to scan the website and verify that directory browsing is not possible on the server.</p> <p>Positive identification of directory browsing must be disclosed with the following Special Note.</p> <ul style="list-style-type: none"> ▪ <i>“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.”</i>

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
Application Server	<p>Application servers act as the interface between the web server and other systems, such as back-end databases. For example, when cardholders share account numbers with merchants or service providers, the application server provides the functionality to transport data in and out of the secured network.</p> <p>Malicious individuals exploit vulnerabilities in these servers and their scripts to gain access to applications or internal databases that potentially store, process or manage access to cardholder data.</p> <p>Some website configurations do not include application servers; the web server itself is configured to act as an application server. These servers are called web application servers.</p>	<p>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.</p>
Common Web Scripts	<p>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).</p>	<p>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.</p>
Built-in Accounts	<p>Built-in, or default accounts and passwords, are commonly used by hardware and software vendors to allow the customer initial access to the product.</p> <p>These accounts may have no password or have passwords assigned by the vendor. These default accounts and passwords 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 if not needed.</p> <p>Note: <i>PCI DSS Requirement 2.1 stipulates that vendor-supplied defaults, including vendor accounts and passwords, are changed before installing a system on a network.</i></p>	<p>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:</p> <ul style="list-style-type: none"> ▪ 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 and passwords. Any such vulnerability must be marked as an automatic failure by the ASV. ▪ Report on services that are available without authentication (e.g., without usernames or passwords).
DNS Servers	<p>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.</p>	<p>The ASV scan solution must be able to detect the presence of a DNS server and detect any known vulnerability and configuration issues, including unrestricted DNS zone transfer (which must be marked as an automatic failure by the ASV).</p>
Mail Servers	<p>Mail servers typically exist in the DMZ and can be vulnerable to attacks by malicious individuals. They are a critical element to maintaining overall website security.</p>	<p>The ASV scan solution must be able to detect the presence of a mail server and detect any known vulnerability and configuration issues.</p>

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
Web Applications	<p>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.</p> <p>Malicious individuals frequently attempt to exploit web application vulnerabilities to gain access to applications or internal databases that may process, store, or manage access to cardholder data.</p>	<p>The ASV scan solution must be able to detect via automated or manual means the following application vulnerabilities and configuration issues:</p> <ul style="list-style-type: none"> ▪ 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: <ul style="list-style-type: none"> • 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.)
Other Applications	<p>Other applications, such as those for streaming media, RSS feeds, proxy servers, media content, etc., are exploited by malicious individuals to gain access to cardholder data that may be processed or accessed by these applications.</p>	<p>The ASV scan solution must be able to detect the presence of other applications and to detect any known vulnerability and configuration issues.</p>
Common Services	<p>Many common services present by default on servers have known vulnerabilities which malicious individuals can exploit to gain access to the network. These common services should either be disabled or patched to properly protect the systems.</p>	<p>The ASV scan solution must be able to detect common services known to have vulnerabilities.</p>
Wireless Access Points	<p>Wireless networks introduce new information security risks to those companies that deploy them. Wireless networks, if not securely configured, allow malicious individuals an easy way to eavesdrop on traffic, capture data and passwords, and gain access to a network from, for example, a store parking lot. Wireless vulnerabilities and security misconfigurations should be identified and corrected.</p>	<p>The ASV scan solution must scan detected wireless access points visible from the Internet (over the wire) and detect known vulnerabilities and configuration issues.</p>
Backdoors	<p>A backdoor is a malicious software application that is commonly known in hacker communities. This malicious software should be identified and eliminated.</p>	<p>The ASV scan solution must detect and report well-known, remotely detectable backdoor applications installed on the servers. The presence of any such malware, including rootkits, backdoors, or Trojan horse programs must be marked as an automatic failure by the ASV.</p>

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
SSL/TLS	<p>The SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols provide encryption and integrity for data during transit over a network. There are well-known and easily exploitable vulnerabilities affecting SSL version 2.0 and earlier, which allow for interception or modification of encrypted data during transit. There are also vulnerabilities (“forced downgrade” attacks) which can trick an unsuspecting client into downgrading to the less secure SSL 2.0 when both client and server support newer, more secure versions of the protocol along with SSL 2.0 for backwards compatibility reasons.</p> <p>Per PCI DSS, strong cryptography and security protocols must be deployed and SSL v3.0/TLS v1.0 is the minimum standard.</p>	<p>The ASV scan solution must:</p> <ul style="list-style-type: none"> ▪ Detect the presence of SSL/TLS on a component or service along with the supported SSL/TLS protocol versions ▪ Detect the supported encryption algorithms and encryption key strengths in all SSL/TLS-enabled services ▪ Detect the signature-signing algorithms used for all SSL/TLS 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. <p>Note: <i>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.</i></p> <p>A component must be considered non-compliant and marked as an automatic failure by the ASV if it supports SSL version 2.0 or older OR if SSL v3.0/TLS v1.0 with 128-bit encryption is supported in conjunction with SSL v2.0 (due to the risk of “forced downgrade” attacks described to the left).</p>
Remote Access	<p>Often remote access software is visible to the Internet and not established securely. Sometimes the presence of this software is not needed for business purposes or may not be known to the scan customer. In some cases, these tools are used by software vendors or resellers/integrators to provide support for payment applications. 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. Remote access software is a path frequently used for cardholder data compromises.</p>	<p>The ASV scan solution must be able to detect the presence of remote access software and detect any known vulnerability or configuration issues.</p> <p>Remote access software includes, but is not limited to: VPN (IPSec, PPTP, SSL), pcAnywhere, VNC, Microsoft Terminal Server, remote web-based administration, SSH, and Telnet.</p> <p>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:</p> <ul style="list-style-type: none"> ▪ <i>“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 per Appendix D of the ASV Program Guide, or 2) confirm it is disabled/removed. Consult your ASV if you have questions about this Special Note.”</i>

	For Scan Customers	For ASVs
Scan Components	Why must it be scanned?	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.	<p>If the ASV scan solution detects point-of-sale (POS) software, the following note should be included in the Special Notes section of the scan report:</p> <ul style="list-style-type: none"> ▪ <i>“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.”</i>

Vulnerability Reporting

To demonstrate compliance, a scan must not contain high or medium severity vulnerabilities, or any vulnerability that indicates features or configurations that are in violation of PCI DSS. If these 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.

Vulnerability Categorization

To assist 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 in the next page.

Whenever possible, ASVs must use two tools to categorize and rank vulnerabilities, and determine 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, which is maintained by the National Institute of Standards and Technology (NIST). The NVD contains details of known vulnerabilities based on the 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 a common vulnerability database and scoring authority (the NVD) is intended to provide consistency across ASVs.

With a few exceptions (see the *Compliance Determination—Overall and by Component* section below for details), any vulnerability with a CVSS base score of 4.0 or higher will result in a non-compliant scan, 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 Scoring

CVSS Score	Severity Level	Scan Results	Guidance
7.0 through 10.0	High Severity	Fail	To achieve a passing scan, these vulnerabilities must be corrected and the affected systems must be re-scanned after the corrections (with a report that shows a passing scan). Organizations should take a risk-based approach to correct these types of vulnerabilities, starting with the most critical (rated 10.0), then those rated 9, followed by those rated 8, 7, etc., until all vulnerabilities rated 4.0 through 10.0 are corrected.
4.0 through 6.9	Medium Severity	Fail	
0.0 through 3.9	Low Severity	Pass	While passing scan results can be achieved with vulnerabilities rated 0.0 through 3.9, organizations are encouraged, but not required, to correct these vulnerabilities.

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.

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.

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 “Exceptions to Scoring Vulnerabilities with the NVD” below.

Exceptions to Scoring Vulnerabilities with the NVD

There are four exceptions to the NVD scoring guidance described above in the preceding section titled *Component Compliance Determination*. Only these exceptions may supersede any established CVSS scores. Document these exceptions under “Exceptions, False Positives, or Compensating Controls” as noted in *Appendix B: ASV Scan Report Executive Summary*.

1. **The vulnerability is not included in the NVD.** In this case, the ASV must provide its own risk score using the CVSS scoring system 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
 - Why the ASV disagrees with the NVD rating

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.** The ASV scan solution 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 which are considered violations of the PCI DSS and must therefore be scored as **automatic failures**.

Scan Reporting

ASVs produce an informative report based on the results of the network scan:

- Appendices A and B are required templates for the Attestation of Scan Compliance cover sheet and the ASV Scan Executive Summary.
- Appendix C for the ASV Scan Vulnerability Details provides a suggested format, but ASVs may use a different format as long as the format is easy to read, contains all of the required elements, and has been approved by the PCI SSC as part of the ASV validation process.

The scan report describes the type of vulnerability or risk, diagnoses the associated issues, and provides guidance on how to fix or patch vulnerabilities. The report will assign a rating for vulnerabilities identified in the scan process.

Table 2 above describes how an ASV scan solution categorizes vulnerabilities and demonstrates the types of vulnerabilities and risks that are considered high or medium severity.

Special Notes

Special Notes are to be used to disclose the presence of certain software 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 Executive Summary*, Part 3b: Special Notes by IP Address, 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
- Any action taken by the scan customer, including removal, to secure the software, as well as the details that comprise those controls

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

Generating, Reading, and Interpreting Scan Reports

After conducting a scan, the ASV produces a report with findings and recommendations. The report must assess compliance with the PCI DSS external vulnerability-scanning requirement and provide the following types of reports:

1. Attestation of Scan Compliance cover sheet—an overall summary for the entire customer infrastructure, and the required cover sheet for the reports below. See *Appendix A: ASV Scan Report Attestation of Scan Compliance* for template and required format.
2. ASV Scan Executive Summary—a component summary for each scanned component. See *Appendix B: ASV Scan Report Executive Summary* for template and required format.
3. ASV Scan Vulnerability Details—vulnerability details for each scanned component in the customer infrastructure. See *Appendix C: ASV Scan Report Vulnerability Details* for required

content.

Note: There is no required template or format for the Vulnerability Details report. ASVs can design their own format for this report as long as the content specified in Appendix C is included.

ASVs must produce reports that meet all the reporting requirements in this document. This section contains a summary of the three sections of the ASV Scan Report. For details about the reporting requirements, see *Appendices A, B, and C*.

The ASV Scan Report consists of three sections as follows:

1. **Attestation of Scan Compliance**

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

Attestation of Scan Compliance Generation and Submission

- The Attestation of Scan Compliance can be submitted alone without the ASV Scan Executive Summary or ASV Scan Vulnerability Details, or is also the mandatory cover sheet for the ASV Scan Executive Summary and/or ASV Scan Vulnerability Details, at acquirer's or payment brand's discretion.
- ASV **must** generate this Attestation of Scan Compliance according to the template at *Appendix A: ASV Scan Report Attestation of Scan Compliance*. See "Report Customization" to the right.
- **Attestation of Scan Compliance content**, see *Appendix A: ASV Scan Report Attestation of Scan Compliance* for required template.
 - Scan customer contact information
 - Scan customer assertions per the Scan Finalization section
 - ASV contact information (individual name or corporate contact)
 - Overall scan results (pass or fail) without IP address or vulnerability details
 - Number of components scanned, number of identified failing vulnerabilities, and number of components identified but not scanned due to scan customer's out-of-scope assertion
 - Dates for scan completion and scan expiration
 - ASV company assertion per Scan Finalization section

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

- 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* language or language within the *ASV Program Guide*
- Font style, sizes, and colors, and page spacing
- Placement of information

While the compliance status radio buttons 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 Executive Summary**

This section lists vulnerabilities by components (IP address) and shows whether each IP address scanned received a passing score and met the scan validation requirement. This section shows all vulnerabilities noted for a given IP address, with one line per vulnerability noted. For example, an IP address will show one line when only one vulnerability is noted, but will have five lines if five vulnerabilities are noted, etc.

Executive Summary generation and submission

- The Executive 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 payment brand's discretion.

- ASVs **must** generate this according to the template at *Appendix B: ASV Scan Report Executive Summary*. See “*Report Customization*” above.

Executive Summary content – See *Appendix B: ASV Scan Report Executive Summary* for required template, which includes the following:

- Scan 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 page.)
- Dates for scan completion and scan expiration
- Vulnerability summary for each IP address, including severity, CVSS score, compliance status for that IP address (pass/fail), and any exceptions, false positives, or compensating controls noted by ASV
- A consolidated solution/correction plan, provided as a separate line item for each IP address

3. *ASV Scan Report Vulnerability Details*

This section is the overall summary of vulnerabilities that shows compliance status (pass/fail) and details for all vulnerabilities detected. This section of the report is in vulnerability order, showing each affected IP address as a separate line item for a given vulnerability.

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 Executive Summary at acquirer’s or payment brand’s discretion.
- For this report section, the ASV can optionally generate it according to the template at *Appendix C: Scan Report Vulnerability Details*. If the template is not used, all information specified in *Appendix C* must be clearly included.

Note: Use of the template at *Appendix C: ASV Scan Report Vulnerability Details* is *OPTIONAL* but all elements from *Appendix C* must be included in the ASV’s report

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 IP addresses are listed, including severity and scoring, industry reference numbers, vulnerability compliance status (pass/fail), detailed explanation, and other information about the vulnerability that the ASV may add.

Scan Customer and ASV Attestations

Before completion of the scan results and generation of the scan report, each ASV must provide a mechanism within their 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 identified in the Scan Report, and must be completed before each Scan Report is finalized.

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 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 attestation includes the following elements:

- ASV Program Guide and other supplemental guidance from PCI SSC was followed for this scan.
- ASV's practices for this scan included an automated or manual Quality Assurance process that:
 - Reviews scan customer scoping practices
 - Detects incorrect, incomplete, 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 exceptions.

Scan Customer Attestation

Mandatory text

(Scan customer name) attests that: This scan 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 is accurate and complete. (Scan customer name) also acknowledges the following: 1) proper 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 the PCI DSS; this scan result does not represent (Scan customer name)'s overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements.

ASV Attestation

Mandatory text

(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, and 3) active interference. This report and any exceptions were reviewed by (name).

Note: See section entitled "ASV's Internal Quality Assurance Program" for more details.

Scan Finalization

A completed scan has one of the following results:

- A passing scan
 - Scan customers ONLY submit passing scan reports
 - Scan customers submit passing scans according to the "Compliance Reporting" section of this document
- A failing scan for which the scan customer disputes the results
 - Scan customer and ASV resolve any scan disputes or exceptions according to the "Managing False Positives and Other Disputes" section of this document
- A failing scan that the scan customer does not dispute
 - Scan customer resolves failing vulnerabilities according to the "Resolving Failing Scans" section of this document
- A failing scan due to scan interference
 - Scan customer and ASV resolve such scan failures according to the "Resolving Inconclusive Scans" section of this document

Resolving Failing Scans

For failing 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 passing scan is achieved, scan customer submits results according to the “Compliance Reporting” section below.
 - For failing scans, scan customer repeats this “Resolving Failing Scans” section.

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 a 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 lab-validated ASV scan solution to complete a scan of the external interface(s) of all hosts 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 solution¹ (such as an appliance or agent) could be installed at the scan customer’s site.

The ASV scan solution must complete a full 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 Security Engineers who have been qualified by PCI SSC as per Section 3.2, “ASV Staff – Skills and Experience” in the document *PCI DSS Validation Requirements for Approved Scanning Vendors (ASVs)*.

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

Managing False Positives and Other Disputes

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

- Vulnerabilities that are incorrectly found (false positives)

¹ The ASV scan solution must be the same lab-validated scan solution tested and approved by the PCI SSC for the ASV.

- Vulnerabilities that have a disputed CVSS Base score
- Vulnerabilities for which a compensating control is in place (see next section entitled “Addressing Vulnerabilities with Compensating Controls”)
- Exceptions in the report
- Conclusions of the scan report
- List of components designated by scan customer as segmented from PCI DSS scope
- Inconclusive ASV scans or ASV scans that cannot be completed due to scan interference

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 dumps, 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 if 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 if the submitted written evidence is sufficient proof to resolve the dispute. This includes assessing 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 Executive Summary*.
- Not remove disputes from a 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/resubmitted by scan customer and evaluated again by the ASV for each quarterly scan.
- Allow evaluation of disputes only by ASV Security Engineers who have been qualified by PCI SSC as per Section 3.2, "ASV Staff – Skills and Experience" in the document *PCI DSS Validation Requirements for Approved Scanning Vendors (ASVs)*.
- Include the name of the security engineer who handled the exception along with each exception within the scan report.

Addressing Vulnerabilities with Compensating Controls

The 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 scanning 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 should be documented in the scanning report under "Exceptions, False Positives, or Compensating Controls" as noted in *Appendix B: ASV Scan Report Executive 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 met by compensating controls.

Compliance Reporting

Merchants and service providers need to follow each payment brand's respective compliance reporting requirements to ensure each payment brand acknowledges an entity's compliance status. Scan reports must be submitted according to each payment brand's requirements. Contact your acquiring bank or check each payment brand's website to determine to whom results should be submitted.

Report Delivery and Integrity

The ASV solution's final scan report should 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.

Quality Assurance

ASV's Internal Quality Assurance Program

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

The ASV will include in the report contact information for inquiries relating to integrity of the specific report. This can EITHER be a generic corporate contact OR a named individual per the ASV's discretion. In either case, whoever is responsible for responding to inquiries, whether a generic contact or a named individual, must have been qualified by PCI SSC as per section 3.2 "ASV Staff - Skills and Experience" in the document *PCI DSS Validation Requirements for Approved Scanning Vendors (ASVs)*.

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

- The QA process may be performed automatically or manually. Automatic QA processes should 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 such as IPS.
- The QA process should perform basic sanity tests to detect obvious inconsistencies in findings.

PCI SSC's Quality Assurance Program for ASVs

The PCI SSC, in accordance with the *Validation Requirements for ASVs*, reviews work associated with ASV scan reports for quality assurance purposes. As stated in the *Validation Requirements for ASVs* and the *PCI ASV Compliance Test 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 Test Bed. Additionally, at least every two years the ASV will be validated by reviewing the results of scan reports developed for ASV clients.

The PCI SSC has determined that the discovery of specific and severe violations of ASV agreements or validation requirements may warrant immediate remediation or possibly revocation of the ASV. These violations include, but are not limited to:

- Intentionally deciding not to scan relevant IP addresses
- Operating a different solution or methodology than what was validated during the ASV test
- Failure to renew specified insurance requirements
- Unqualified professionals operating the scan solution and/or reviewing results
- Failure to complete annual validation to the ASV Test Bed
- Misrepresentation of the PCI DSS to sell products or services
- Removing systems or applications from scope that directly 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 *Validation Requirements for ASVs* for a complete list of requirements.

Remediation

During remediation, ASVs are still permitted to conduct scans, but reports and scanning activity will be monitored by the PCI SSC to determine whether the issues have been mitigated. ASVs will be charged a fee to cover the cost of monitoring.

The ASV must also submit a remediation plan to PCI SSC detailing how the ASV plans to improve quality of their reports. PCI SSC may also require an onsite visit with the ASV to audit their QA program, at the expense of the ASV.

Revocation

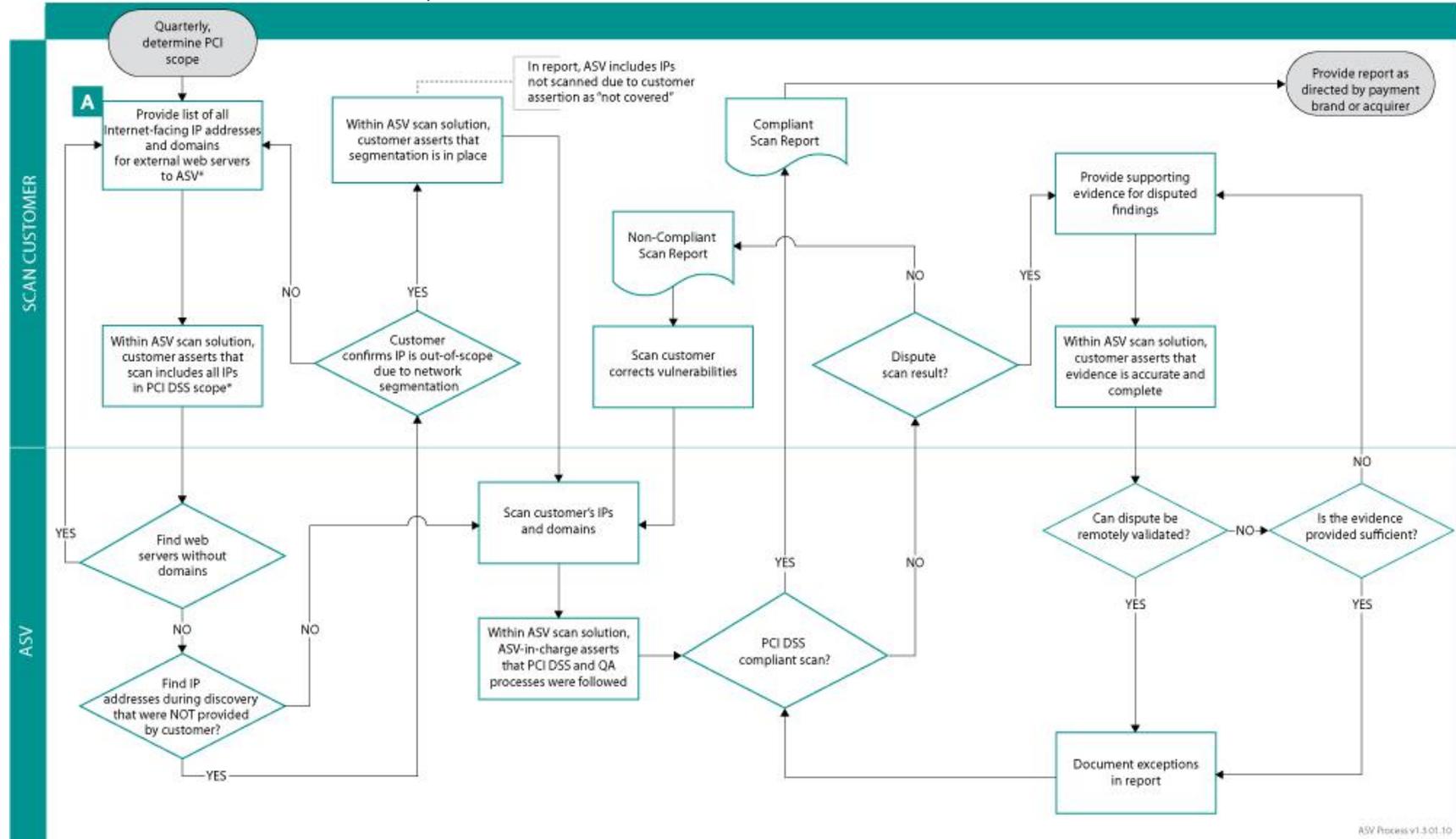
When ASV status is revoked, the vendor is removed from the PCI SSC List of ASVs. Once an ASV status is revoked, the vendor cannot perform scans to help merchants and service providers achieve compliance with PCI DSS Requirement 11.2.2. The vendor can appeal the revocation of ASV status but must meet requirements as documented in the *Validation Requirements for ASVs* and supporting documents.

After a revocation period of at least six months, a vendor can resubmit to become an ASV according to the process and fees detailed in the “Scanning Vendor Testing and Approval Process” section.

PCI SSC reserves the right to remove a vendor from the list of Approved Scanning Vendors when it is clear that the ASV is not performing their services in accordance with the *Validation Requirements for ASVs* or with the requirements in this *Approved Scanning Vendors Program Guide*. If PCI SSC intends to remove a vendor from the list of Approved Scanning Vendors, PCI SSC will notify the vendor in writing.

Figure 1: Overview of ASV Processes

The flowchart below illustrates the overall process of the ASV Scan.



ASV Process v1.3 01.10

PCI DSS scan applies if an entity:
 1. Stores, processes, or transmits cardholder data, and
 2. Has Internet-facing IP addresses.

Even if an entity does not offer Internet-based payment card transactions, other services may make systems Internet-accessible. Basic functions such as e-mail and employee Internet access result in Internet accessibility of a network. Such seemingly insignificant paths to and from the Internet can provide unprotected pathways into an entity's systems and potentially expose cardholder data if not properly controlled.

* Scan customers (merchants and service providers) have the ultimate responsibility for defining PCI DSS scan scope, though they may seek expertise from QSAs and guidance from ASVs. If an account data compromise occurs via an IP address or component not included in the scan, the scan customer is accountable.

Appendix A: ASV Scan Report Attestation of Scan Compliance

Scan Customer Information		Approved Scanning Vendor Information	
Company:		Company:	
Contact:	Title:	Contact:	Title:
Telephone:	E-mail:	Telephone:	E-mail:
Business Address:		Business Address:	
City:	State/Province:	City:	State/Province:
ZIP:	URL:	ZIP:	URL:

Scan Status

- Compliance Status **Fail** **Pass**
- Number of unique components*scanned:
- Number of identified failing vulnerabilities:
- Number of components* found by ASV but not scanned because scan customer confirmed components were out of scope:
- Date scan completed:
- Scan expiration date (90 days from date scan completed):

Scan Customer Attestation

(Customer name) attests on (date) that this scan 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 is accurate and complete. (Scan customer name) also acknowledges the following: 1) proper 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.*

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 and the PCI DSS 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, and 3) active scan interference. This report and any exceptions were reviewed by (ASV reviewer name).

Appendix B: ASV Scan Report Executive Summary

Appendix B must be used to create the ASV Scan Report Executive Summary. See the section “Generating, Reading, and Interpreting Scan Reports” for more details.

The “Attestation of Scan Compliance” from Appendix A must be included as the cover sheet for the ASV Scan Report Executive Summary. The ASV Scan Report Vulnerability Details from Appendix C can accompany this report as well.

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

Part 2. Component Compliance Summary			
IP Address:	Pass	<input type="checkbox"/>	Fail <input type="checkbox"/>
IP Address:	Pass	<input type="checkbox"/>	Fail <input type="checkbox"/>
IP Address:	Pass	<input type="checkbox"/>	Fail <input type="checkbox"/>
IP Address:	Pass	<input type="checkbox"/>	Fail <input type="checkbox"/>
IP Address:	Pass	<input type="checkbox"/>	Fail <input type="checkbox"/>

Part 3a. Vulnerabilities Noted for each IP Address					
IP Address	Vulnerabilities Noted per IP address ²	Severity Level ³	CVSS Score ⁴	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				Pass / Fail	
Consolidated Solution/Correction Plan for above IP Address:					
				Pass / Fail	
Consolidated Solution/Correction Plan for above IP Address:					

² Include CVE identifier and title and rank in descending order by CVSS score.

³ High, Medium or Low Severity in accordance with Table 2

⁴ Common Vulnerability Scoring System (CVSS), <http://www.first.org/cvss/>, base score, as indicated in the National Vulnerability Database (NVD), <http://nvd.nist.gov/cvss.cfm> (where available)

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address ⁵	Severity Level ⁶	CVSS Score ⁷	Compliance Status	Exceptions, False Positives, or Compensating Controls Noted by the ASV for this Vulnerability
				Pass / Fail	
<i>Consolidated Solution/Correction Plan for above IP Address:</i>					
				Pass / Fail	
<i>Consolidated Solution/Correction Plan for above IP Address:</i>					
				Pass / Fail	
<i>Consolidated Solution/Correction Plan for above IP Address:</i>					
				Pass / Fail	
<i>Consolidated Solution/Correction Plan for above IP Address:</i>					
				Pass / Fail	
<i>Consolidated Solution/Correction Plan for above IP Address:</i>					

Part 3b. Special Notes by IP Address

IP Address	Note ⁸	Item Noted (remote access software, POS software, etc.)	Scan customer's declaration that software is implemented securely (see next column if not implemented securely)	Scan customer's description of actions taken to either: 1) remove the software or 2) implement security controls to secure the software

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

⁷ Common Vulnerability Scoring System (CVSS), <http://www.first.org/cvss/>, base score, as indicated in the National Vulnerability Database (NVD), <http://nvd.nist.gov/cvss.cfm> (where available)

⁸ Use appropriate text for each subject, as outlined within the Program Guide.

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 “Attestation of Scan Compliance” from *Appendix A* must be included as the cover sheet for the ASV Scan Report Vulnerability Details if submitted without the ASV Scan Report Executive Summary. The ASV Scan Report Executive Summary from *Appendix B* can accompany this report as well.

Part 1. Scan Information

Scan Customer Company:	ASV Company:
Date scan was completed:	Scan expiration date :

Part 2. Vulnerability Details

Affected IP Address	CVE Number	Vulnerability	CVSS Score ⁹	Severity Level	Compliance Status Pass / Fail	Details
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	

⁹ Common Vulnerability Scoring System (CVSS), <http://www.first.org/cvss/>, base score, as indicated in the National Vulnerability Database (NVD), <http://nvd.nist.gov/cvss.cfm> (where available)

Appendix D: Remote Access Security Features

Examples of remote access security features include:

- Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).
- Allow connections only from specific (known) IP/MAC addresses.
- Use strong authentication, including unique and complex passwords for logins according to PCI DSS Requirements 8.1 - 8.4 and 8.5.8–8.5.15.
- Enable encrypted data transmission according to PCI DSS Requirement 4.1.
- Enable account lockout after a certain number of failed login attempts according to PCI DSS Requirement 8.5.13.
- Configure the system so a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed.
- Enable the logging function.
- Restrict access to customer passwords to authorized reseller/integrator personnel.