Payment Card Industry (PCI)

Approved Scanning Vendors

Program Guide

Reference 1.0

PCI DSS Version 1.2

March 2010

Document Changes

Date	Version	Description
February 11, 2010	1.0	ASV Program Guide Reference Document 1.0 of the PCI DSS Standards 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.

Table of Contents

Approved Scanning Vendor Program Guide – Introduction

This Approved Scanning Vendor (ASV) Program Guide explains the purpose and scope of PCI DSS external vulnerability scans for merchants and service providers undergoing scans as part of validating 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. The PCI SSC recommends, but does not require, that scan customers use the requirements for other vulnerability scanning required by PCI DSS Requirement 11.2, including internal vulnerability scanning, external scanning performed after a significant change to the network, and any external scanning performed in addition to the required quarterly external scans.*

Related Publications

Requirement 11.2 of the *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures* ("PCI DSS") *Version 1.2* requires quarterly external vulnerability scans, which must be performed by an Approved Scanning Vendor (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 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 endeavour to update PCI DSS requirements every 24 months. 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 requirements at any time, and will endeavour to 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:

- *Technical and Operational Requirements for ASVs*, version 1.1
- *Security Scanning Procedures*, version 1.1

ASVs must implement the requirements set forth in this document by no later than September 1, 2010.

Terminology

Throughout this document:

- "PCI DSS" refers to the then-current version of the *Payment Card Industry (PCI) Data Security Standard,* as available through the Website (defined below).
- "PCI SSC" refers to the PCI Security Standards Council, LLC.
- "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.
- "ASV" (Approved Scanning Vendor) refers to a data security firm that has been qualified and trained by the PCI SSC to use a vulnerability scanning solution to determine compliance of their customers with the external vulnerability scanning requirement of PCI DSS Requirement 11.2
- "Scan Customer" refers to a merchant or service provider who undergoes a quarterly external vulnerability scan via an ASV, either through relationship with an ASV, or through a relationship between a scan customer's acquirer and an ASV.
- "ASV scan solution" refers to a set of security services and tool(s) offered by an ASV to validate compliance of a merchant or service provider with the external vulnerability scanning requirement of PCI DSS Requirement 11.2. 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:
  - Operate the ASV scan solution
  - Submit the scan report to the scan customer
  - Review and interpret scan results, as needed
- "QSA" (Qualified Security Assessor) refers to a data security assessment firm that has been qualified and trained by PCI SSC to perform PCI DSS onsite assessments.
- "CVSS" refers to the Common Vulnerability Scoring System version 2.0, an open framework for communicating the characteristics and impacts of IT vulnerabilities.
- "NVD" refers to the National Institute of Standards and Technology (NIST) National Vulnerability Database for known vulnerabilities and vulnerability details.
- "CVE" refers to Common Vulnerabilities and Exposures, a publicly available and free-to-use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.

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 (PCI) 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 all payment brands.

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

- Customers benefit from a broad selection of Approved Scanning Vendors (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 (PCI) 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 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 application 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 (ASVs)

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. 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 Requirements 11.2, and in accordance with this document and other supplemental guidance published by the PCI SSC
- 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 passed 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 at www.pcisecuritystandards.org to conduct quarterly external vulnerability scanning according to PCI DSS Requirement 11.2 and this document
- 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 intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) so they do not interfere with the ASV's scan, as required by this document. See the section entitled *Perform a Scan without Interference from IDS/IPS.*
    - 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 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 IP addresses 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 e-mail 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 PCI DSS vulnerability scans in conjunction 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, 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, 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
- Dispute Resolution
- Reporting/remediation

PCI DSS Requirement 11.2

PCI DSS Requirement 11.2 states:

PCI DSS Requirement	Testing Procedures
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the company's internal staff.*	**11.2.a** Inspect output from the most recent four quarters of internal network, host, and application vulnerability scans to verify that periodic security testing of the devices within the cardholder data environment occurs. Verify that the scan process includes re-scans until passing results are obtained. ***Note:*** *External scans conducted after network changes, and internal scans, may be performed by the company's qualified internal personnel or third parties.*
	11.2.b Verify that external scanning is occurring on a quarterly basis in accordance with the PCI Security Scanning Procedures, by inspecting output from the four most recent quarters of external vulnerability scans to verify that: ▪ Four quarterly scans occurred in the most recent 12-month period; ▪ The results of each scan satisfy the PCI Security Scanning Procedures (for example, no urgent, critical, or high vulnerabilities); ▪ The scans were completed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. ***Note:*** *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.*
	11.2.c Verify that internal and/or external scanning is performed after any significant change in the network, by inspecting scan results for the last year. Verify that the scan process includes re-scans until passing results are obtained.

Can a merchant or service provider perform their own external vulnerability scanning?

Only ASV scan solutions can be used to perform the PCI DSS quarterly external vulnerability scans required by PCI DSS Requirement 11.2, and an ASV scan solution must be run by the ASV. Some ASV scan solutions may, under the control and management of the ASV, be started remotely by a scan customer via an ASV's web portal to allow a scan customer to select the best times to scan their cardholder data environment. However, only an authorized ASV employee can be allowed to configure any settings (e.g., disable any vulnerability checks—SQL injection, XSS checks) 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), please refer to the *Validation Requirements for Approved Scanning Vendors (ASVs)* located at www.pcisecuritystandards.org.

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 www.pcisecuritystandards.org, the company's scanning solution is thoroughly tested in an ASV Validation Lab (the "ASV Test Bed") to ensure the scanning solution performs vulnerability scanning in accordance with this document. Here are the steps for an ASV to prepare for Scanning Vendor Testing:

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 ASV company is ready to be tested.
3. The PCI SSC notifies the scanning vendor to schedule the test.
4. The scanning vendor submits the solution for testing to PCI SSC via the ASV Portal.
    a. The scanning vendor uses this portal to create the solution for testing. (PCI SSC provides instructions for the portal with Step 3 above.)
5. Once the scanning solution is received by PCI SSC via the 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 lab with the next steps in the process for scheduling the scan.

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

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 ASV Compliance Test Agreement, Schedule 1*. Please refer to www.pcisecuritystandards.org for the current *PCI ASV Compliance Test Agreement*.

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: *Per the PCI DSS, "System components" are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses 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 (Internet) applications.*

Scope and Network Segmentation

Scan customers can 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

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 their website).

For ISPs, scan customers need to coordinate with them to allow the ASV scan to be performed without interference from IDS or IPS. For more details, see the section entitled "Perform a Scan without Interference from IDS/IPS."

For hosting providers and their shared hosting environments, it is common practice that a single server will host more than one website. In a shared hosting environment, the scan customer shares the server with the hosting provider's other customers. This could lead to the merchant's website being compromised through security weaknesses on other customers' websites on the hosting provider's server.

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 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 that was previously provided to the ASV that has been removed at the request of 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 – like "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 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 in understanding their risks and prioritizing remediation activities.

  The ASV scan solution should, where possible, identify the operating system running on each live system. The ASV scanning solution should, 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 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 tools 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.

- **Perform a Scan without Interference from IDS/IPS**

  In order to ensure that reliable scans can be conducted, the ASV scan solution must be allowed to perform scanning without interference from intrusion detection systems (IDSs) or intrusion prevention systems (IPSs). Such "active" protection 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.

This 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 IDS/IPS, those vulnerabilities will remain uncorrected and may be exploited if the IDS/IPS changes or fails.

If an ASV detects that an IDS/IPS has blocked or filtered a scan, then the ASV is required to fail the scan as "inconclusive". All ASV scans must be validated by the ASV to ensure they have not been blocked or filtered by an IDS/IPS.

- **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 IDS/IPS, certain temporary configuration changes on the scan customer's network devices must be completed to obtain a scan that accurately assesses the scan customer's external security posture.

  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. We encourage scan customers 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.
  - Reapply the standard secure configurations as soon as the scan is complete.
    - For IDS/IPS, configure the devices to monitor and log, but not to act against, the originating IP address(es) of the ASV.

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 failure noted is mitigated by compensating controls, etc.*

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
Firewalls & Routers	Firewalls and routers, which control traffic between the company's network and external untrusted networks (for example, the Internet), have known vulnerabilities for which patches are released periodically. Another common problem with firewalls and routers is inadequate configuration. To ensure firewalls and routers are protected against these vulnerabilities and are able to protect the network effectively, it is important to apply the patches as soon as possible.	The ASV must scan all 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 devices must be included. The ASV scanning solution must test for known vulnerabilities and determine whether the firewall or router is adequately patched.

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
Operating Systems	An operating system (OS) sits between hardware and applications. Malicious individuals exploit operating system vulnerabilities to get access to internal databases that potentially store cardholder data. New exploits are discovered routinely for OSs and security patches are released for these flaws. To protect operating systems against these exploits and vulnerabilities, it is important to apply vendor patches as soon as possible.	The ASV scan solution must be able to verify that the operating system is patched for these known exploits. The ASV scanning solution must also be able to determine the version of the operating system and whether it is an older version no longer supported by the vendor, in which case it must be marked as an automatic **failure** by the ASV.
Database Servers	Database servers store and manage access to cardholder data. Malicious individuals exploit vulnerabilities in these servers to get access to cardholder data. New vulnerabilities and exploits are discovered routinely for databases, and security patches are released for these flaws. To protect against these exploits and vulnerabilities, it is important to apply the patches as soon as possible.	The ASV 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.
Web servers	Web servers allow Internet users to view web pages, interact with web merchants, and make online web purchases. Malicious individuals exploit vulnerabilities in these servers and their scripts to get access to internal databases that potentially store cardholder data. Because these servers are fully accessible from the public Internet, scanning for vulnerabilities is essential.	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 exploits. Browsing of directories on a web server is not a good practice. The ASV scanning solution must be able to scan the website and verify that directory browsing is not possible on the server. Positive identification of directory browsing must be disclosed with the following Special Note. ▪ "*Note to scan customer: Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.*"

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
Application server	Application servers act as the interface between the web server and the back-end databases and legacy systems. 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. Malicious individuals exploit vulnerabilities in these servers and their scripts to get access to internal databases that potentially store credit card data. 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.	The ASV scanning solution must be able to detect the presence of an application server and/or web application servers and detect any known vulnerability and configuration issues.
Common Web Scripts	Common web scripts enable servers to respond to client-side requests (for example, to enable an e-commerce web server to respond to requests from customers' web browsers).	The ASV scan solution must be able to detect commonly found scripts such as common gateway interface (CGI) scripts, e-commerce related scripts (for example, shopping carts and CRM scripts), ASPs, PHPs, etc. and detect any known vulnerabilities.
Built-in Accounts	Built-in, or default accounts and passwords are commonly used by hardware and software vendors to allow the customer their first access to the product. 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. ***Note:*** *PCI DSS Requirement 2.1 stipulates that vendor-supplied defaults, including vendor accounts and passwords, are changed before installing a system on a network.*	For testing and reporting on built-in or default accounts in routers, firewalls, operating systems, web servers, database servers, applications, POS systems, or other components, the ASV scan solution, **must do the following**: ▪ Detect the presence of built-in or default accounts and passwords, not by using brute-force or dictionary attacks, but rather by concentrating on known built-in or default accounts 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	DNS servers resolve Internet addresses by translating domain names into IP addresses. 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 a merchant's or service provider's web page and collect cardholder data.	The ASV scan solution must be able to detect the presence of 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).
Mail Servers	Mail servers typically exist in the DMZ and can be vulnerable to attacks by malicious individuals. They are a critical element to maintaining overall website security.	The ASV scan solution must be able to detect the presence of a mail server and detect any known vulnerability and configuration issues.

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
Web Applications	Web applications reside on application servers or web application servers (see above), and interface with the back-end databases and legacy systems. For example, when cardholders share account numbers with merchants, the web application may take the cardholder data from a customer to process and complete the transaction, and store the transactions results and cardholder data in a database, all as part of the customer's online purchase. Malicious individuals frequently exploit application vulnerabilities to gain access to internal databases that potentially store cardholder data.	The ASV scan solution must be able to detect via automated or manual means, the following application vulnerabilities and configuration issues: ▪ Unvalidated parameters that lead to SQL injection attacks (which must be marked as an automatic **failure**) ▪ Cross-site scripting (XSS) flaws (which must be marked as an automatic **failure**) ▪ Directory traversal vulnerabilities (which must be marked as an automatic **failure**) ▪ HTTP response splitting/header injection (which must be marked as an automatic **failure**) ▪ Information leakage, including: • Detailed application error messages • Backup script files (for example home.asp.bak, index.jsp.old, etc.) • Include file source code disclosure • Insecure HTTP methods enabled • WebDAV or FrontPage extensions enabled • Default web server files • Testing and diagnostics pages (for example phpinfo.html, test-cgi, etc.)
Other Applications	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.	The ASV scan solution must be able to detect the presence of other applications and to detect any known vulnerability and configuration issues.
Common Services	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.	The ASV scan solution must be able to detect common services known to have vulnerabilities.
Wireless Access Points	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.	The ASV scan solution must scan detected wireless access points visible from the Internet (over the wire) and detect known vulnerabilities and configuration issues.
Backdoors	A backdoor is a malicious software application that is often commonly known in hacker communities. This malicious software should be identified and eliminated.	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.

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
SSL/TLS	The SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols 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. Per PCI DSS, strong cryptography and security protocols must be deployed and **SSL v3.0/TLS v1.0** is the **minimum standard**.	The ASV scan solution must: ▪ 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. ***Note:*** *When scanning systems by IP address, it may not always be possible for an ASV scanning solution to determine whether the server hostname matches a certificate Common Name or wildcard.* A component must be considered non-compliant and marked as an automatic **failure** by the ASV if it supports SSL 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).
Remote Access	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.	The ASV scan solution must be able to detect the presence of remote access software and detect any known vulnerability or configuration issues. Remote access software includes, but is not limited to: VPN (IPSec, PPTP, SSL), pcAnywhere, VNC, Microsoft Terminal Server, remote web-based administration, ssh, Telnet. In addition to reporting any identified vulnerability or configuration issues in the remote access software, the ASV scan solution must note the presence of remote access software with the following Special Note: ▪ *"Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note."*

Scan Components	For Scan Customers Why must it be scanned?	For ASVs ASV Scan Solution must:
Point-of-sale (POS) Software	POS software that is visible from the Internet increases risk to the cardholder data environment. Well-known default passwords and publicized weaknesses for POS software are frequently used for cardholder data compromises.	If the ASV scan solution detects point-of-sale (POS) software, the following note should be included in the Special Notes section of the scan report: ▪ *"Note to scan customer: Due to increased risk to the cardholder data environment when a point-of-sale system is visible on the Internet, please 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. Please consult your ASV if you have questions about this Special Note."*

Vulnerability Reporting

To demonstrate compliance, a scan must not contain high-level vulnerabilities, or any vulnerability that indicate features or configurations that are in violation of PCI DSS. If these exist, the ASV must consult with the client 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 mitigation of identified issues, ASVs must assign a severity level to each identified vulnerability or misconfiguration.

The designation of each severity level must allow for an easy comparison between levels. Therefore, a severity ranking that is easy to understand must be presented, with High Severity, Medium Severity, Low Severity.

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 (NVD), which is maintained by the National Institute of Standards and Technology (NIST). The NVD contains details of known vulnerabilities based on the Common Vulnerabilities and Exposures (CVE) dictionary. The NVD has adopted the CVSS and publishes CVSS Base Scores for each vulnerability. ASVs should use the CVSS scores whenever they are available.

The use of the CVSS and CVE standards, in conjunction with 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 mitigation of 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 environment 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 ones (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 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 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 denial-of-service 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-level.

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, please 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.

   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.

   - **Attestation of Scan Compliance content**, please 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.

2. ***ASV Scan Report Executive Summary***

   This 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 – Please 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 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, however, 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 – Please 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.

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 vulnerability scan requirement (PCI DSS 11.2) 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 scanner 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 my 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
  - Submit passing scans according to "*Compliance Reporting"* section
- A failing scan for which the scan customer disputes the results
  - Scan customer and ASV resolve any scan disputes or exceptions according to "*Managing False Positives and Other Disputes*" section
- A failing scan that the scan customer does not dispute
  - Scan customer resolves failing vulnerabilities according to "*Resolving Failing Scans*" section

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 “Compliance Reporting” section below.
    - For failing scans, scan customer repeats this “Resolving Failing Scans” section.

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)
- 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 as segmented from PCI-scope by scan customer

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).

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 Customer's evidence for relevance and accuracy. If evidence is sufficient, the ASV updates the scan report.
- 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 customer to edit the scanning 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 accuracy 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 customer must not be permitted to edit the scanning 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 solutions 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 should 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 it is a generic contact or a named individual, that contact 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 scanner and the target network, including those resulting from link failure or active security measures such as those implemented in 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 and/or reviewing results*
- *Misrepresentation of the PCI DSS to sell products or services*
- *Removing systems or applications out of 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 the systems or system components*

Please 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 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

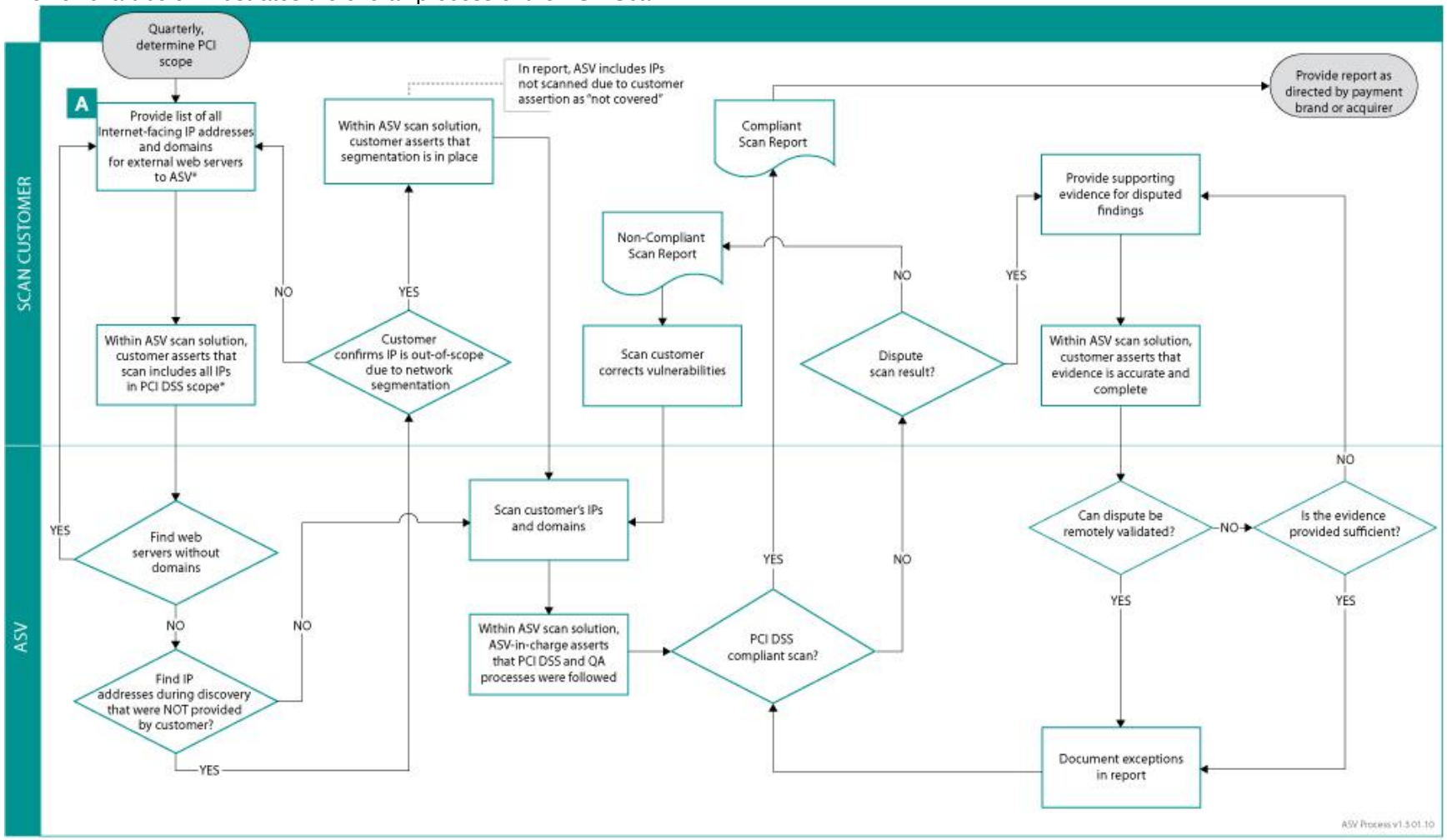
When ASV status is revoked, the vendor is removed from the PCI SSC List of ASVs. Once an ASV status is revoked, the vendor cannot perform scans to help merchants and service providers achieve compliance with PCI DSS Requirement 11.2. The vendor can appeal the revocation of ASV status but must meet requirements 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.



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

Even if a entity does not offer Interned-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	☐	Fail	☐
IP Address:	Pass	☐	Fail	☐
IP Address:	Pass	☐	Fail	☐
IP Address:	Pass	☐	Fail	☐
IP Address:	Pass	☐	Fail	☐

Part 3a. Vulnerabilities Noted for each IP Address

IP Address	Vulnerabilities Noted per IP address[1]	Severity Level[2]	CVSS Score[3]	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:					

[1] Include CVE identifier and title and rank in descending order by CVSS score.
[2] High, Medium or Low Severity in accordance with Table 2
[3] 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[4]	Severity Level[5]	CVSS Score[6]	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:					
				Pass / Fail	
Consolidated Solution/Correction Plan for above IP Address:					
				Pass / Fail	
Consolidated Solution/Correction Plan for above IP Address:					
				Pass / Fail	
Consolidated Solution/Correction Plan for above IP Address:					

Part 3b. Special Notes by IP Address

IP Address	Note[7]	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

[4] Include CVE identifier and title and rank in descending order by CVSS score.
[5] High, Medium or Low Severity in accordance with Table 2
[6] 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)
[7] 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[8]	Severity Level	Compliance Status Pass / Fail	Details
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	
					Pass / Fail	

[8] 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.