

## Achieving PCI Security Scan Compliance

To comply with the PCI Security Scanning requirement, your organization's web sites or IT infrastructures with Internet-facing IP addresses must be scanned according to certain procedures.

Below are key points you should know when selecting an Approved Scanning Vendor (ASV) and before initiating your PCI Security Scan:

1. All scans must be conducted by an ASV selected from the list of approved scanning vendors provided by the PCI Security Standards Council. ASVs are required to conduct scans in accordance with the "Technical and Operational Requirements for ASVs" procedures.
2. Quarterly Scans are required in accordance with PCI DSS Requirement 11.2.
3. Prior to scanning the web site and IT infrastructure, merchants and service providers must:
  - Provide the ASV with a list of all Internet-facing IP addresses and/or IP address ranges
  - Provide a list of all domains to be scanned if domain-based virtual hosting is used.
4. Using the IP address range provided by the Client, the ASV must conduct network probing to determine which IP addresses and services are active.
5. Merchants and service providers must contract with the ASV to perform periodic scans of all active IP addresses (or domains, if applicable) and devices.
6. The ASV must scan all filtering devices such as firewalls or external routers (if used to filter traffic). If a firewall or router is used to establish a demilitarized zone (DMZ), these devices must be scanned for vulnerabilities.
7. The ASV must scan all web servers. Because these servers are fully accessible from the public Internet, scanning for vulnerabilities is essential.
8. The ASV must scan application servers if present, since they act as the interface between the web server and the back-end databases and legacy systems. Hackers exploit vulnerabilities to get access to internal databases that potentially store credit card data.
9. The ASV must scan Domain Name Servers (DNSs). If DNS servers are vulnerable, hackers can spoof a merchant or service provider web page and collect credit card information.
10. The ASV must scan mail servers. Since they typically exist in the DMZ and can be vulnerable to hacker attacks, they are a critical element to overall web site security.
11. The ASV must scan Virtual Hosts. If a single server hosts more than one web site, the merchant's site could be exploited through the other Clients. All merchants whose web sites are hosted must request their provider to scan their entire Internet-facing IP range and demonstrate compliance while merchants are required to have their own domains scanned.
12. The ASV must scan wireless access points in wireless LANs (WLANs) to identify potential vulnerabilities and misconfigurations.
13. Arrangements must be made to configure the intrusion detection system/intrusion prevention system (IDS/IPS) to accept the originating IP address of the ASV. If this is not possible, the scan should be originated in a location that prevents IDS/IPS interference.