Mapping the Qualys Cloud Suite to the

PCI Data Security Standard Requirements

Contributing Qualys modules

Module	Description
PCI Compliance	Automate, simplify and attain PCI compliance quickly. Qualys PCI is the most accurate, easy and cost-effective solution for PCI compliance testing, reporting and submission.
Policy Compliance	Assess security configurations of IT systems throughout your network. Qualys PC is a next-gen solution for continuous risk reduction and compliance with internal policies and external regulations.
CloudVIew	Continuously monitor and assess your cloud assets and resources for misconfigurations and non-standard deployments. Qualys CSA is a next-generation cloud app for unparalleled visibility and continuous security of public cloud infrastructure.
Security Assessment Questionnaire	Minimize the risk of doing business with vendors and other third parties. Qualys SAQ is a transformative solution for automating and streamlining an organization's vendor risk management process.
File Integrity Monitoring	Log and track file changes across global IT systems. Qualys FIM is a cloud solution for detecting and identifying critical changes, incidents, and risks resulting from normal and malicious events.
Global IT Asset Inventory	Qualys AI detects all IT assets everywhere, giving you a complete, categorized inventory that's enriched with details, like vendor lifecycle information.
Vulnerability Management	Continuously detect and protect against attacks, anytime, anywhere. Qualys VM is the industry's most advanced, scalable and extensible solution for vulnerability management.
Certificate View	Assess your digital certificates and TLS configurations. Qualys CRA is a next-generation cloud app for continuous monitoring, dynamic dashboarding and custom reporting of certificate issues and vulnerabilities
Indication of Compromise	Continuously monitor endpoints to detect suspicious activity. Qualys IOC is a solution for flagging telemetry data possibly indicating malware or breaches on devices on and off the network.

PM Patch Management	Streamline and accelerate vulnerability remediation for all your IT assets. Qualys PM automatically correlates vulnerabilities to patch deployments so you can remediate quickly, proactively, and consistently.
CM Continuous Monitoring	Alerts you in real time about network irregularities. Qualys CM is a next-generation solution for identifying threats and monitoring unexpected network changes before they turn into breaches.
WAS Web Application Scanning	Secure web applications with end-to-end protection. Qualys WAS is a robust solution for continuous web app discovery and detection of vulnerabilities and misconfigurations.

Mapping of Qualys Suite to PCI Data Security Standard Requirements

PCI DSS Requirements v3.2			
Requirement 1: Install and maintain a firewall configuration to protect cardholder data			
1.1	Establish and implement firewall and router configuration standards that include the following:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.1.5	Description of groups, roles, and responsibilities for management of network components	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.1.6	Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.1.7	Requirement to review firewall and router rule sets at least every six months	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	Qualys enables you to check for the presence of firewalls and ensure appropriate configurations.	PC CV

1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Qualys enables you to check for the presence of firewalls and ensure appropriate configurations.	PC CV
1.2.2	Secure and synchronize router configuration files.	Qualys enables you to check for the presence of firewalls and ensure appropriate configurations.	PC CV
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Qualys enables you to check for the presence of firewalls and ensure appropriate configurations.	PC CV
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.3.5	Permit only “established” connections into the network.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.3.7	Do not disclose private IP addresses and routing information to unauthorized parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
1.4	Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include:	Qualys enables you to check for the presence of personal firewalls deployed on servers, desktops, and laptops remotely.	PC PCI CV

1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters			
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Qualys enables you to verify that vendor-provided defaults are not used by checking for default and system accounts on servers, desktops, and network devices.	PC CV VM PCI
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Qualys can be used to verify that default settings and default passwords are not used across wireless devices connected to the wired network.	PC CV VM PCI
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Qualys enables you to discover systems on the network as well as detect the network-exposed services that are running on systems, significantly reducing the effort needed to bring the environment in compliance.	PC CV VM PCI
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.	Qualys enables you to assess whether configuration settings are accurately hardened for insecure services in the organization. You can also report on insecure protocols and daemons that are being used based on security benchmarks and best practices.	VM
2.2.4	Configure system security parameters to prevent misuse.	Qualys enables you to effectively and automatically validate if the systems are configured as per the organization's security requirements, so that any kind of misuses can be prevented.	PC CV VM PCI
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Qualys enables you to discover some of the insecure and typically unnecessary functionalities exposed to the network, significantly reducing the effort needed to bring the environment in compliance.	PC CV VM PCI

2.3	Encrypt all non-console administrative access using strong cryptography.	Qualys enables you to validate that encrypted protocols are in use across the systems and that unencrypted communication is not enabled on servers and workstations (SSH, not telnet; SSL, not unencrypted HTTP, etc).	PC CV VM PCI
2.4	Maintain an inventory of system components that are in scope for PCI DSS.	Qualys enables you to automate asset detection and inventory management work.	AI
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 3: Protect stored cardholder data			
3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.2.1	Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the first six/last four digits of the PAN.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:	Qualys enables you to confirm that encryption is in use across all the PCI systems in scope by checking system configuration settings relevant to encryption.	PC CV VM PCI
3.4.1	If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:	Qualys enables you to validate security settings required for the protection of system encryption keys.	VM SAQ PC CV PCI
3.5.1	Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.	Qualys enables you to get confirmation on the presence of policy or procedural controls by using its survey-based workflow. It can also help you check access rights and permissions on critical directories and key files.	SAQ
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.5.4	Store cryptographic keys in the fewest possible locations.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.6.1	Generation of strong cryptographic keys	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.6.2	Secure cryptographic key distribution	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

3.6.3	Secure cryptographic key storage	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.6.6	If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.6.7	Prevention of unauthorized substitution of cryptographic keys.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 4: Encrypt transmission of cardholder data across open, public networks			
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks, including the following:	Qualys enables you to validate the use of strong cryptographic protocols by checking relevant system configuration settings as well as detect instances of insecure cipher used across the systems that are in scope for assessments.	PC CV VM CERT PCI
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.	Qualys enables you to detect wireless access points from within the network and validate the use of appropriate encryptions across the access points.	PC CV VM PCI
4.2	Never send unprotected PANs by end-user messaging technologies (for	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

	example, e-mail, instant messaging, SMS, chat, etc.).		
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 5: Use and regularly update anti-virus software or programs			
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Qualys enables you to validate whether an anti-virus software is installed on the systems that are in scope for assessments.	PC CV PCI
5.1.1	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Qualys enables you to validate whether the installed anti-virus mechanisms are current, perform scans regularly, and generate logs.	PC CV PCI
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
5.2	Ensure that all anti-virus mechanisms are maintained as follows:	Qualys enables you to validate whether the installed anti-virus mechanisms are current, perform scans regularly, and generate logs.	PC CV PCI
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Qualys enables you to check for the current status of the installed anti-virus tools.	PC CV PCI
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 6: Develop and maintain secure systems and applications			
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities.	Qualys VM is the leading vulnerability management solution in the industry that scans systems, generates reports, and prioritizes vulnerabilities on the basis of their criticality.	VM WAS
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.	Qualys enables you to detect missing OS and application patches and security updates. Qualys is constantly updated with new vulnerability information and can be used in a process of tracking newly discovered vulnerabilities.	PC VM PCI PM

6.3	Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.2	Separation of duties between development/test and production environments	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.3	Production data (live PANs) are not used for testing or development	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.4	Removal of test data and accounts from system components before the system becomes active/goes into production.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.5	Change control procedures must include the following:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.5.1	Documentation of impact.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.5.2	Documented change approval by authorized parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.5.4	Back-out procedures.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.4.6	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

6.5	Address common coding vulnerabilities in software-development processes as follows:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.2	Buffer overflows	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.3	Insecure cryptographic storage	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.4	Insecure communications	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.5	Improper error handling	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.6	All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.7	Cross-site scripting (XSS)	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.9	Cross-site request forgery (CSRF)	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.5.10	Broken authentication and session management	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:	Qualys WAS crawls your web applications to analyze threats. It reports and prioritizes the actions that you need to take for remediation.	PCI WAS
6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 7: Restrict access to cardholder data by business need to know			
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	Qualys can analyze database user rights and permissions, looking for broad and insecure permissions.	PC CV

7.1.1	Define access needs for each role, including:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
7.1.3	Assign access based on individual personnel's job classification and function.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
7.1.4	Require documented approval by authorized parties specifying required privileges.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
7.2.1	Coverage of all system components	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
7.2.2	Assignment of privileges to individuals based on job classification and function.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
7.2.3	Default "deny-all" setting.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 8: Assign a unique ID to each person with computer access			
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
8.1.3	Immediately revoke access for any terminated users.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
8.1.4	Remove/disable inactive user accounts within 90 days.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.1.5	Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.2	In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:	Qualys enables you to you detect user accounts with inappropriate authentication settings, such as accounts with no passwords or with blank passwords.	PC CV
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Qualys enables you to detect misconfigurations in system settings to ensure that credentials are properly encrypted.	PC CV
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
8.2.3	Passwords/passphrases must meet the following:	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.2.4	Change user passwords/passphrases at least once every 90 days.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.2.6	Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV

8.4	Document and communicate authentication policies and procedures to all users including:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.5.1	Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:	Qualys can be used to validate an extensive set of user account security settings and password security parameters across systems.	PC CV
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 9: Restrict physical access to cardholder data			
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.1.1	Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to include:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.3	Control physical access for onsite personnel to sensitive areas as follows:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

9.4	Implement procedures to identify and authorize visitors.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.5	Physically secure all media.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.6.1	Classify media so the sensitivity of the data can be determined.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.7	Maintain strict control over the storage and accessibility of media.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.8.1	Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

	storage containers used for materials that are to be destroyed.		
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.9.1	Maintain an up-to-date list of devices. The list should include the following:	Qualys enables you to automate asset detection and inventory management work.	AI
9.9.2	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
9.1	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 10: Track and monitor all access to network resources and cardholder data			
10.1	Implement audit trails to link all access to system components to each individual user.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.2	Implement automated audit trails for all system components to reconstruct the following events:	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.2.1	All individual user accesses to cardholder data	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.2.2	All actions taken by any individual with root or administrative privileges	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.2.3	Access to all audit trails	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.2.4	Invalid logical access attempts	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV

10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.2.6	Initialization, stopping, or pausing of the audit logs	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.2.7	Creation and deletion of system-level objects	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.3	Record at least the following audit trail entries for all system components for each event:	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.3.1	User identification	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.3.2	Type of event	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.3.3	Date and time	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.3.4	Success or failure indication	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.3.5	Origination of event	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.3.6	Identity or name of affected data, system component, or resource.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	Qualys logs and audit trails are time-stamped and synchronized to ensure appropriate logging of events.	PC CV
10.4.1	Critical systems have the correct and consistent time.	Qualys enables you to validate if the systems are pointing to the correct NTP server.	PC CV
10.4.2	Time data is protected.	Qualys enables you to verify system configurations as per your organization's security requirements.	PC CV
10.4.3	Time settings are received from industry-accepted time sources.	Qualys enables you to validate if the systems are pointing to the correct NTP server.	PC CV
10.5	Secure audit trails so they cannot be altered.	Qualys enables you to verify system access.	PC CV
10.5.1	Limit viewing of audit trails to those with a job-related need.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.5.2	Protect audit trail files from unauthorized modifications.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Qualys enables you to detect any unauthorized changes made in files.	FIM
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.6.1	Review the following at least daily:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.6.3	Follow up exceptions and anomalies identified during the review process.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.8	Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.8.1	Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
10.9	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 11: Regularly test security systems and processes			
11.1	Implement processes to test for the presence of wireless access points (802.11) and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI AI

11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.	Qualys enables you to automate asset detection and inventory management work.	AI
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
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).	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI
11.2.1	Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI
11.3	Implement a methodology for penetration testing that includes the following:	Qualys includes active penetration testing that can be automated to run at specific intervals and create reports on the status of all tests, so that you can understand the risks to your network.	VM PCI
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Qualys includes active penetration testing that can be automated to run at specific intervals and create reports on the status of all tests, so that you can understand the risks to your network.	VM PCI
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used	VM PCI

		for both external scanning or ongoing internal scanning.	
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI
11.3.4.1	Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	Qualys enables you to scan for vulnerabilities from inside and outside of your network. Qualys is an Approved Scanning Vendor (ASV) by the PCI Council and can be used for both external scanning or ongoing internal scanning.	VM PCI
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
11.5	Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	Qualys enables you to detect any unauthorized changes made in files.	FIM
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
Requirement 12: Maintain a policy that addresses information security for all personnel			
12.1	Establish, publish, maintain, and disseminate a security policy.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.1.1	Review the security policy at least annually and update the policy when the environment changes.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.2	Implement a risk-assessment process that:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

12.3	Develop usage policies for critical technologies and define proper use of these technologies.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.1	Explicit approval by authorized parties	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.2	Authentication for use of the technology	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.3	A list of all such devices and personnel with access	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.5	Acceptable uses of the technology	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.6	Acceptable network locations for the technologies	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.7	List of company-approved products	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.4	Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.4.1	Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.5	Assign to an individual or team the following information security management responsibilities:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

12.5.1	Establish, document, and distribute security policies and procedures.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.5.4	Administer user accounts, including additions, deletions, and modifications.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.5.5	Monitor and control all access to data.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.6	Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.6.1	Educate personnel upon hire and at least annually.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.8	Maintain and implement policies and procedures to manage service providers, with whom cardholder data is shared, or that could affect the security of cardholder data, as follows	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.8.1	Maintain a list of service providers including a description of the service provided.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.8.3	Ensure there is an established process for engaging service providers	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

	including proper due diligence prior to engagement.		
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.9	Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.1	Implement an incident response plan. Be prepared to respond immediately to a system breach.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.10.2	Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.10.4	Provide appropriate training to staff with security breach response responsibilities.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	Qualys enables you to alert the organization for various security events through multiple modules.	IOC CM FIM CM
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ
12.11	Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

12.11.1	Additional requirement for service providers only: Maintain documentation of quarterly review process to include:	Qualys enables you to have a confirmation on the presence of policy or procedural controls using its survey-based workflow.	SAQ

Qualys, Inc. (NASDAQ: QLYS)
Headquarters
1600 Bridge Parkway
Redwood City, CA 94065 USA
T: 1 (800) 745 4355, info@qualys.

Qualys is a global company with offices around the world. To find an office near you, visit http://www.qualys.com