eSENTIRE

CHECKLIST

# PCI DSS 3.2.1 Checklist for Protecting Payment Account Data

Preparing for, conducting, and reporting the results of a PCI DSS assessment while mitigating risk from an evolving threat landscape with constrained resources can be challenging. At eSentire, we work with organizations to ensure they have systems, processes and controls in place to protect company data and cardholder data.

In this document, we've mapped the PCI DSS 3.2.1 requirements (best practices effective until March 31, 2025) and testing procedures where eSentire can facilitate PCI compliance to help your team maintain compliance standards and mitigate cyber risk.

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Build and Maintain a Secure Network and Systems** | Requirement 1:<br>Install and maintain a firewall configuration to protect cardholder data | 1.1 | Establish and implement firewall and router configuration standards that include the following: (see 1.1.1 - 1.1.7) | eSentire Managed Risk Programs<br>✔ vCISO Security Architecture Review |
| | | 1.1.1 | Establish and implement firewall and router configuration standards that include the following:<br>A formal process for approving and testing all network connections and changes to the firewall and router configurations | |
| | | 1.1.3 | Establish and implement firewall and router configuration standards that include the following:<br>Current diagram that shows all cardholder data flows across systems and networks | |
| | | 1.1.4 | Establish and implement firewall and router configuration standards that include the following:<br>Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone | |
| | | 1.1.5 | Establish and implement firewall and router configuration standards that include the following:<br>Description of groups, roles, and responsibilities for management of network components | |
| | | 1.1.6 | Establish and implement firewall and router configuration standards that include the following:<br>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. | |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Build and Maintain a Secure Network and Systems** | Requirement 1:<br>Install and maintain a firewall configuration to protect cardholder data | 1.1.7 | Establish and implement firewall and router configuration standards that include the following:<br>Requirement to review firewall and router rule sets at least every six months | eSentire Managed Risk Programs<br>✔ vCISO Security Architecture Review |
| | | 1.2 | Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.<br>*Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.* | |
| | | 1.5 | Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| | Requirement 2:<br>Do not use vendor-supplied defaults for system passwords and other security parameters | 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.<br>Sources of industry-accepted system hardening standards may include, but are not limited to:<br>- Center for Internet Security (CIS)<br>- International Organization for Standardization (ISO)<br>- SysAdmin Audit Network Security (SANS) Institute<br>- National Institute of Standards Technology (NIST). | eSentire Managed Risk Programs<br>✔ vCISO Security Architecture Review<br>✔ vCISO Security Policy Review & Guidance |
| | | 2.2.3 | Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.<br>*Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* | eSentire Managed Detection and Response for:<br>✔ Network<br>✔ Endpoint |
| | | 2.2.4 | Configure system security parameters to prevent misuse. | eSentire Managed Detection and Response for:<br>✔ Log |
| | | 2.4 | Maintain an inventory of system components that are in scope for PCI DSS. | eSentire Managed Risk Programs<br>✔ vCISO Vendor Risk Management Program |
| | | 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. | |
| | | 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*. | |
| **Protect Cardholder Data** | Requirement 3:<br>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:<br>- Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements<br>- Specific retention requirements for cardholder data<br>- Processes for secure deletion of data when no longer needed<br>- A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention. | eSentire Managed Vulnerability and Risk<br>✔ vCISO Security Policy review & Guidance |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Protect Cardholder Data** | Requirement 4:<br>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:<br>- Only trusted keys and certificates are accepted.<br>- The protocol in use only supports secure versions or configurations.<br>- The encryption strength is appropriate for the encryption methodology in use.<br>Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.<br>*Examples of open, public networks include but are not limited to:*<br>*- The Internet*<br>*- Wireless technologies, including 802.11 and Bluetooth*<br>*- Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)*<br>*- General Packet Radio Service (GPRS)*<br>*- Satellite communications* | eSentire Managed Detection and Response |
| | | 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. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| **Maintain a Vulnerability Management Program** | Requirement 5:<br>Protect all systems against malware 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). | eSentire Managed Detection and Response for:<br>✔ Endpoint |
| | | 5.1.1 | Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. | |
| | | 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. | |
| | | 5.2 | Ensure that all anti-virus mechanisms are maintained as follows:<br>- Are kept current,<br>- Perform periodic scans<br>- Generate audit logs which are retained per PCI DSS Requirement 10.7. | |
| | | 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.<br>*Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active.* | |
| | | 5.4 | Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Maintain a Vulnerability Management Program** | Requirement 6:<br>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.<br>*Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.*<br>*Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk- assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.* | eSentire Managed Risk Programs<br>✔ vCISO Vulnerability Management Program<br>✔ Internal Vulnerability Scan<br>✔ External Vulnerability Scan<br>✔ Managed Vulnerability Service - Cloud, Co-Managed |
| | | 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.<br>*Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.* | |
| | | 6.3 | Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:<br>- In accordance with PCI DSS (for example, secure authentication and logging)<br>- Based on industry standards and/or best practices.<br>- Incorporating information security throughout the software-development life cycle<br>*Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.* | eSentire Managed Risk Programs<br>✔ Web Application Vulnerability Assessment<br><br>eSentire Managed Detection and Response for:<br>✔ Log |
| | | 6.3.1 | Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers. | |
| | | 6.4.6 | Follow change control processes and procedures for all changes to system components. The processes must include the following:<br>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.<br>*Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | eSentire Managed Risk Programs<br>✔ Internal Vulnerability Scan<br>✔ External Vulnerability Scan |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Maintain a Vulnerability Management Program** | Requirement 6:<br>Develop and maintain secure systems and applications<br>*Note: Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external).*<br>*Note: Requirements 6.5.7 through 6.5.10 apply to web applications and application interfaces (internal or external).* | 6.5 | Address common coding vulnerabilities in software-development processes as follows (see 6.5.1 - 6.5.10):<br>- Train developers at least annually in up- to-date secure coding techniques, including how to avoid common coding vulnerabilities.<br>- Develop applications based on secure coding guidelines.<br>*Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.* | eSentire Managed Risk Programs<br>✔ Internal testing<br>✔ External testing<br>✔ Red Team Exercise<br>✔ Web Application Vulnerability Assessment |
| | | 6.5.1 | Address common coding vulnerabilities in software-development processes as follows:<br>Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws. | |
| | | 6.5.2 | Address common coding vulnerabilities in software-development processes as follows:<br>Buffer overflows | |
| | | 6.5.3 | Address common coding vulnerabilities in software-development processes as follows:<br>Insecure cryptographic storage | |
| | | 6.5.4 | Address common coding vulnerabilities in software-development processes as follows:<br>Insecure communications | |
| | | 6.5.5 | Address common coding vulnerabilities in software-development processes as follows:<br>Improper error handling | |
| | | 6.5.6 | Address common coding vulnerabilities in software-development processes as follows:<br>All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1). | |
| | | 6.5.7 | Address common coding vulnerabilities in software-development processes as follows:<br>Cross-site scripting (XSS) | |
| | | 6.5.8 | Address common coding vulnerabilities in software-development processes as follows:<br>Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions). | |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Maintain a Vulnerability Management Program** | Requirement 6:<br>Develop and maintain secure systems and applications<br>*Note: Requirements 6.5.7 through 6.5.10 apply to web applications and application interfaces (internal or external).* | 6.5.9 | Address common coding vulnerabilities in software-development processes as follows:<br>Cross-site request forgery (CSRF) | eSentire Managed Risk Programs<br>✔ Internal testing<br>✔ External testing<br>✔ Red Team Exercise<br>✔ Web Application Vulnerability Assessment |
| | | 6.5.10 | Address common coding vulnerabilities in software-development processes as follows:<br>Broken authentication and session management. | |
| | | 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:<br>- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes<br>*Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.*<br>- Installing an automated technical solution that detects and prevents web- based attacks (for example, a web- application firewall) in front of public- facing web applications, to continually check all traffic. | |
| | | 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. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| **Implement Strong Access Control Measures** | Requirement 7:<br>Restrict access to cardholder data by business need to know | 7.3 | Ensure that security policies and operational procedures for restricting access tocardholder data are documented, in use, and known to all affected parties. | |
| | Requirement 8:<br>Identify and authenticate access to system components | 8.1.5 | Define and implement policies and procedures to ensure proper user identification management for non- consumer users and administrators on all system components as follows:<br>Manage IDs used by third parties to access, support, or maintain system components via remote access as follows:<br>- Enabled only during the time period needed and disabled when not in use.<br>- Monitored when in use. | eSentire Managed Detection and Response for:<br>✔ Log |
| | | 8.4 | Document and communicate authentication policies and procedures to all users including:<br>- Guidance on selecting strong authentication credentials<br>- Guidance for how users should protect their authentication credentials<br>- Instructions not to reuse previously used passwords<br>- Instructions to change passwords if there is any suspicion the password could be compromised. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| | | 8.8 | Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties. | |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Regularly Monitor and Test Networks** | Requirement 10:<br>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. | eSentire Managed Detection and Response for:<br>✔ Log |
| | | 10.2 | Implement automated audit trails for all system components to reconstruct the following events: (see 10.2.1 - 10.2.7) | |
| | | 10.2.1 | Implement automated audit trails for all system components to reconstruct the following events:<br>All individual user accesses to cardholder data | |
| | | 10.2.2 | Implement automated audit trails for all system components to reconstruct the following events:<br>All actions taken by any individual with root or administrative privileges | |
| | | 10.2.3 | Implement automated audit trails for all system components to reconstruct the following events:<br>Access to all audit trails | |
| | | 10.2.4 | Implement automated audit trails for all system components to reconstruct the following events:<br>Invalid logical access attempts | |
| | | 10.2.5 | Implement automated audit trails for all system components to reconstruct the following events:<br>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 | |
| | | 10.2.6 | Implement automated audit trails for all system components to reconstruct the following events:<br>Initialization, stopping, or pausing of the audit logs | |
| | | 10.2.7 | Implement automated audit trails for all system components to reconstruct the following events:<br>Creation and deletion of system- level objects | |
| | | 10.3 | Record at least the following audit trail entries for all system components for each event: (see 10.3.1 - 10.3.6) | |
| | | 10.3.1 | Record at least the following audit trail entries for all system components for each event:<br>User identification | |
| | | 10.3.2 | Record at least the following audit trail entries for all system components for each event:<br>Type of event | |
| | | 10.3.3 | Record at least the following audit trail entries for all system components for each event:<br>Date and time | |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Regularly Monitor and Test Networks** | Requirement 10:<br>Track and monitor all access to network resources and cardholder data | 10.3.4 | Record at least the following audit trail entries for all system components for each event:<br>Success or failure indication | eSentire Managed Detection and Response for:<br>✔ Log |
| | | 10.3.5 | Record at least the following audit trail entries for all system components for each event:<br>Origination of event | |
| | | 10.3.6 | Record at least the following audit trail entries for all system components for each event:<br>Identity or name of affected data, system component, or resource. | |
| | | 10.5 | Secure audit trails so they cannot be altered. | |
| | | 10.5.1 | Limit viewing of audit trails to those with a job-related need. | |
| | | 10.5.2 | Protect audit trail files from unauthorized modifications. | |
| | | 10.5.3 | Promptly back up audit trail files to a centralized log server or media that is difficult to alter. | |
| | | 10.5.4 | Write logs for external-facing technologies onto a secure, centralized, internal log server or media device. | |
| | | 10.6 | Review logs and security events for all system components to identify anomalies or suspicious activity.<br>*Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.* | |
| | | 10.6.1 | Review the following at least daily:<br>- All security events<br>- Logs of all system components that store, process, or transmit CHD and/or SAD<br>- Logs of all critical system components<br>- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/ intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.). | |
| | | 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. | |
| | | 10.6.3 | Follow up exceptions and anomalies identified during the review process. | |
| | | 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). | |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Regularly Monitor and Test Networks** | Requirement 10:<br>Track and monitor all access to network resources and cardholder data | 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:<br>- Firewalls<br>- IDS/IPS<br>- FIM<br>- Anti-virus<br>- Physical access controls<br>- Logical access controls<br>- Audit logging mechanisms<br>- Segmentation controls (if used)<br>*Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | eSentire Managed Detection and Response |
| | | 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:<br>- Restoring security functions<br>- Identifying and documenting the duration (date and time start to end) of the security failure<br>- Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause<br>- Identifying and addressing any security issues that arose during the failure<br>- Performing a risk assessment to determine whether further actions are required as a result of the security failure<br>- Implementing controls to prevent cause of failure from reoccurring<br>- Resuming monitoring of security controls<br>*Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | |
| | | 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. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| | Requirement 11:<br>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.<br>*Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.*<br>*Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.* | eSentire Managed Risk Programs<br>✔ Internal testing<br>✔ External testing |
| | | 11.1.2 | Implement incident response procedures in the event unauthorized wireless access points are detected. | eSentire Managed Risk Programs<br>✔ vCISO Security Incident Response Planning |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Regularly Monitor and Test Networks** | Requirement 11:<br>Regularly test security systems and processes. | 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).<br>*Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.*<br>*For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.* | eSentire Managed Risk Programs<br>✔ vCISO Vulnerability Management Program<br>✔ Internal Vulnerability Scan<br>✔ External Vulnerability Scan |
| | | 11.2.1 | Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel. | |
| | | 11.2.2 | 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.<br>*Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).*<br>*Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.* | |
| | | 11.2.3 | Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. | |
| | | 11.3 | Implement a methodology for penetration testing that includes the following:<br>- Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)<br>- Includes coverage for the entire CDE perimeter and critical systems<br>- Includes testing from both inside and outside the network<br>- Includes testing to validate any segmentation and scope-reduction controls<br>- Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5<br>- Defines network-layer penetration tests to include components that support network functions as well as operating systems<br>- Includes review and consideration of threats and vulnerabilities experienced in the last 12 months<br>- Specifies retention of penetration testing results and remediation activities results. | eSentire Managed Risk Programs<br>✔ Internal Vulnerability Scan<br>✔ External Vulnerability Scan<br>✔ Red Team Exercise |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Regularly Monitor and Test Networks** | Requirement 11:<br>Regularly test security systems and processes. | 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). | eSentire Managed Risk Programs<br>✔ Internal Vulnerability Scan<br>✔ External Vulnerability Scan<br>✔ Red Team Exercise |
| | | 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). | |
| | | 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. | |
| | | 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.<br>*Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | |
| | | 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.<br>Keep all intrusion-detection and prevention engines, baselines, and signatures up to date. | eSentire Managed Detection and Response for:<br>✔ Network<br>✔ Endpoint<br>✔ Log |
| | | 11.6 | Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| **Maintain an Information Security Policy** | Requirement 12:<br>Maintain a policy that addresses information security for all personnel. | 12.1 | Establish, publish, maintain, and disseminate a security policy. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance<br>✔ vCISO Security Incident Response Planning |
| | | 12.1.1 | Review the security policy at least annually and update the policy when the environment changes. | |
| | | 12.2 | Implement a risk-assessment process that:<br>- Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),<br>- Identifies critical assets, threats, and vulnerabilities, and<br>- Results in a formal, documented analysis of risk.<br>*Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.* | eSentire Managed Risk Programs<br>✔ vCISO Security Program Maturity Assessment |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Maintain an Information Security Policy** | Requirement 12:<br>Maintain a policy that addresses information security for all personnel. | 12.3 | Develop usage policies for critical technologies and define proper use of these technologies.<br>*Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.*<br>*Ensure these usage policies require the following: (see 12.3.1 - 12.3.10)* | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| | | 12.3.1 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>Explicit approval by authorized parties | |
| | | 12.3.2 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>Authentication for use of the technology | |
| | | 12.3.3 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>A list of all such devices and personnel with access.<br>*Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.*<br>*Ensure these usage policies require the following: (see 12.3.1 - 12.3.10)* | |
| | | 12.3.4 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices) | |
| | | 12.3.5 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>Authentication for use of the technology | |
| | | 12.3.6 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>Acceptable network locations for the technologies | |
| | | 12.3.7 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>List of company-approved products | |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Maintain an Information Security Policy** | Requirement 12:<br>Maintain a policy that addresses information security for all personnel. | 12.3.8 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| | | 12.3.9 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use | eSentire Managed Risk Programs<br>✔ vCISO Vendor Risk Management Program |
| | | 12.3.10 | Develop usage policies for critical technologies and define proper use of these technologies.<br>Ensure these usage policies require the following:<br>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.<br>Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance |
| | | 12.4 | Ensure that the security policy and procedures clearly define information security responsibilities for all personnel. | |
| | | 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:<br>- Overall accountability for maintaining PCI DSS compliance<br>- Defining a charter for a PCI DSS compliance program and communication to executive management<br>*Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.* | |
| | | 12.5 | Assign to an individual or team the following information security management responsibilities: | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance<br>✔ vCISO Security Incident Response Planning |
| | | 12.5.1 | Assign to an individual or team the following information security management responsibilities:<br>Establish, document, and distribute security policies and procedures. | |
| | | 12.5.2 | Assign to an individual or team the following information security management responsibilities:<br>Monitor and analyze security alerts and information, and distribute to appropriate personnel. | |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Maintain an Information Security Policy** | Requirement 12:<br>Maintain a policy that addresses information security for all personnel. | 12.5.3 | Assign to an individual or team the following information security management responsibilities:<br>Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. | eSentire Managed Risk Programs<br>✔ vCISO Security Policy Review & Guidance<br>✔ vCISO Security Incident Response Planning |
| | | 12.5.4 | Assign to an individual or team the following information security management responsibilities:<br>Administer user accounts, including additions, deletions, and modifications. | |
| | | 12.5.5 | Assign to an individual or team the following information security management responsibilities:<br>Monitor and control all access to data. | |
| | | 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: (see 12.8.1 - 12.8.5) | eSentire Managed Risk Programs<br>✔ vCISO Vendor Risk Management Program |
| | | 12.8.1 | 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:<br>Maintain a list of service providers including a description of the service provided. | |
| | | 12.8.2 | 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:<br>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.<br>*Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party.*<br>*The acknowledgement does not have to include the exact wording provided in this requirement.* | |
| | | 12.8.3 | 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:<br>Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. | |
| | | 12.8.4 | 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:<br>Maintain a program to monitor service providers' PCI DSS compliance status at least annually. | |

| Category | Requirements | Sections | Testing Procedures | eSentire Services |
|---|---|---|---|---|
| **Maintain an Information Security Policy** | Requirement 12:<br>Maintain a policy that addresses information security for all personnel. | 12.8.5 | 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:<br>Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. | eSentire Managed Risk Programs<br>✔ vCISO Vendor Risk Management Program |
| | | 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.<br>*Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.* | |
| | | 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:<br>- Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum<br>- Specific incident response procedures<br>- Business recovery and continuity procedures<br>- Data backup processes<br>- Analysis of legal requirements for reporting compromises<br>- Coverage and responses of all critical system components<br>- Reference or inclusion of incident response procedures from the payment brands. | eSentire Managed Risk Programs<br>✔ vCISO Security Incident Response Planning |
| | | 12.10.2 | Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually. | |
| | | 12.10.3 | Designate specific personnel to be available on a 24/7 basis to respond to alerts. | |
| | | 12.10.4 | Provide appropriate training to staff with security breach response responsibilities. | |
| | | 12.10.5 | Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems. | |
| | | 12.10.6 | Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. | |

Our cybersecurity services portfolio is designed to stop breaches, simplify security and minimize business risk. We provide around-the-clock threat protection that is proactive, personalized and cost effective to put your business ahead of disruption.

## Managed Risk Services

TAKE CONTROL OF CYBER RISK

Strategic services including Vulnerability Management, vCISO and Managed Phishing & Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

## Managed Detection & Response

PREVENT THREATS BECOMING BUSINESS DISRUPTING EVENTS

We deliver Response + Remediation you can trust. By combining our cutting-edge XDR platform, 24/7 threat hunting and security operations leadership, we hunt and disrupt known and unknown threats before they impact your business.

## Incident Response & Digital Forensics

BE READY WITH THE WORLD'S FASTEST THREAT SUPPRESSION

Battle-tested Incident Commander level expertise, crime scene reconstruction and digital forensics investigations that can bear scrutiny in a court of law. The world's fastest threat suppression with a 4-hour SLA available with our IR Retainer.

## Reach out to connect with an eSentire security specialist.

**Get Started**

If you're experiencing a security incident or breach contact us  1-866-579-2200

eSENTIRE

eSentire is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts & Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.