PCI-DSS Compliance for Services

Sl. No.	Services	PCI-DSS Control Number	Description
1	24x7 Security Operation Center – Implementation and Finetuning	10.4.1	The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).
		10.4.1.1	Automated mechanisms are used to perform audit log reviews.
		A3.5.1	A methodology is implemented for the prompt identification of attack patterns and undesirable behaviour across systems that includes: • Identification of anomalies or suspicious activity as it occurs. • Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel.• Response to alerts in accordance with documented response procedures.
2	24x7 Security Operation Center – Active Monitoring	10.4.1	The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).
		10.4.1.1	Automated mechanisms are used to perform audit log reviews.
		11.5.1	Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.
		A3.5.1	A methodology is implemented for the prompt identification of attack patterns and undesirable behavior across systems that includes: • Identification of anomalies or suspicious activity as it occurs. • Issuance of prompt alerts upon detection of suspicious activity or anomaly to responsible personnel. • Response to alerts in accordance with documented response procedures.
3	Security Advisory services	2.1.1	All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.
		2.1.2	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.
		2.2.1	Configuration standards are developed, implemented, and maintained to: • Cover all system components.

			• Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.
4	Threat Hunting Services	10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.
5	Cyber Emergency Response	10.7.3	Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.
		11.2.2	An inventory of authorized wireless access points is maintained, including a documented business justification.
		12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.
		12.10.3	Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.
		12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.
6	Active Vulnerability Management – External Network	6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections
		6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at

			least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert
		11.4.1	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities result for at least 12 months
		11.4	External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected
7	Active Vulnerability Management – Internal Network	6.1	Establish a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking (e.g. “high,” “medium,” or “low”) to newly discovered security vulnerabilities.
		6.2	Protect all system components and software from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
		6.3	Develop internal and external software applications including web-based administrative access to applications in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle. This applies to all software developed internally as well as bespoke or custom software developed by a third party
		6.5	Prevent common coding vulnerabilities in software development processes by training developers in secure coding techniques and developing application
8	Active Penetration testing – Full Blackbox/Greybox	11.4.3	External penetration testing is performed: • Per the entity’s defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester
		11.4.4	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity’s assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.
9		11.4.3	External penetration testing is performed: • Per the entity’s defined methodology

	Active Penetration testing – Periodic Scans		• At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester
		11.4.4	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.
		11.4.5	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).
10	Threat intelligence service	6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.
11	Red & Purple team activities	11.4.3	External penetration testing is performed: • Per the entity's defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester
		11.4.4	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity's assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.
12	OSINT Threat Exposure Assessment	1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties.
		2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.
		2.3.1	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points.

			• SNMP defaults. • Any other security-related wireless vendor
13	Threat Modeling	1.2.5	All services, protocols, and ports allowed are identified, approved, and have a defined business need.
		1.2.6	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.
		1.2.8	Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.
14	Wireless Penetration Testing	2.3	Wireless environments are configured and managed securely.
		2.3.1	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-
15	Security Configuration Assessment	1.1.1	All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.
		1.2.1	Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.
		1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks
		1.2.5	All services, protocols, and ports allowed are identified, approved, and have a defined business need.
		1.2.6	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.
		2.2.1	Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component
16	Active Attack Surface Monitoring	1.4.2	Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.

		1.4.3	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.
		10.3.4	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.
		10.2.1	Audit logs are enabled and active for all system components and cardholder data.
		10.4.1	The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).
17	Malware Analysis	10.2.1.7	Audit logs capture all creation and deletion of system-level objects.
		11.5.1	Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.
18	Cyber Forensics	10.6.1	System clocks and time are synchronized using time-synchronization technology
		12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.
19	Response Readiness Assessment	12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.
		12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.
		12.10.2	At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.