PCI DSS v4.0 变更系列之八

——第五大类要求点

要求点变更的说明之第五大类：定期监控和测试网络

要求 10：记录监控系统组件和持卡人数据的所有访问权限

要求 10 的主要变化体现在如下两个要求点：

要求 10.4.1.1 从允许人工每日审计，变为自动化审计机制。

对于非关键事件，要求 10.4.2.1 允许通过风险评估，确定其检查的频率。

v4.0 要求点的英文原文	对应的 v3.2.1 要求	与 v3.2.1 的变化/新要求说明
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.		
10.1.1 All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	8.8	在原 10.9 要求的基础上，增加了策略和流程需要保持更新的要求。
10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	新要求	记录、分配及理解执行要求 10 的管理活动所对应的角色及职责。
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	10.1 10.2	在原要求 10.1 和 10.2 的基础上，更新了描述。
10.2.1.1 Audit logs capture all individual user access to cardholder data.	10.2.1	在原要求 10.2.1 的基础上，更新了描述。
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	10.2.2	在原要求 10.2.2 的基础上，更新了描述。强调此要求也包括对应用或系统账号的交互操作。
10.2.1.3 Audit logs capture all access to audit logs.	10.2.3	在原要求 10.2.3 的基础上，更新了描述。
10.2.1.4 Audit logs capture all invalid logical access attempts.	10.2.4	在原要求 10.2.4 的基础上，更新了描述。

10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	10.2.5	在原要求 10.2.5 的基础上，更新了描述。
10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	10.2.6	在原要求 10.2.6 的基础上，更新了描述。
10.2.1.7 Audit logs capture all creation and deletion of system-level objects.	10.2.7	在原要求 10.2.7 的基础上，更新了描述。
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	10.3-10.3.6	将原来的日志记录的具体内容的要求，合并为一个要求。
10.3 Audit logs are protected from destruction and unauthorized modifications.		
10.3.1 Read access to audit logs files is limited to those with a job-related need.	10.5.1	在原要求 10.5.1 的基础上，更新了描述。强调对审计日志只能给予读的权限。
10.3.2 Audit log files are protected to prevent modifications by individuals.	10.5.2	在原要求 10.5.2 的基础上，更新了描述。
10.3.3 Audit log files, including those for external- facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	10.5.3 10.5.4	把原要求 10.5.3 和 10.5.4 进行了合并。
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.	10.5.5	在原要求 10.5.5 的基础上，更新了描述。
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.		

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).	10.6.1	在原要求 10.6.1 的基础上，更新了描述。
10.4.1.1 Automated mechanisms are used to perform audit log reviews.	新要求	该要求在 2025 年 3 月 31 日后变为强制。要求使用自动化机制进行日志审查。
10.4.2 Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	10.6.2	在原要求 10.6.2 的基础上，更新了描述。
10.4.2.1 The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	新要求	该要求在 2025 年 3 月 31 日后变为强制。 对于非关键日志的审查的频率，要求通过风险评估流程进行确定。
10.4.3 Exceptions and anomalies identified during the review process are addressed.	10.6.3	在原要求 10.6.3 的基础上，更新了描述。
10.5 Audit log history is retained and available for analysis.		
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	10.7	在原要求 10.7 的基础上，更新了描述。
10.6 Time-synchronization mechanisms support consistent time settings across all systems.		
10.6.1 System clocks and time are synchronized using time-synchronization technology.	10.4	在原要求 10.4 的基础上，更新了描述。
10.6.2 Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is	10.4.1 10.4.3	将原来 10.4.1 和 10.4.3 关于时间同步的架构的要求进行了合并。

based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).		
10.6.3 Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	10.4.2	在原要求 10.4.2 的基础上，更新了描述。
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.		
10.7.1 ***Additional requirement for service providers only:*** Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used).	10.8	在原要求 10.8 的基础上，更新了描述。
10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls.	新要求	该要求在 2025 年 3 月 31 日后变为强制。 要求所有的机构均实施该控制，并且增加了对日志审查机制和自动安全测试工具的失效响应要求。

• Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used).		
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.	10.8.1	在原要求 10.8.1 的基础上，更新了描述。 同时，对于服务供应商以外的合规机构，该要求在 2025 年 3 月 31 日后将变为强制。

要求 11：定期测试系统和网络的安全性

与 v.3.2.1 版本的要求 11 相比，新版本的要求趋严，主要体现在如下要求点：

要求 11.3.1.1 对于非紧急、非高危的漏洞修复，应基于风险评估所定义的修复周期展开。

要求 11.3.1.2 对于内部漏扫，需要使用认证登陆的方法进行。

要求 11.3.2.1 对于外部漏扫，CVSS4.0 及以上的漏洞必须修复。

要求 11.5.1 入侵检测机制，应识别、告警和处理隐秘的恶意软件通讯。

要求 11.6.1 对支付页面的非授权访问进行识别、告警和响应。

v4.0 要求点的英文原文	对应的 v3.2.1 要求	与 v3.2.1 的变化/新要求说明
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.		
11.1.1 All security policies and operational procedures that are identified in Requirement 11 are: • Documented.	11.6	在原 11.6 要求的基础上，增加了策略和流程需要保持更新的要求。

• Kept up to date. • In use. • Known to all affected parties.		
11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	新要求	记录、分配及理解执行要求 11 的管理活动所对应的角色及职责。
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.		
11.2.1 Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.	11.1	在原要求 11.1 的基础上，更新了描述。
11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.	11.1.1	在原要求 11.1.1 的基础上，更新了描述。
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.		
11.3.1.1 All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed.	新要求	该要求在 2025 年 3 月 31 日后变为强制。要求通过风险评估确定修复周期来处理非紧急/高危的漏洞，并要求重新扫描以确定得到修复。
11.3.1.2 Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used for those systems that accept credentials for scanning.	新要求	该要求在 2025 年 3 月 31 日后变为强制。对漏洞扫描的过程提出了额外要求： 不能进行登陆认证扫描的系统应进行记录 应使用足够的特权进行登陆认证扫描。 进行交互登陆的账号不能是共享、组和通用账号。

• If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.		
11.3.1.3 Internal vulnerability scans are performed after any significant change as follows: • High-risk and critical vulnerabilities (per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	11.2.3	将原 11.2.3 的要求拆分为内部和外部的外部重大变更后进行扫描的要求。此处是对内部的重大变更，要求按 6.3.1 的漏洞评级为高危和紧急的漏洞必须解决，并进行修复验证。
11.3.2 External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan.	11.2.2	在原要求 11.2.2 的基础上，更新了描述。
11.3.2.1 External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	11.2.3	将原 11.2.3 的要求拆分为内部和外部的外部重大变更后进行扫描的要求。此处是对外部的重大变更，要求 CVSS4.0 必须解决，并进行修复验证。
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		

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 results for at least 12 months.	11.3	在原要求 11.3 的基础上，更新了描述。进一步澄清了对方法论的定义、记录与实施，测试结果要保留至少一年，记录对发现的漏洞进行评估和解决的方法。
11.4.2 Internal 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 exists (not required to be a QSA or ASV).	11.3.2	在原要求 11.3.2 的基础上，更新了描述。
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	11.3.1	在原要求 11.3.1 的基础上，更新了描述。

application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV).		
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.	11.3.3	在原要求 11.3.3 的基础上，更新了描述。澄清了基于要求 6.3.1 的评估结果进行漏洞修复。
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).	11.3.4	在原要求 11.3.4 的基础上，更新了描述。
11.4.6 ***Additional requirement for service providers only:*** If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation	11.3.4.1	在原要求 11.3.4.1 的基础上，更新了描述。

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).		
11.4.7 ***Additional requirement for multi-tenant service providers only:*** Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4.	新要求	该要求在2025年3月31日后变为强制。对多租户的服务供应商，要求其支持客户的内外部渗透测试。
11.5 Network intrusions and unexpected file changes are detected and responded to.		
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.	11.4	在原要求11.4的基础上，更新了描述。
11.5.1.1 ***Additional requirement for service providers only:*** Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels.	新要求	该要求在2025年3月31日后变为强制。要求通过入侵检测机制对隐秘的恶意软件通讯进行识别、报警和处理。
11.5.2 A change-detection mechanism (for	11.5	在原要求11.5的基础上，更新了描述。

example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.		
11.6 Unauthorized changes on payment pages are detected and responded to.		
11.6.1 A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. • The mechanism functions are performed as follows: – At least once every seven days **OR** – Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).	新要求	该要求在 2025 年 3 月 31 日后变为强制。要求实施支付页面的非授权更改控制机制，进行告警、分析并定期评估。