PCI DSS v4.0 变更系列之九

——第六大类要求点

要求点变更的说明之第六大类：使用组织政策和计划支持信息安全

要求 12：使用组织政策和计划支持信息安全

要求 12 在 v4.0 版本也增加了安全管理方面的要求，主要体现在：

要求 12.3.1-12.3.2 涉及到标准中可自行决定频率的点，通过该要求进行风险评估并确定适合的频率。

要求 12.3.3 对所使用的加密套件的维护要求。

要求 12.3.4 对所使用的硬软件技术的维护要求。

要求 12.5.2 对 PCI DSS 范围的维护要求。

要求 12.6.3.1-12.6.3.2 对安全意识培训的内容要求。

要求 12.10.7 强调在任何时候发现未知的持卡人数据存储位置时应采取的应急响应流程。

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
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.		
12.1.1 An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	12.1	在原 12.1 要求的基础上，增加了策略和流程需要保持更新的要求。
12.1.2 The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.	新要求	记录、分配及理解执行要求 12 的管理活动所对应的角色及职责。
12.1.3 The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	12.4	在原要求 12.4 的基础上，更新了描述。

12.1.4 Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	12.5-12.5.5	对原要求的 12.5-12.5.5 进行了合并，强调安全管理的责任在 CISO 或管理层。
12.2 Acceptable use policies for end-user technologies are defined and implemented.		
12.2.1 Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.	12.3-12.3.9	对原要求的 12.5-12.5.5 进行了合并，强调此要求针对终端用户技术的使用。
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.		
12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review.	新要求	该要求在 2025 年 3 月 31 日后变为强制。对于涉及到灵活执行频率的要求点，应通过风险评估的方法进行确定。具体的分析方法包括但不限于： 识别保护的资产。 识别相应的威胁。 识别影响威胁事件发生可能性的因素。 降低发生可能性的频率分析。 至少每年确定一次以及风险的变化进行调整。
12.3.2 A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include:	新要求	该要求在 2025 年 3 月 31 日后变为强制。对于用定制化方法的风险评估，要求记录相应的证据、高层批准以及至少每年分析一次相应的风险。

• Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.		
12.3.3 Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	新要求	该要求在 2025 年 3 月 31 日后变为强制。对于涉及加密套件使用的情况，要求维护并更新加密套件清单、监控业界趋势以及对密码学漏洞的响应处理战略。
12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	新要求	该要求在 2025 年 3 月 31 日后变为强制。对于所使用的硬件和软件技术，每年进行一次评估。
12.4 PCI DSS compliance is managed.		

12.4.1 ***Additional requirement for service providers only:*** Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program and communication to executive management.	12.4.1	在原要求 12.4.1 的基础上，更新了描述。
12.4.2 ***Additional requirement for service providers only:*** Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes.	12.11	在原要求 12.11 的基础上，更新了描述。
12.4.2.1 ***Additional requirement for service providers only:*** Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. • Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.	12.11.1	在原要求 12.11.1 的基础上，更新了描述。
12.5 PCI DSS scope is documented and validated.		
12.5.1 An inventory of system components that are in scope for PCI DSS, including a	2.4	在原要求 2.4 的基础上，更新了描述。

description of function/use, is maintained and kept current.		
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.	新要求	该要求立即生效。要求每年评估并记录 PCI DSS 的范围。包括但不限于： 数据流向的识别与维护。 涉及站点。 系统组件。 分隔控制。 第三方连接。
12.5.2.1 ***Additional requirement for service providers only:*** PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping	新要求	该要求在 2025 年 3 月 31 日后变为强制。要求供应商在发生重大变更、每半年一次确定和记录 PCI DSS 范围。

validation includes all the elements specified in Requirement 12.5.2.		
12.5.3 ***Additional requirement for service providers only:*** Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management.	新要求	该要求在 2025 年 3 月 31 日后变为强制。要求供应商在发生组织结构重大变化时记录对 PCI DSS 范围和相应控制的影响。
12.6 Security awareness education is an ongoing activity.		
12.6.1 A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	12.6.2	在原要求 12.6.2 的基础上，更新了描述。
12.6.2 The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data.	新要求	该要求在 2025 年 3 月 31 日后变为强制。具体指出了安全意识项目至少每年检查一次、更新并基于新威胁和脆弱性解决组织面临的问题。
12.6.3 Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	12.6.1	在原要求 12.6.1 的基础上，更新了描述。
12.6.3.1 Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering.	新要求	该要求在 2025 年 3 月 31 日后变为强制。具体指出了安全意识项目应包括影响 CDE 的威胁和脆弱性的内容，比如钓鱼攻击、社会工程学等。

12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	新要求	该要求在 2025 年 3 月 31 日后变为强制。具体指出了安全意识培训应包括对终端技术的安全使用方法。
12.7 Personnel are screened to reduce risks from insider threats.		
12.7.1 Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	12.7	在原要求 12.7 的基础上，更新了描述。
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.		
12.8.1 A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	12.8.1	在原要求 12.8.1 的基础上，更新了描述。将原来的“服务供应商”的说法，调整为“第三方服务供应商”，使得要求的适用更明确。
12.8.2 Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity’s CDE.	12.8.2	在原要求 12.8.2 的基础上，更新了描述。将原来的“服务供应商”的说法，调整为“第三方服务供应商”，使得要求的适用更明确。
12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	12.8.3	在原要求 12.8.3 的基础上，更新了描述。将原来的“服务供应商”的说法，调整为“第三方服务供应商”，使得要求的适用更明确。
12.8.4 A program is implemented to monitor TPSPs’ PCI DSS compliance status at least once every 12 months.	12.8.4	在原要求 12.8.5 的基础上，更新了描述。将原来的“服务供应商”的说法，调整为“第三方服务供应商”，使得要求的适用更明确。
12.8.5 Information is maintained about which PCI DSS requirements are managed by each	12.8.5	在原要求 12.8.5 的基础上，更新了描述。将原来的“服务供应商”的说

TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.		法，调整为“第三方服务供应商”，使得要求的适用更明确。
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.		
12.9.1 ***Additional requirement for service providers only:*** TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP 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 CDE.	12.9	在原要求 12.9 的基础上，更新了描述。将原来的“服务供应商”的说法，调整为“第三方服务供应商”，使得要求的适用更明确。
12.9.2 ***Additional requirement for service providers only:*** TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).	新要求	该要求立即生效，要求服务供应商在客户需要时提供 12.8.4-12.8.5 的相应信息。
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.		
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.	12.10.1	在原要求 12.10.1 的基础上，更新了描述。

• 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.	12.10.2	在原要求 12.10.2 的基础上，更新了描述。
12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	12.10.3	在原要求 12.10.3 的基础上，更新了描述。
12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	12.10.4	在原要求 12.10.4 的基础上，更新了描述。
12.10.4.1 The frequency of periodic training for incident response personnel 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。具体指出了基于 12.3.1 的要求确定应急响应人员培训的频率。
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Detection of unauthorized wireless access points.	11.1.2 11.5.1 12.10.5	综合原要求 11.1.2，11.5.1，12.10.5 的要求，整合为统一的要求点。同时增加了对支付页面变更及改动探测机制的响应。

12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	12.10.6	在原要求 12.10.6 的基础上，更新了描述。
12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	新要求	该要求在 2025 年 3 月 31 日后变为强制。强调在任何时候发现未知的持卡人数据存储位置时应采取的应急响应流程。包括但不限于： 发现后确定如何操作。 确定是否有敏感认证数据一同存储。 确定账户数据从哪来以及如何闭环的。 修正数据泄露的问题及流程上的缺陷。

要求 A1：针对多租户服务供应商的额外 PCI DSS 要求

A1 的要求对象，从 v3.2.1 的共享的主机托管商变为 v4.0 的多租户服务供应商。在概要部分进行了多租户服务供应商的说明与澄清。

该章节增加了新的要求 A1.1.1，A1.1.4 和 A1.2.3，这三个要求均是将在 2024 年 3 月 31 日后变为强制要求。其中 A1.1.1 要求实施供应商环境与客户环境的逻辑分离；要求 A1.1.4 通过渗透测试的方法确认逻辑分离的有效性；要求 A1.2.3 强调对可疑和确认的安全事件和漏洞的报告流程与处理机制。