PCI DSS v4.0 变更系列之六

——第三大类要求点

要求点变更的说明之第三大类：维护漏洞管理计划

要求 5：保护所有系统和网络免受恶意软件侵害

要求 5.2.3 和 5.2.3.1 增加了灵活性，通过风险评估流程确定评估不受恶意软件影响的系统组件的频率。

要求 5.3.2 和 5.3.2.1 增加了基于风险评估流程确定磁盘扫描执行的频率。

要求 5.3.3 增加了对可移动介质的防恶意软件要求。

要求 5.4.1 增加了防止钓鱼攻击的要求。

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
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.		
5.1.1 All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	5.4	在原 5.4 要求的基础上，增加了策略和流程需要保持更新的要求。
5.1.2 Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	新要求	记录、分配及理解执行要求 5 的管理活动所对应的角色及职责。
5.2 Malicious software (malware) is prevented, or detected and addressed.		
5.2.1 An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	5.1	对原 5.1 的要求重新进行了描述。
5.2.2 The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	5.1.1	对原 5.1.1 的要求重新进行了描述。
5.2.3 Any system components that are not at risk for malware are evaluated periodically to include the following:	5.1.2	在原 5.1.2 要求的基础上，强调重点在于不受恶意软件影响的系统组件，定期评估提出了具体的记录系统组件、识别恶意软

• A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.		件的影响及确认是否继续不进行恶意软件防护等细节要求。
5.2.3.1 The frequency of periodic evaluations of system components identified as not at risk for malware 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	基于风险评估的目标，确定对要求 5.2.3 的执行频率。
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.		
5.3.1 The anti-malware solution(s) is kept current via automatic updates.	5.2	对原 5.2 要求进行了拆分，此要求覆盖防恶意软件的特征更新的要求。
5.3.2 The anti-malware solution(s): • Performs periodic scans and active or real-time scans. **OR** • Performs continuous behavioral analysis of systems or processes.	5.2	对原 5.2 要求进行了拆分，此要求覆盖定期磁盘扫描的要求。
5.3.2.1 If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans 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	基于风险评估的目标，确定对要求 5.3.2 定期扫描的执行频率。
5.3.3 For removable electronic media, the anti- malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, **OR** • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	新要求	添加对可移动电子介质的扫描与行为分析的要求。

5.3.4 Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	5.2	对原 5.2 要求进行了拆分，此要求覆盖日志启用与保存的要求。
5.3.5 Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	5.3	对原 5.3 的要求重新进行了描述。
5.4 Anti-phishing mechanisms protect users against phishing attacks.		
5.4.1 Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	新要求	对钓鱼攻击的防护流程与自动机制的要求。

要求 6：开发和维护安全系统和软件

要求 6 的主要变化体现在如下要求点:

要求 6.3.2 提出对软件及组件的维护，要求纳入到漏洞管理中。

要求 6.4.2 提到了向自动化的 web 攻击检测机的过渡。

要求 6.4.3 提及了对支付页面的保护要求。

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
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.		
6.1.1 All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	6.7	在原 6.7 要求的基础上，增加了策略和流程需要保持更新的要求。
6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	新要求	记录、分配及理解执行要求 6 的管理活动所对应的角色及职责。
6.2 Bespoke and custom software are developed securely.		

6.2.1 Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	6.3	将原 6.3 要求中的“内部和外部软件”的要求，调整为“定制软件”的要求。声明这个要求并不适用于第三方开发商。
6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.	6.5	将原 6.5 要求进一步进行了澄清，提出了至少每年一次的要求，针对软件开发相关人员，包括软件工具使用等内容。
6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	6.3.2	将原 6.3.2 的要求进行了拆分，此要求针对自动化工具和人工代码审核的情况。
6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. • Reviewed and approved by management prior to release.	6.3.2	将原 6.3.2 的要求进行了拆分，此要求针对人工代码审核的额外要求。

6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP , XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client- side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.	6.5.1 6.5.2 6.5.3 6.5.4 6.5.5 6.5.6 6.5.7 6.5.8 6.5.9 6.5.10	原 6.5.1-6.5.10 要求的攻击类型，合并为该要求。该要求研究软件工程技术及方法，以阻止所列出的常见的软件问题 。
6.3 Security vulnerabilities are identified and addressed.		
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	6.1	在原 6.1 要求的基础上，声明安全漏洞的管理要求适用于自制软件以及第三方软件。

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 a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.		
6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	新要求	对涉及的自制软件以及所集成的第三方组件进行维护，以用于漏洞和补丁管理。
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	6.2	对原 6.2 的要求重新进行了描述。
6.4 Public-facing web applications are protected against attacks.		
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.	6.6	对原 6.6 的要求重新进行了描述。

– 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 **OR** • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications 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 that is immediately investigated.		
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 that is immediately investigated.	新要求	对原 6.6 的要求中的自动化方案进行了强制，将在未来日期要求自动化的实现方案（如 WAF）。
6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script.	新要求	对支付页面脚本进行管理的要求，包括授权的检查、检查脚本的完整性以及脚本清单的论证及维护要求。

• An inventory of all scripts is maintained with written justification as to why each is necessary.		
6.5 Changes to all system components are managed securely.		
6.5.1 Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.	6.4.5 6.4.5.1 6.4.5.2 6.4.5.3 6.4.5.4	对原 6.4.5-6.4.5.4 的要求重新进行了整合。
6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	6.4.6	对原 6.4.6 的要求重新进行了描述。
6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.	6.4.1	对原 6.4.1 的要求进行了强化，要求预生产环境与生产环境进行访问控制。
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	6.4.2	对原 6.4.2 的要求进行了强化，要求预生产环境与生产环境进行角色和功能的分离控制。
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	6.4.3	对原 6.4.3 的要求进行了强化，要求持卡人数据环境之外不能存在生产的账户数据，强调预生产环境也不能存储生产的账户数据。

6.5.6 Test data and test accounts are removed from system components before the system goes into production.	6.4.4	对原 6.4.4 的要求进行了描述。