PCI DSS V3.0 变更分析

atsec(Beijing) information technology Co., Ltd

Room 119, Building 2, No.1, Street 7, Shangdi,

Haidian District, Beijing, P.R.China 10085
Tel +86-10-84834011
Fax +86-10-82890017

www.atsec.com

版权声明：

本文的所有内容仅用于读者了解 PCI DSS 标准变更的情况，其中的描述仅代表 atsec 的观点，具体的内容和说明请以 PCI 标准委员会发布的文档和说明为准。

目录

1 前言

按照 PCI 安全标准委员会（PCI SSC）（以下简称“标委会”）对于支付卡行业数据安全标准（以下简称“PCI DSS”）的更新周期，在 2013 年 11 月正式发布了 PCI DSS V3.0 版本。作为周期性的新版本发布，该版本主要基于 PCI 标准在使用过程中各种信息反馈，对数据安全的要求进行完善，并未产生重大的变化。PCI 标准主要是卡品牌（Card brand）从持卡人数据所存在安全风险的角度，制定了覆盖数据安全所涉及的各个方面的安全标准。

对于新版本所引入的变更，本文旨在通过新版本 V3.0 与旧版本 V2.0 变化的角度，对新版本所涉及的主要变化进行解读，使读者能较快地理解和掌握标准变更的主要方面。如需要了解所有的变更，感兴趣的读者可通过 PCI 标委会网站所提供的"PCI DSS Summary of Changes V2.0 to V3.0"以及 PA-DSS 的相应内容了解全部变更细节。

2 变更概述

在 PCI 安全标准委员会（PCI SSC）发布的 PCI DSS v3.0 版本中，与 2010 年发布的 V2.0 相比，并没有颠覆性的变化，主要的变更在于添加了更多的解释和细化，以利于对标准的准确把握与执行。

2.1 合规要求的变更分析

整体上来看，PCI DSS v3.0 版本中更有效地应对了当前支付环境以及 IT 环境的变化，趋向于更严格、更合理。

对于要求更严格的部分，主要围绕在默认帐号的范围、持卡人数据的管理、公共网络的范围、安全认证、接触类设备的管理、日志审计、安全扫描及渗透测试等方面。详细信息，请参见第 3.3.1 章节。

为便于合规工作的执行，标委会也发布了很多针对特定领域的指导说明文件，为便于读者使用，相应的链接及内容概述请参见《附件 1：PCI DSS 相关指导文件及链接》。

2.2 语言和格式方面的变化

对于广大中文读者来说，在 V3.0 版本中添加了中文的对应版本。尽管如此，笔者仍建议广大读者对标准的引用和理解以英文版本为准，以避免语言翻译上的偏差。中、英文所对应的链接如下：

- https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_ZH-CN.pdf
- https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

对于格式方面，主要变化有如下几点：

- V2.0 版本中 12.1.1 对于文档的要求，添加到了每一个章节的最后一个要求。
- 把 V2.0 中的“navitating_dss_v20”指导文件中的对应内容，添加到了 “testing procedure”之后，使读者可通过 “pci_dss_v3”一个文件即可完整地了解。
- 新的合规报告模板。

2.3 PCI DSS 合规的最佳实践

新版本中提出了将 PCI DSS 合规要求融入到日常的管理流程（Business-as-Usual Processes）的要求，这需要合规机构通过如下流程将合规流程融入到管理环节。

- 首先，从组织机构的层面定期梳理 PCI DSS 环境的合规范围，将所有涉及的系统组件纳入到管理的范畴。
- 其次，将系统组件涉及的 PCI DSS 要求纳入到日常的管理流程，包括但不限于：安全配置标准的实施、补丁管理、防病毒管理、日志审计等。
- 最后，将合规检查的诸多事项纳入到内部的检查活动中（比如组织机构自身在内审环节中检查 PCI DSS 要求），并保留合规的证据。

2.4 新标准的转换日期

对于 PCI DSS 标准的转换日期，如下表所示：

日　期	所应用的标准
在 2014 年 12 月 31 日前	可使用 V2.0 或 V3.0 标准进行合规工作。
在 2015 年 1 月 1 日后	V3.0 版本将于 2015 年 1 月 1 日正式生效，合规工作中必须使用 V3.0。
2015 年 6 月 30 日前	PCI-DSS V3.0 要求中的 6.5.10、8.5.1、9.9、11.3 和 12.9 仅作为最佳实践和建议。在之后，这些条款将作为强制要求。

在此建议需要通过 PCI-DSS 标准的组织尽早展开新版本的转换工作，以减少合规建设过程中对信息系统的影响。对于正在开展 PCI-DSS 合规的组织，推荐使用新版本进行 PCI 合规。

3 具体的变更内容说明

以下内容主要侧重于 pci-dss 的主要变化，因篇幅原因未能覆盖所有变化。

注：本章内容所描述的"原版本"指的是 PCI-DSS 的 V1.2.1 版本，"新版本"指的是 PCI-DSS 的 V2.0 版本。

3.1 适用性更强

为适应于组织的发展和合规的要求，在新版本中将所涉及适用范围和合规要求方面进行了更加明确的描述，使得某些概念更清晰、要求更明确。同时，也更多地引用了大量的业界标准和最佳实践，使得组织在合规过程中有更多的依据可寻。具体来看，适用性的变化主要体现在如下方面：

3.2 解释性说明

除了本文 2.3 章节提及的将合规要求融入日常业务流程外，新版本还作出了相应的解释。主要的解释性说明如下：

对应内容	对应的解释性说明	V3.0 标准原文
持卡人数据的适用性	PCI DSS 的要求适用于对帐号数据（持卡人数据/敏感认证数据）进行存储、处理和传输的机构。也适用于将支付处理和持卡人环境管理外包给外部服务商的机构（该机构仍需要确保外部服务商按 PCI DSS 的要求进行相应的保护）。 即使是加密的敏感认证数据，在授权后也不允许存储，这同样适用于不使用 PAN 的情况。机构应与收单行/卡品牌联系以确认敏感认证数据在授权前是否允许存储，存多久，以及相应的保护要求。	PCI DSS requirements apply to organizations and environments where account data (cardholder data and/or sensitive authentication data) is stored, processed or transmitted. Some PCI DSS requirements may also be applicable to organizations that have outsourced their payment operations or management of their CDE. Additionally, organizations that outsource their CDE or payment operations to third parties are responsible for ensuring that the account data is protected by the third party per the applicable PCI DSS requirements. Sensitive authentication data must not be stored after authorization, even if encrypted. This applies even where there is no PAN in the environment. Organizations should contact their acquirer or the individual payment brands directly to understand whether SAD is permitted to be stored prior to authorization, for how long, and any related usage and protection requirements.
与 PA-DSS 的关系	所有存储、处理与传输持卡人数据的应用（包括已通过 PA-DSS 验证的）均在机构的 PCI DSS 评估范围内。PCI DSS 评估中需要验证经过 PA-DSS 合规的应用是否已正确配置并安全地实施。如果该应用经过了某些定制，会导致与经 PA-DSS 验证的版本有差异，因此需要详细基于 PCI DSS 要求来确认。	All applications that store, process, or transmit cardholder data are in scope for an entity's PCI DSS assessment, including applications that have been validated to PA-DSS. The PCI DSS assessment should verify the PA-DSS validated payment application is properly configured and securely implemented per PCI DSS requirements. If the payment application has undergone any customization, a more in-depth review will be required during the PCI DSS assessment, as the application may no longer be representative of the version that was validated to PA-DSS.
针对第三方服务/外包方的合规	如果第三方服务商独立通过 PCI DSS 合规，应向其客户提供充足的证据以确保该评估范围覆盖了适用于其客户的服务，并需要确认相应的要求已被验证。第三方服务商提供给其客户的证据将依赖于双方间的约定/合同，比如提供 AOC/相关部分的 ROC 内容。	If the third party undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The specific type of evidence provided by the service provider to their customers will depend on the agreements/contracts in place between those parties. For example, providing the AOC and/or relevant sections of the service provider's ROC (redacted to protect any confidential information) could help provide all or some of the information.
抽样	在整个机构的 PCI DSS 合规中，可以接受评估师抽取其中的部分设施/系统组件进行验证，但不允许仅抽样的环境达到 PCI DSS 的要求（比如，季度脆弱性扫描应适用于所有的系统组件）。同样的，评估师也不允许仅检查部分 PCI DSS 要求。	While it is acceptable for an assessor to sample business facilities/system components as part of their review of an entity's PCI DSS compliance, it is not acceptable for an entity to apply PCI DSS requirements to only a sample of their environment (for example, requirements for quarterly vulnerability scans apply to all system components). Similarly, it is not acceptable for an assessor to only review a sample of PCI DSS requirements for compliance.

	系统组件的抽样应包括使用中的每个类型及其组合。比如，在应用的抽样中，抽样中必须包括针对每种应用的不同版本和平台的组合。	Samples of system components must include every type and combination that is in use. For example, where applications are sampled, the sample must include all versions and platforms for each type of application.

3.3 针对合规机构的合规要求

为适应于支付环境的变化以及信息技术的发展，新版本中添加了一定的变化，整体来讲使得要求更清晰、更明确。归纳起来，可概括为两类，说明如下：

3.3.1 合规要求更高

新版本在 SNMP 协议的界定、个人防火墙软件使用、敏感认证数据删除、向用户宣贯认证策略、审计日志记录要求等方面提出了更高的要求；在删除默认机密信息、公共网络、每日审计、重大变更需执行安全性扫描等方面的适用范围，提出了更明确的界定；另外，新版本还添加了 2.4、6.5.10、9.9、12.8.5 等新的要求。对于主要的变更点及其说明，如下：

变更类型	变更内容解读	标准原文参考（V3.0）
原要求中的变更	V2.0 中仅明确 SNMP 为不安全协议，新版本中明确不安全的协议为 SNMP 的 V1 和 V2 版本。 对于使用这两个版本的 SNMP 协议的系统组件，需要考虑相应的加固措施或升级为 SNMP V3 版本。 注意：新版本中变更的内容见黑色字体部分。	1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and **SNMP v1 and v2.**
原要求中的添加	需要在 V2.0 版本中确保个人防火墙软件实时运行以及防止被停用的基础上，针对个人防火墙软件定义清晰明确的控制规则。 注意：新版本中添加的内容见黑色字体部分。	**1.4** Install personal firewall software on any mobile and/or employee-owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the network. Firewall configurations include: · **Specific configuration settings are defined for personal firewall software.** · Personal firewall software is actively running. · Personal firewall software is not alterable by users of mobile and/or employee-owned devices.
更广的适用范围	V2.0 版本中仅明确要更改掉所有厂商提供的默认机密信息，新版本中明确了涉及的范围。 这需要合规机构针对系统组件所涉及的默认机密信息进行梳理，并逐一删除和修改。 注意：新版本中添加的内容见黑色字体部分。	2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. **This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, *point-of-sale* (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).** 2.2.d Verify that system configuration standards include the following procedures for all types of system components: **· Changing of all vendor-supplied defaults and elimination of unnecessary default accounts** · Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server · Enabling only necessary services, protocols, daemons, etc., as required for the function of the system · Implementing additional security features for any required

		services, protocols or daemons that are considered to be insecure · Configuring system security parameters to prevent misuse · Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
新出现的要求	新版本中明确要求合规机构维护涉卡系统组件的列表。对于持续合规的客户来讲，可参考已有的合规报告进行初始版本的建立和维护。	2.4 Maintain an inventory of system components that are in scope for PCI DSS.
原要求中的添加	V2.0 版本中不允许在授权后存储敏感认证数据，新版本除了保持该要求外，还要求使敏感认证数据在删除后不可恢复。 建议完善支付应用程序，并参考业界认可的安全删除标准将敏感认证数据删除。 注意：新版本中添加的内容见黑色字体部分。	3.2 Do not store sensitive authentication data after authorization (even if encrypted). **If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.** It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: · There is a business justification and · The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:
原要求中的添加	V2.0 版本中要求有明确业务需要的人员可查看全卡号，新版本中添加了对具有查看全卡号的角色、业务原因等进行记录的要求。 建议合规机构基于每个全卡号显示的位置进行梳理，对显示位置、对应的角色、业务需求等进行维护。 注意：新版本中添加的内容见黑色字体部分。	**3.3.a** Examine written policies and procedures for masking the display of PANs to verify: · **A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access.** · PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN. · All other roles not specifically authorized to see the full PAN must only see masked PANs.
更广的适用范围	对于需要保护持卡人数据传输在公共网络传输的要求，新版本中明确把蓝牙、GSM、CDMA、卫星网络纳入到公共网络的范围。 建议合规机构梳理持卡人数据传输所涉及的公共网络，并进行相应的强加密传输保护。 注意：新版本中添加的内容见黑色字体部分。	4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: · Only trusted keys and certificates are accepted. · The protocol in use only supports secure versions or configurations. · The encryption strength is appropriate for the encryption methodology in use. *Examples of open, public networks include but are not limited to:* · *The Internet* · *Wireless technologies,* ***including 802.11 and Bluetooth*** · ***Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)*** · *General Packet Radio Service (GPRS).* · ***Satellite communications.***
更广的适用范围	新版本中明确了对开发人员进行培训的具体范围，包括了安全编码的技能和基于编码指导进行开发等方面。 建议合规机构基于此要求完善和落实针对软件开发、测试人员的培训。 注意：新版本中添加的内容见黑色字体部分。	6.5 Address common coding vulnerabilities in software-development processes as follows: · **Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory.** · **Develop applications based on secure coding guidelines.** *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.
新出现的要求	新版本中将失效的验证和会话管理纳入到软件的生命管理中。 建议合规机构从安全编码规范、培训、代码审核、安全性测试等环节融入针对该要求的措施。	**6.5.10 Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include:** **· Flagging session tokens (for example cookies) as "secure"** **· Not exposing session IDs in the URL** **· Incorporating appropriate time-outs and rotation of session IDs after a successful login.** ***Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.***
原要求中的添加	新版本要求对角色、特权的级别以及所访问的资源进行定义。 建议合规机构梳理持卡人系统组件、访问权限以及人员角色间的对应关系，并进行维护。 注意：新版本中添加的内容见黑色字体部分。	7.1.1 Define access needs for each role, including: **· System components and data resources that each role needs to access for their job function** **· Level of privilege required (for example, user, administrator, etc.) for accessing resources.**
更广的适用范围	新版本明确了需验证用户身份以更改机密信息的场景。 建议合规机构梳理访问持卡人环境的各种机密信息（包括令牌、密钥、密码等），并在重置流程中验证用户身份。 注意：新版本中添加的内容见黑色字体部分。	8.2.2 Verify user identity before modifying any authentication credential—for example**, performing password resets, provisioning new tokens, or generating new keys.**
原要求中的添加	新版本中明确了向所有用户通告的认证策略和要求，包括选用强认证的指导、对认证信息保护的指导等。 建议合规机构基于所使用的机密信息（包括令牌、密钥、密码等）建议相应的指导文档并进行宣贯。 注意：新版本中添加的内容见黑色字体部分。	**8.4** Document and communicate authentication procedures and policies to all users including: · **Guidance on selecting strong authentication credentials** **· Guidance for how users should protect their authentication credentials** **· Instructions not to reuse previously used passwords** **· Instructions to change passwords if there is any suspicion the password could be compromised.**
新出现的要求	添加了服务供应商对其用户设备进行维护时使用唯一性帐号的要求。 建议合规机构落实帐号唯一性的要求。	8.5.1 *Additional requirement for service providers:* Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. *Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.* *Note: Requirement 8.5.1 is a best practice until June 30, 2015, after which it becomes a requirement.*
新出现的要求	添加了对非密码以外的认证机制使用唯一性帐号的要求。 建议合规机构落实帐号唯一性的要求。	8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: · Authentication mechanisms must be assigned to an individual

		account and not shared among multiple accounts. · Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.
新出现的要求	添加了对可接触式的读卡类设备的管理要求。 建议合规机构从维护设备的列表、定期对设备进行巡查以及培训使用人员方面加强管理。具体如下： 1、维护并更新设备的列表。包括但不限于设备型号、使用的位置、序列号或其它唯一性标识等。 2、定期对设备进行巡查，以发现对设备的破坏和替换。参考“skimming_prevention_IS”文档。 3、对人员进行培训，以确保使用人员可发现破坏和替换的企图。包括但不限于确认维修人员的身份、不在未验证的情况下进行安装和退回、识别可疑的行为等。	9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. *Note: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.* *Note: Requirement 9.9 is a best practice until June 30, 2015, after which it becomes a requirement.* 9.9.1 Maintain an up-to-date list of devices. The list should include the following: Make, model of device Location of device (for example, the address of the site or facility where the device is located) Device serial number or other method of unique identification. 9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). *Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.* 9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. Do not install, replace, or return devices without verification. Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).
更广的适用范围	新版本中明确了鉴权和认证机制的记录范围。 建议合规机构基于对应的范围（包括帐号的创建、权限变更、删除等）进行审计日志的记录和集中管理。 注意：新版本中添加的内容见黑色字体部分。	**10.2 5** 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**
原要求中的添加	新版本中添加了对审计日志的停止以及中断进行记录的要求。 建议合规机构对涉卡应用程序进行改进，以确保可有效记录审计日志的动作和状态。 注意：新版本中添加的内容见黑色字体部分。	**10.2.6** Initialization**, stopping, or pausing** of the audit logs

更广的适用范围	新版本中明确了每日进行日志审计的范围。 建议合规机构梳理所对应的每日审计的范围，尽可能以集中、自动的形式对范围内的日志进行检查，并在出现异常后进行响应。 注意：新版本中添加的内容见黑色字体部分。	10.6.1 Review the following at least daily: **· All security events** **· Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD** **· Logs of all critical system components** **· 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.**
更广的适用范围	对于重大变更后需要执行内、外部弱点扫描的要求，新版本中明确了重大变更的适用范围。 建议合规机构将内、外部扫描的工作纳入到范围所界定的变更环节中（比如添加了新的服务器、添加了新网段、操作系统升级等），并在出现高危漏洞时及时修复。 注意：新版本中添加的内容见黑色字体部分。	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).** ***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*** 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).** 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).**
原要求中的添加	新版本中明确了对渗透性测试所覆盖内容的要求。 其中一个显著的变化就是需要验证网络分割的有效性，建议合规机构梳理渗透测试的要求，通过专业化的机构和人员来执行该工作。 注意：新版本中添加的内容见黑色字体部分。	11.3 Implement a methodology for penetration testing that includes the following: **· Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115)** **· Includes coverage for the entire CDE perimeter and critical systems** **· Includes testing from both inside and outside the network** **· Includes testing to validate any segmentation and scope-reduction controls** **· Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5** **· Defines network-layer penetration tests to include components that support network functions as well as operating systems** **· Includes review and consideration of threats and vulnerabilities experienced in the last 12 months** **· Specifies retention of penetration testing results and remediation activities results.** **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 in-scope systems.**
原要求中的添加	新版本中要求机构自身识别需要执行文件完整性监控的关键文件。 建议合规机构同时将标准所对应的以及自身识别的关键文件进行文件完整性的监	11.5.a Verify the use of a change-detection mechanism within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: § System executables § Application executables

	控。 注意：新版本中添加的内容见黑色字体部分。	§ Configuration and parameter files § Centrally stored, historical or archived, log and audit files § **Additional critical files determined by entity (for example, through risk assessment or other means).**
新出现的要求	新版本要求在合规机构通过服务供应商的某些服务达到合规要求时，对服务供应商所覆盖的 PCI DSS 要求进行维护。 建议所涉及的合规机构梳理服务供应商的服务内容，维护不同的服务供应商与 PCI DSS 标准的对应关系列表。	12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.

3.3.2 合规要求更合理

新版本的要求在防病毒软件的安装范围、漏洞的评级要求、补丁的修复周期等方面的要求相对合理，同时在入侵检测技术、文件完整性技术等方面的要求更具灵活性。主要的变化如下：

变更类型	变更内容解读	标准原文参考（V3.0）
更明确的要求	新版本对于密钥管理环节所涉及的非对称公钥，明确提出不适用于密钥管理的要求。 注意：新版本中添加的内容见黑色字体部分。	**3.5** Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following: · Access to keys is restricted to the fewest number of custodians necessary. · **Key-encrypting keys are at least as strong as the data-encrypting keys they protect.** · **Key-encrypting keys are stored separately from data-encrypting keys.** · Keys are stored securely in the fewest possible locations and forms. **3.5.2** Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: · **Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key** · **Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device)** · **As at least two full-length key components or key shares, in accordance with an industry-accepted method** ***Note: It is not required that public keys be stored in one of these forms.***
更灵活的要求	对于有明确需要来关闭防病毒软件的情况，标准允许在审批后关闭一段时间。 对于非易感染的系统，标准要求执行定义的评估，以确认是否安装防病毒软件。这给予了合规机构在该类系统（如 linux、手机操作系统等）更大的灵活性。 注意：新版本中添加的内容见黑色字体部分。	**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.** **5.3 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.** ***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.***
更灵活的要求	原标准中明确 CVSS 4.0 分值 4.0 以上的漏洞是需要一月内修复的，新版	**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”)

	本给予合规机构在漏洞评级中的灵活性。 注意：新版本中变更的内容见黑色字体部分。	to newly discovered security vulnerabilities. ***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.* ***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.***
更明确的要求	新版本对于所有来自于供应商的安全补丁，要求在恰当的时间断进行修复，而没有强制性的三个月的要求。 注意：新版本中变更的内容见黑色字体部分。	6.2.a Examine policies and procedures related to security-patch installation to verify processes are defined for: · Installation of applicable critical vendor-supplied security patches within one month of release. · **Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).** **6.2.b** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following: · That applicable critical vendor-supplied security patches are installed within one month of release. · **All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).**
更灵活的要求	V2.0 版本中明确要求其中的措施之一是使用 WAF 设备；新版本中要求的描述更贴近于该机制的本质，使合规机构在选择具体的防护措施时更具备灵活性。 注意：新版本中变更的内容见黑色字体部分。	**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: · Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ***Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2.*** · 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.
更灵活的要求	V2.0 版本中明确要求密码必须包括字母和数据的组合；新版本中也允许密码组合在达到同等强度条件下的其它组合和方法，比如使用特殊字符和字母的组合。 注意：新版本中添加的内容见黑色字体部分。	**8.2.3** Passwords/phrases must meet the following: · Require a minimum length of at least seven characters. · Contain both numeric and alphabetic characters. **Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.**
更灵活的要求	V2.0 版本对于网络边界和关键点明确要求部署 IDS/IPS 设备或者系统；新版本中的要求变为使用入侵检测/入侵阻止类的技术，这使得合规机构在使用具体措施时更具备灵活性。 注意：新版本中变更的内容见黑色字体部分。	**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.

更灵活的要求	V2.0 版本对于网络边界和关键点明确要求部署 IDS/IPS 设备或者系统；新版本中的要求变为使用入侵检测/入侵阻止类的技术，这使得合规机构在使用具体措施时更具备灵活性。 注意：新版本中变更的内容见黑色字体部分。	11.5 Deploy a **change-detection mechanism (for example, file-integrity monitoring tools)** to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).***
更灵活的要求	V2.0 版本明确要求在设备上标识出所有者、联系方式及用途；新版本中的要求变为使用相应的方法可准确识别所有者、联系方式及用途等信息，同时也列出了可能采取的方法，使合规机构在设备管理环节的灵活性更大。 注意：新版本中变更的内容见黑色字体部分。	12.3.4 A method to accurately and readily determine owner, contact information, and purpose **(for example, labeling, coding, and/or inventorying of devices)**
更灵活的要求	新版本中明确界定了需维护的供应商范围，使得合规机构可更准确地在对供应商进行维护。 注意：新版本中变更的内容见黑色字体部分。	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:**

3.4 针对审核机构的验证要求

对于具体的审核要求，新版本也对审核机构提出了更多的要求，主要变化的部分列举如下：

变更类型	变更说明	V3.0 标准原文参考
增加的抽样要求	对测试环境中禁止使用生产卡号的要求，明确要求对测试数据进行抽样。	**6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.**
增加的抽样要求	对生产发布前需移除测试数据和帐号的要求，明确要求进行抽样验证。	**6.4.4.b Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.**
增加的抽样要求	对用户角色、职责以及访问权限间的关系，明确要求进行抽样验证。	**7.1.2.b Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are:** **· Necessary for that individual's job function** **· Restricted to least privileges necessary to perform job responsibilities.** **7.1.4 Select a sample of user IDs and compare with documented approvals to verify that:** **· Documented approval exists for the assigned privileges** **· The approval was by authorized parties** **· That specified privileges match the roles assigned to the individual.**
增加的抽	对离职用户需要交还各种认证方法并	**8.1.3.a Select a sample of users terminated in the past six months, and review current user access lists—for both local and**

样要求	禁用使用帐号的要求，明确要求抽样验证。	**remote access—to verify that their IDs have been deactivated or removed from the access lists.** **8.1.3.b Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated.**
变更的报告要求	对于涉及密码在存储和传输过程中的强加密要求，明确要求按不同分类进行阐述。	**8.2.1.a** Examine vendor documentation and **system configuration settings to verify that passwords are protected with strong cryptography during transmission and storage.** **8.2.1.b** For a sample of system components, examine password files to verify that passwords are unreadable during storage. **8.2.1.c** For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission. **8.2.1.d *Additional testing procedure for service providers*:** Observe password files to **verify that customer passwords are unreadable during storage.** **8.2.1.e *Additional testing procedure for service providers:*** Observe data transmissions to **verify that customer passwords are unreadable during transmission**.

4 合规建议

无论是首次执行 PCI DSS 合规的机构，还是处于合规状态持续维护的机构，建议参考新版本中的最佳实践要求（见本文第 2.3 章节），将 PCI DSS 合规工作融入到日常的运营管理活动中。同时也建议合规机构尽早展开对 PCI DSS 合规难度的评估，尽早完成从 V2.0 到 V3.0 的过渡。

对于具体的合规工作，不同层面的建议如下：

- 对于持卡人数据保护，建议以最小化的原则，在持卡人数据的存储位置、传输路径、存储形式等方面进行梳理，从而最小化合规的难度。而对于因业务原因需要使用的持卡人数据，则严格遵循安全的生命周期理念，从产生、梳理、维护、过期、销毁等环节，确保持卡人数据被安全地使用。
- 对于涉及支付的应用，首先要考虑应用对持卡人数据的安全处理，在存储、显示、销毁等环境确保数据的安全；其次，要通过安全的软件生命周期管理（包括但不限于：编码规范、代码审核、安全性测试、上线代码的定期检查、漏洞评级与管理等），确保应用本身的安全性；最后，在软件设计过程中应充分考虑软件的安全特性与实现，包括但不限于：密码管理、密钥管理、错误处理、角色管理、日志审计等。

如有更多的问题，也欢迎与 atsec 进行沟通和交流。

atsec 在此愿与各界同仁一道，为共同推进支付环境的安全性贡献力量。

附件 1：PCI DSS 相关的指导文件及链接

指导文件的说明	对应的链接
对于移动支付类的设备的安全指导	https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Merchants_v1.pdf https://www.pcisecuritystandards.org/documents/Mobile_Payment_Security_Guidelines_Developers_v1.pdf
涉及 ATM 设备的安全指导	https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf
电子商务环境的合规指导	https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf
云计算环境下的安全指导	https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf
合规环境下无线网络使用的安全指导	https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf
令牌化技术使用的安全指导	https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf
在电话支付环境中对持卡人数据保护的指导	https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf
EMV 环境对于 PCI DSS 的适用性说明	https://www.pcisecuritystandards.org/documents/pci_dss_emv.pdf
在电话支付环境中对持卡人数据保护的指导	https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf
对终端设备的安全保护指导	https://www.pcisecuritystandards.org/documents/skimming_prevention_IS.pdf
对要求 6.6 中应用检查和 Web 应用防火墙（WAF）设备适用性的声明	https://www.pcisecuritystandards.org/documents/information_supplement_6.6.pdf
对渗透性测试的要求说明	https://www.pcisecuritystandards.org/documents/information_supplement_11.3.pdf
在虚拟化环境下的合规指导	https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

参考文献

[1] PCI DSS V3.0 中文版本

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_ZH-CN.pdf

[2] PCI DSS V3.0 英文版本

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[3] PCI DSS V3.0 变更摘要

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3_Summary_of_Changes.pdf

[4] ″Payment Card Industry Compliance For Large Computing Systems″ from atsec

http://www.atsec.com/downloads/white-papers/PCI_Compliance_for_LCS.pdf