PCI DSS v3.2 变更分析

atsec 信息安全

作者：高向东

关键词：PCI DSS、支付卡行业、atsec、信息安全

atsec(Beijing) information technology Co., Ltd

Floor 3, Block C, Building 1, Boya C-Center,

Beijing University Science Park, Life Science Park

Changping District, Beijing, Postcode: 102206

P.R.China
Tel +86-10-53056681
Fax +86-10-53056678

www.atsec-information-security.cn
www.atsec.com

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”）的更新周期以及伴随信息技术产业发展，在 2016 年 4 月正式发布了 PCI DSS v3.2 版本。作为周期性的新版本发布，该版本主要基于 PCI DSS v3.1 标准在使用过程中根据定期的社区会议所收集的各种信息反馈，对支付卡行业数据安全标准的要求进行完善，在本更新版本中并未产生重大的变化。PCI DSS 标准主要是标委会针对持卡人数据环境可能存在的安全风险制定的一套覆盖数据安全各个方面的安全标准。

本文旨在通过新版本 v3.2 与旧版本 v3.1 之间差异变化的角度，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_v3-2_Summary_of_Changes”以及“PCI_DSS_v3-2”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 v3.2 版本中，与 2015 年发布的 v3.1 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 v3.2 版本中更有效地应对了当前支付环境以及 IT 环境的变化，呈现出更严格、更合理的趋势。

对于要求更严格的部分，主要围绕在多因素认证、密钥体系管理、安全控制机制管理、应急演练与响应等方面。详细信息，请参见第 3.3 章节。同时，有些要求也更趋合理，比如不安全协议的定义、个人防火墙软件的实施等方面，详细信息请参见 3.4 章节。

2.2 PCI DSS 合规的最佳实践

在 PCI DSS v3.1 将 PCI DSS 合规要求融入到日常的管理流程（Business-as-Usual Processes）的基础上，PCI DSS v3.2 版本将这些日常管理流程融入到了 DESV（指定机构的合规验证要求）的合规要求中。该最佳实践的要求及其大体流程说明如下：

- 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。
- 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。
- 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。

2.3 新标准的转换日期

对于 PCI DSS 标准的转换日期，如下表所示：

对应的标准版本	发布日期	到期日期
PCI DSS v3.0	2013 年 10 月	2015 年 12 月 31 日
PCI DSS v3.1	2015 年 4 月	2016 年 10 月 31 日
PCI DSS v3.2	2016 年 4 月	待定

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v3.1版本，“新版本”指的是PCI DSS的v3.2版本。

3.1 澄清性说明的调整

为适应于组织的发展和合规的要求，在新版本中对所适用的各种业务场景和业务流程中所遇到的疑问进一步进行了澄清。具体来看，澄清性说明的变化主要体现在如下方面：

对应章节内容	对应的解释性说明	v3.2 标准原文
Relationship between PCI DSS and PA-DSS	需要注意既使在环境中使用了符合 PA-DSS 的软件，因软件厂商不再提供支持的情况，相应的支付软件存在不能达到所支持的安全级别的风险。	As security threats are constantly evolving, applications that are no longer supported by the vendor (e.g., identified by the vendor as “end of life”) may not offer the same level of security as supported versions.
Scope of PCI DSS Requirements	需要在梳理范围的过程中覆盖各种系统类型以及物理位置。比如备份/灾难恢复站点、故障迁移系统等。	All types of systems and locations should be considered as part of the scoping process, including backup/recovery sites and fail-over systems.
Best Practices for Implementing PCI DSS into Business-as-Usual Processes	推荐将 PCI DSS 作为常规业务的一部分进行维护。在 DESV（指定机构附加验证）中强制要求 Appendix A3 部分进行了明确的要求。但对广大合规机构来讲，也推荐使用这些原则和最佳实践进行合规建设。	***Note:*** *For some entities, these best practices are also requirements to ensure ongoing PCI DSS compliance. For example, PCI DSS includes these principles in some requirements, and the Designated Entities Supplemental Validation (PCI DSS Appendix A3) requires designated entities to validate to these principles.* *All organizations should consider implementing these best practices into their environment, even where the organization is not required to validate to them.*

3.2 新增加的合规要求分析

所有新增加要求的强制时间点是 2018 年 6 月 30 日。在此时间之前，仅作为安全建议，合规机构可以有较长时间进行相应措施的落实。在此之后，如下要求将作为强制的要求内容。新增加要求的内容说明如下：

新增加要求的说明分析	标准原文参考（V3.2）
该要求针对服务提供商涉及对持卡人数据进行加密保护的加密架构体系的维护，这需要从数据加密的角度阐述加密措施及其体系的具体实现。从具体的实现来看，服务供应商可通过文档化的密钥体系、密钥映射关系表以及加密设备列表等信息的维护来达到要求。 无论是通过何种方法，需注意所维护的内容包括了加密算法、协议、密钥强度、密钥有效期、密钥用途以及用于密钥管理的加密机以及其他安全加密设备的列表的维护等。	3.5.1 *Additional requirement for service providers only:* Maintain a documented description of the cryptographic architecture that includes: Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date Description of the key usage for each key Inventory of any HSMs and other SCDs used for key management
该要求主要目的为了弥补因重大变更而引入的合规风险，这需要合规机构在完成重大变更后，对因变更增加或调整过的系统组件部分进行安全的维护并实施保护手段。同时，也建议合规机构将此处涉及的 PCI DSS 的合规要求融入到变更管理的流程中。	6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. Examples of PCI DSS requirements that could be impacted include, but are not limited to:

具体的要求包括但不限于： ➢ 更新拓扑图图 ➢ 参照系统配置标准对系统组件进行加固，比如删除默认密码、禁用不需要的服务、端口、协议、功能等。 ➢ 提升系统的安全性，比如实施文件完整性监控、防病毒软件、安装补丁、对日志进行审计等。 ➢ 在新系统中不存储敏感认证数据并对需要存储的持卡人数据的必要性、存储周期等进行维护。 ➢ 新系统纳入到例行化的季度弱点扫描流程中。	Network diagram is updated to reflect changes. Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging. Sensitive authentication data (SAD) is not stored and all cardholder data (CHD) storage is documented and incorporated into data-retention policy and procedures New systems are included in the quarterly vulnerability scanning process.
在服务提供商的关键安全控制系统出现失效的情况下，应及时得以识别和报告。此处提及的关键安全控制功能指的是与 PCI DSS 合规环境安全相关的技术措施，包括但不限于： ➢ 防火墙 ➢ 入侵检测系统/入侵防护系统 ➢ 文件完整性监控系统 ➢ 防病毒系统 ➢ 物理访问控制系统 ➢ 逻辑访问控制措施 ➢ 日志审计机制 ➢ 网络隔离控制 （如果适用） 这要求合规机构借助于日志集中管理等手段对失效行为进行识别，通过内部的报告流程进行及时响应。	10.8 *Additional requirement for service providers only*: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: Firewalls IDS/IPS FIM Anti-virus Physical access controls Logical access controls Audit logging mechanisms Segmentation controls (if used)
此要求在 10.8 的基础上对关键安全控制系统失效响应的具体流程进行了约束，其目的是降低失效带来的影响并避免类似事件的再次发生。流程中应覆盖的内容包括但不限于： ➢ 恢复安全功能 ➢ 识别并记录安全功能失效持续的时间 ➢ 识别并记录失效的原因（包括根本原因）并记录所需要的修复措施 ➢ 识别并解决因该问题导致的任何其它安全问题 ➢ 通过风险评估识别是否需要执行额外的操作 ➢ 实施必要的控制以避免失效再次发生 ➢ 恢复对安全控制的监控	10.8.1 *Additional requirement for service providers only*: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: Restoring security functions Identifying and documenting the duration (date and time start to end) of the security failure Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause Identifying and addressing any security issues that arose during the failure Performing a risk assessment to determine whether further actions are required as a result of the security failure Implementing controls to prevent cause of failure from reoccurring Resuming monitoring of security controls
在使用网络分隔的情况下，需要至少每半年以及在对分隔措施进行变更后执行分段控制有效性确认的渗透测试工作。该要求进一步强化了通过渗透测试验证网络分隔有效性的频率，需要合规服务提供商及时调整渗透测试工作的范围和执行频率。	11.3.4.1 *Additional requirement for service providers only*: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.

12.4.1 要求合规服务提供商的经营管理层应该建立对持卡人数据保护的责任以及维护包含下列内容的 PCI DSS 合规程序: ➢ 经营管理层应该对维护 PCI DSS 合规状态总体负责 ➢ 定义 PCI DSS 合规程序特许权并且和经营管理层沟通此特权。	12.4.1 *Additional requirement for service providers only:* Executive management shall establish responsibility 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
为了持续监视服务提供商 PCI DSS 合规的执行情况，此点要求至少每季度对人员遵循安全策略和流程的情况进行评估。评估应覆盖的流程包括但不限于： ➢ 每日的日志检查 ➢ 防火墙规则检查 ➢ 新系统实施所规定的配置标准 ➢ 对安全警告进行响应 ➢ 变更管理流程	12.11 *Additional requirement for service providers only:* Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: Daily log reviews Firewall rule-set reviews Applying configuration standards to new systems Responding to security alerts Change management processes
对于如上的评估过程，其结果应进行记录，并确保 PCI DSS 合规项目的负责人审查并签署该评估结果。	12.11.1 *Additional requirement for service providers only:* Maintain documentation of quarterly review process to include: Documenting results of the reviews Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program
对于服务供应商所使用的 SSL3.0 以及 TLS1.1 以下版本的不安全协议，应于 2016 年 6 月 30 日前递交安全服务声明，该声明应包含下列内容二选一： 1. 服务提供商声明自 2016 年 6 月 30 日之后仅使用安全的协议. 2. 服务提供商提交风险的降低和整改计划，该计划应该包含具体的降低风险的措施及不安全协议版本的停用时间，整改的完成日期不得晚于 2018 年 6 月 30 日。	A2.3 *Additional Requirement for Service Providers Only:* All service providers must provide a secure service offering by June 30, 2016.

3.3 趋严格的要求点说明

对比于 PCI DSS v3.1 的相应要求，增加的部分以加粗字体标出，删除的部分以删除线的形式标出。

变更内容解读	**标准原文参考（V3.2）**
对于在系统组件部署前要变更默认值的要求，覆盖的范围中增加了支付应用软件中涉及的默认值（如默认密码等）。	**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, **payment applications,** Simple Network Management Protocol (SNMP) community strings, etc.).
在使用磁盘加密技术进行持卡人数据加密后，加密密钥的管理要求仍适用于标准中对于密钥管理的要求（如 3.5 和 3.6 等）。这要求磁盘加密技术在具体的实施过程中考虑密钥的安全管理，包括但不限于： ➢ 密钥存储位置的最小化	**3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. ***Note: This requirement applies in addition to all other PCI DSS encryption and key-management requirements.***

➢ 密钥的加密层级 ➢ 使用强加密算法 ➢ 密钥的生命周期安全（包括但不限于生成、分发、存储、销毁、替换、变更等）	
无论支付应用是否经过了 PA-DSS 验证，新版本进一步明确将支付应用纳入到管理范畴，即要求在一月内实施关键的安全补丁。 对于合规机构来讲，需要扩大补丁管理的覆盖范围，确保包括支付应用在内的各类涉卡系统组件均得以覆盖。	**6.2** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. ***Note:*** *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.* This requirement applies to applicable patches for all installed software**, including payment applications (both those that are PA-DSS validated and those that are not)**.
此处删除了原标准中对于变更控制流程的范围限定，要求所有的变更流程必须执行相应的流程。如下： ➢ 影响分析 ➢ 被授权方的变更审批记录 ➢ 功能性测试 ➢ 回退流程	**6.4.5** Change control procedures ~~for the implementation of security patches and software modifications~~ must include the following:
新要求进一步明确对开发人员的培训的频率为至少每年一次。	**6.5** Address common coding vulnerabilities in software-development processes as follows: Train developers **at least annually in up-to-date** secure coding techniques, including how to avoid common coding vulnerabilities. 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.*
该要求进一步明确在涉及多种访问控制机制的情况下，每种访问控制机制对于业务必须原则以及“默认禁止所有”原则的执行。	**7.2** Establish an access control system for systems components that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed. **Entities may have one or more access controls systems to manage user access.**
此处将原标准中的“外部厂商”更改为“第三方”，即对任何外部机构所持有的合规机构的管理帐号均应纳入监控的范围，即仅在需要时启用、在使用过程中进行监控、使用完成立即关闭。	**8.1.5** Manage IDs used by **third parties** to access, support, or maintain system components via remote access as follows: Enabled only during the time period needed and disabled when not in use. Monitored when in use.
该要求是 PCI DSS v3.2 版本的一个重大变更，将原有的双因素认证更新为多因素认证，并将原 8.3 的要求拆分为 8.3.1 和 8.3.2 两个要求。 要求 8.3.1 适用于所有对持卡人数据环境的非控制台管理访问。8.3.2 涉及来自合规机构外部的远程网络访问，包括内部用户、管理员、第三方访问等。 对于如上涉及的访问，需要实施覆盖所知、所有以及个人特征三大认证类别中的两个或多个方法。	**8.3** Secure all individual non-console administrative access and all remote access to the CDE using **multi-factor authentication**. **8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.** ***Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*** **8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity’s network.**

此要求明确在合规机构同时使用物理环境的录像监控和访问控制措施的情况下，这两种措施的相关记录均适用于存储期限的要求。	**9.1.1** Use either video cameras or access control mechanisms **(or both)** to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.
该要求进一步说明了通过合规机构的漏洞评级并由重新扫描流程修复所有“高风险”及以上级别的漏洞。	**11.2.1** Perform quarterly internal vulnerability scans. Address vulnerabilities **and perform rescans to verify all “high risk” vulnerabilities are resolved in accordance with the entity’s vulnerability ranking** (per Requirement 6.1). Scans must be performed by qualified personnel.
在维护设备的使用策略中，每一类与合规相关的设备除了要维护设备列表外，新标准还要求维护所对应的授权访问人员。	**12.3.3** Verify that the usage policies define: A list of all critical devices, and **A list of personnel authorized to use the devices**.
在供应商的维护列表中，新标准需要维护对应服务机构的描述。	**12.8.1** Maintain a list of service providers **including a description of the service provided**.
新要求明确了应急演练的范围，需要覆盖到 12.10.1 的所有要求。包括但不限于： ➢ 出现威胁时的角色、责任以及沟通与联系策略，至少包括支付品牌通知 ➢ 详细的事故响应程序 ➢ 业务恢复和继续程序 ➢ 数据备份流程 ➢ 报告威胁的法律要求分析 ➢ 所有关键系统组件的范围和响应 ➢ 支付品牌对事故响应程序的参考或应用	**12.10.2** Review and test the plan, **including all elements listed in Requirement 12.10.1**, at least annually.

3.4 趋合理的要求点说明

新版本的要求在不安全协议的范围、个人防火墙软件要求、密码管理要求的适用性等方面的要求相对合理。对比于 PCI DSS v3.1 的相应要求，增加的部分以加粗字体标出，主要的变化如下：

变更内容解读	标准原文参考（V3.0）
不安全协议随着产业的变化也在不断更新，新标准中删除了具体不安全协议的示例，使得合规机构可以基于风险评估、缺陷评级以及产业最佳实践等角度来灵活地选择可用的安全协议。	**1.1.6** Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.
该要求不再限定于合规机构实施个人防火墙软件，作为达到等同安全效果的方案也可以纳入考虑的范畴内，这使得合规机构可以在满足合规的前提下使用灵活的合规方案。	**1.4** Install personal firewall software **or equivalent functionality** on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall **(or equivalent)** configurations include: Specific configuration settings are defined. Personal firewall **(or equivalent functionality)** is actively running. Personal firewall **(or equivalent functionality)** is not alterable by users of the portable computing devices.
新版本进一步说明了显示的卡号超出前 6 位和后 4 位情况下的处理要求。	**3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see **more than the**

	first six/last four digits of the PAN.
新版本要求企业更多地参考业界的最佳实践生成强密钥。所推荐的指导资源如下： ➢ NIST Special Publication 800-133: Recommendation for Cryptographic Key Generation ➢ ISO 11568-2 Financial services — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle 4.3 Key generation ➢ ISO 11568-4 Financial services — Key management (retail) — Part 4: Asymmetric cryptosystems — Key management and life cycle 6.2 Key life cycle stages — Generation ➢ European Payments Council EPC 342-08 Guidelines on Algorithms Usage and Key Management 6.1.1 Key generation [for symmetric algorithms] 6.2.1 Key generation [for asymmetric algorithms]	**3.6.1.b** Observe the procedures for generating keys to verify that strong keys are generated.
此处更清晰地说明了测试数据和帐号的来源。	**6.4.4** Removal of test data and accounts **from system components** before the system becomes active **/ goes into production**.
在第 8 章节的前言部分，进一步澄清第 8 章节的所有要求不适用于消费者（即持卡人）。	*Requirement 8: Identify and authenticate access to system components* Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes. The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage. ***Note:*** *These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance).* ***These requirements do not apply to accounts used by consumers (e.g., cardholders).*** *However, Requirements 8.1.1, 8.2, 8.5, 8.2.3 through 8.2.5, and 8.1.6 through 8.1.8 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).*

3.5 格式方面的调整说明

涉及的格式调整主要是把原标准的 Appendix A，变更为 Appendix A1，增加了 Appendix A2 和 A3。具体的几点变化说明如下：

- 原 PCI DSS v3.1 版本要求 1.3.3 所涉及的要求内容已在其它要求点（如 1.2.1，1.3.1）中被覆盖，因而新版本中删除了该点的要求。
- 因当前时间已晚于 2015 年 6 月 30 日，因而在 3.2 版本中去掉了针对 6.5.10，8.5.1，9.9，11.3 以及 12.9 等要求点的生效时间的要求。
- 增加了 Appendix A2， 将涉及 2.2.3，2.3 以及 4.1 要求点对于 SSL 和早期 TLS 版本整改的内容移到了 Appendix A2。
- 增加了 Appendix A3，将涉及 DESV 的要求整合到该部分。

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 2.2 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 v3.1 到 v3.2 版本的过渡。

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，从而最小化合规的范围，降低复杂度。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。

如有更多的关于 PCI DSS 合规方面的问题，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。

参考文献

[1] PCI DSS V3.2 英文版本

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

[2] PCI DSS V3.2 变更摘要

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2_Summary_of_Changes.pdf

[3] PCI DSS V3.2 术语表

https://www.pcisecuritystandards.org/documents/PCI_DSS_Glossary_v3-2.pdf

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

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