# 寻求 PCI DSS 遵从性的优先方法

支付卡行业数据安全标准 (PCI DSS) 提供了 12 条详细的要求结构，旨在确保商户和其他组织存储、处理和/或传输的持卡人数据的安全性。鉴于该标准的综合性，该标准提供了大量的安全性信息，以致于有些负责持卡人数据安全的人员可能不知道持续的遵从旅程应该从何入手。为此，PCI 安全标准委员会提供如下优先方法，旨在帮助利益相关者了解可以从何入手，以降低遵从流程早期的风险。优先方法中的单个里程碑无法提供全面安全或实现 PCI DSS 遵从性，但遵循该指南将有助于利益相关者加快保护持卡人数据的进程。


### 亮点

可以帮助商户确定风险等级最高的目标

围绕 PCI DSS 的实施和评估工作建立通用语言

借助里程碑，商户可以展示遵从性流程取得的进展

## 什么是优先方法？

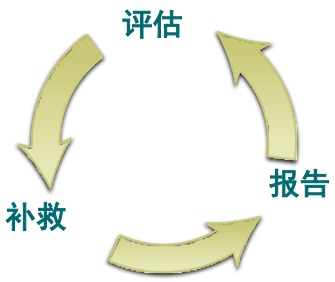
优先方法包括六个安全里程碑，这些里程碑将帮助商户和其他组织在实现 PCI DSS 遵从性的道路上，渐进性地防御风险等级最高的因素以及不断升级的威胁。优先方法及其里程碑（如第 2 页描述）旨在带来以下好处：

- 组织可用于按优先顺序化解风险的路线图
- 有助于“快速致胜”的实用方法
- 支持财务和运营规划
- 促进客观且可衡量的进展指示
- 帮助促进评估商之间达成一致

## 优先方法的目标

优先方法基于与存储、处理和/或传输持卡人数据相关联的风险，提供遵从性活动的路线图。路线图帮助确定实现遵从性、确立里程碑、尽早降低遵从性流程中持卡人数据外泄的风险等工作的优先顺序，并且帮助收单机构客观地衡量商户、服务提供商以及其他人的遵从性活动和风险降低情况。优先方法是在考量实际的数据外泄，并获得合格安全性评估商、取证调查者和 PCI 安全标准委员会顾问委员会的反馈之后制定的。优先方法并非作为实现 PCI DSS 遵从性的替代、捷径或权宜方法，也不是适用于每个组织的强制性、通用框架。优先方法适合于经历现场评估或使用 SAQ D 的商户。

**PCI DSS 遵从性是持续的过程**




**PCI SSC 创始人**

**参与组织**

商户、银行、处理商、开发人员以及销售点供应商

## 免责声明

要实现 PCI DSS 遵从性，组织必须满足所有的 PCI DSS 要求，不管满足要求的顺序如何，或者寻求遵从性的组织是否遵照 PCI DSS 优先方法。本文档不修改或删减 PCI DSS 或 PCI DSS 的任何要求，并且如有变更，恕不另行通知。

PCI SSC 对于错误之处，或者因使用本文档中包含的信息而引发的任何损失概不负责。PCI SSC 不担保、保证或者陈述本文档中所含的任何信息的准确性或充分性，并且 PCI SSC 对于此类信息的使用或滥用概不承担任何责任。

## 用于确定 PCI DSS 遵从性工作的优先顺序的里程碑

优先方法包括六个里程碑。下列矩阵总结了各里程碑的宏伟目标和意图。本文档的其余部分将各里程碑映射到 12 条 PCI DSS 要求及其子要求。

| 里程碑 | 目标 |
|---|---|
| 1 | **移除敏感验证数据，并限制数据保留。**该里程碑针对已受到威胁的实体的关键风险领域。记住，如果并未存储敏感验证数据以及其他持卡人数据，则威胁的影响将大大降低。如果不需要，则不存储 |
| 2 | **保护系统和网络，并且准备好对系统漏洞作出响应。**该里程碑针对对于大多数威胁的侵入点的控制，以及对于响应流程的控制。 |
| 3 | **安全支付卡应用程序。**该里程碑针对对于应用程序、应用程序流程以及应用程序服务器的控制。这些方面的漏洞使入侵者轻松破坏系统，并获取对持卡人数据的访问权限。 |
| 4 | **监测并控制系统访问。**通过对该里程碑的控制，您可以检测访问者、访问内容、访问时间以及访问者通过何种方式访问您的网络和持卡人数据环境。 |
| 5 | **保护存储的持卡人数据。**对于已经分析业务流程并决定必须存储主帐户的组织，里程碑 5 针对已存储数据的主要保护机制。 |
| 6 | **最终确定余下的遵从性工作，并确保所有控制措施均落实到位。**里程碑 6 的目的是完成 PCI DSS 要求，并最终确定保护持卡人数据环境所需的其余所有的相关政策、程序和流程。 |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **要求 1：安装并维护防火墙配置以保护持卡人数据** | | | | | | |
| **1.1** 建立并实施包含以下内容的防火墙和路由器配置标准： | | | | | | |
| **1.1.1** 批准和测试所有网络连接以及防火墙和路由器配置变更的正式流程 | | | | | | 6 |
| **1.1.2** 识别持卡人数据环境和其他网络（包括任何无线网络）间所有连接的当前网络图 | 1 | | | | | |
| **1.1.3** 显示整个系统和网络中所有持卡人数据流的当前图表 | 1 | | | | | |
| **1.1.4** 各互联网连接以及任何非军事区 (DMZ) 和内部网络区域间的防火墙要求 | | 2 | | | | |
| **1.1.5** 网络组件管理群组、角色与责任的说明 | | | | | | 6 |
| **1.1.6** 使用所有获准服务、协议和端口的业务理由和许可文档记录，包括对非安全协议实施安全功能的文档记录。 | | 2 | | | | |
| **1.1.7** 审核防火墙和路由器规则集（至少每半年一次）的要求 | | | | | | 6 |
| **1.2** 构建防火墙和路由器配置，以限制不可信网络与持卡人数据环境中任意系统组件之间连接。<br>*注：“不可信网络”指受审核实体所属网络之外的任何网络，和/或不受该实体控制或管理的任何网络。* | | | | | | |
| **1.2.1** 将输入和输出流量限制到持卡人数据环境所需的范围，并明确拒绝所有其他流量。 | | 2 | | | | |
| **1.2.2** 保护并同步路由器配置文件。 | | 2 | | | | |
| **1.2.3** 在所有无线网络和持卡人数据环境间安装外围防火墙，并配置这些防火墙以拒绝流量或（如果业务需要流量）仅允许无线环境和持卡人数据环境间的授权流量。 | | 2 | | | | |
| **1.3** 禁止互联网与持卡人数据环境中任何系统组件之间的直接公共访问。 | | | | | | |
| **1.3.1** 实施 DMZ，仅向提供授权服务、协议和端口（支持公共访问）的系统组件输入流量。 | | 2 | | | | |
| **1.3.2** 仅向 DMZ 内的 IP 地址输入互联网流量。 | | 2 | | | | |
| **1.3.3** 实施反欺骗措施以检测并阻止伪造的源 IP 地址进入网络。（例如，阻止带内部源地址的互联网流量。） | | 2 | | | | |
| **1.3.4** 禁止从持卡人数据环境到互联网的非授权出站流量。 | | 2 | | | | |
| **1.3.5** 仅允许“已建立”连接进入网络。 | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **1.3.6** 将存储持卡人数据的系统组件（例如：数据库）放置在与 DMZ 以及其他不可信网络隔离的内部网络区域中。 | | 2 | | | | |
| **1.3.7** 不要将私人 IP 地址和路由信息泄露给非授权方。<br>*注：掩盖 IP 地址的方法包括但不限于：*<br>• *网络地址转换 (NAT)*<br>• *将包含持卡人数据的服务器放置在代理服务器/防火墙中，*<br>• *删除或过滤针对采用注册地址的专用网络的路由器广告，*<br>• *在内部使用 RFC1918 地址空间而非注册地址。* | | 2 | | | | |
| **1.4** 在可在网络外连接互联网且可用于访问 CDE 的任何便携式计算设备（包括公司和/或员工所有的便携式计算设备，例如，员工使用的笔记本电脑）上安装个人防火墙软件或等效功能。防火墙（或等效功能）配置包括：<br>• 定义了具体的配置设备。<br>• 个人防火墙（或等效功能）正在活跃运行。<br>• 便携式计算设备用户无法更改个人防火墙（或等效功能）。 | | 2 | | | | |
| **1.5** 确保用于防火墙管理的安全政策和操作程序已记录、使用，并为所有相关方所了解。 | | 2 | | | | |
| **要求 2：不要使用供应商提供的默认系统密码和其他安全参数** | | | | | | |
| **2.1** 始终更改供应商提供的默认值并于在网络中安装系统之前删除或禁用不必要的默认帐户。<br>此要求适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、销售点 (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的默认密码。 | | 2 | | | | |
| **2.1.1** 对于连接到持卡人数据环境或传输持卡人数据的无线环境，在安装时更改所有无线供应商的默认值，包括但不限于默认的无线密钥、密码和 SNMP 社区字符串。 | | 2 | | | | |
| **2.2** 制定适合所有系统组件的配置标准。确保这些标准能解决所有已知的安全漏洞并与行业认可的系统强化标准一致。<br>行业认可的系统强化标准来源包括但不限于：<br>• 互联网安全中心 (CIS)<br>• 国际标准化组织 (ISO)<br>• 美国系统网络安全协会 (SANS)<br>• 国家标准与技术研究所 (NIST)。 | | | 3 | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **2.2.1** 每台服务器仅执行一项主要功能，以防需要不同安全级别的功能并存于同一台服务器上。（例如 Web 服务器、数据库服务器和 DNS 均应在单独的服务器上执行。）<br>*注：如果使用虚拟化技术，每个虚拟系统组件仅执行一项主要功能。* | | | 3 | | | |
| **2.2.2** 仅启用系统功能所需的必要服务、协议、守护进程等。 | | | 3 | | | |
| **2.2.3** 针对任何被视为不安全的必要服务、协议或守护进程实施附加安全功能。<br>*注：若要使用 SSL/早期 TLS，须完成附录 A2 中的要求。* | | 2 | | | | |
| **2.2.4** 配置系统安全参数，以防滥用。 | | | 3 | | | |
| **2.2.5** 删除所有非必要功能，例如脚本、驱动程序、特性、子系统、文件系统和不必要的 Web 服务器。 | | | 3 | | | |
| **2.3** 使用强效加密法对所有非控制台管理访问进行加密。<br>*注：若要使用 SSL/早期 TLS，须完成附录 A2 中的要求。* | | 2 | | | | |
| **2.4** 保留一份 PCI DSS 范围内系统组件的清单。 | | 2 | | | | |
| **2.5** 确保已记录、正在使用且所有相关方了解用于管理供应商默认设置及其他安全参数的安全政策和操作程序。 | | 2 | | | | |
| **2.6** 共享托管服务提供商必须保护每个实体的托管环境和持卡人数据。这些提供商必须符合附录 A1：《针对共享托管服务提供商的 PCI DSS 附加要求》中详述的具体要求。 | | | 3 | | | |
| **要求 3：保护存储的持卡人数据** | | | | | | |
| **3.1** 通过实施数据保留和处理政策、程序和流程最大限度地减少持卡人数据存储，对所有持卡人数据 (CHD) 存储而言，这些政策、程序和流程至少应包含以下方面：<br>• 将数据存储量和保留时间限制在法律、法规和/或业务要求的范围内<br>• 持卡人数据的具体保留要求<br>• 不再需要时安全删除数据的流程<br>• 按季度查找并安全删除所存储的超过规定保留期限的持卡人数据的流程。 | 1 | | | | | |
| **3.2** 授权之后，不要存储敏感验证数据（即使已加密）。如果收到敏感验证数据，在完成验证流程后使所有数据不可恢复。<br>在下列情况下，允许发卡机构和支持发卡服务的公司存储敏感验证数据：<br>• 有正当的业务理由且<br>• 数据存储安全。<br>敏感验证数据包括下文要求 3.2.1 至 3.2.3 中列举的数据： | 1 | | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **3.2.1** 切勿在授权后存储卡片背面磁条上任何磁道的完整内容、芯片或其他地方上的等效数据。此类据也可称为全磁道、磁道、磁道 1、磁道 2 和磁条数据。<br>注：在正常业务过程中，以下磁条数据元素可能需要保留：<br>• 持卡人的姓名<br>• 主帐户 (PAN)<br>• 失效日<br>• 业务码<br>为将风险降至最低，只存储业务所需的数据元素。 | 1 | | | | | |
| **3.2.2** 切勿在授权后存储用于确认无实卡交易的卡验证代码或值（印在支付卡正面或背面的三或四位数值）。 | 1 | | | | | |
| **3.2.3** 授权后，请勿存储个人识别码 (PIN) 或经加密的 PIN 数据块。 | 1 | | | | | |
| **3.3** 显示 PAN 时予以掩盖（最多显示前六位和后四位数字），以便仅限具有正当业务需要的工作人员查看除前六位/后四位以外的 PAN。<br>*注：该要求不能取代现行更严格的有关持卡人数据显示的要求，例如法律或支付卡品牌对销售点 (POS) 收据的要求。* | | | | | 5 | |
| **3.4** 通过下述任何方法使所有位置（包括便携式数字媒介上、备份媒介上和日志中）存储的 PAN 均不可读：<br>• 基于强效加密法的单向散列函数（散列必须要有完整的 PAN）<br>• 截词（不能用散列代替 PAN 被截词的部分）<br>• 索引令牌与索引簿（索引簿必须安全地存储）<br>• 具有相关密钥管理流程和程序的强效加密法。<br>*注：对恶意个人而言，如果能访问被截词和散列的 PAN，要重建原始 PAN 数据是件相当轻松的事。如果在实体环境中出现同一个 PAN 的散列版本和截词版本，则须采取额外控制措施，确保散列版本和截词版本不能被相互关联，用于重建原始 PAN。* | | | | | 5 | |
| **3.4.1** 如使用磁盘加密（而不是文件级或列级数据库加密），则逻辑访问必须得到单独管理并独立于本地操作系统的验证和访问控制机制（例如，不使用本地用户帐户数据库或通用网络登录凭证）。解密密钥决不能与用户帐户关联。<br>*注：除了所有其他 PCI DSS 加密和密钥管理要求外，此要求也适用。* | | | | | 5 | |
| **3.5** 记录并实施保护程序，以保护用于防止存储的持卡人数据被泄露和滥用的密钥：<br>*注：本要求适用于用来为存储的持卡人数据加密的密钥，也适用于用来保护数据加密密钥的密钥加密密钥，这些密钥加密密钥至少须与数据加密密钥一样强效。* | | | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **3.5.1 仅针对服务提供商的附加要求：**维护包含以下内容的加密架构文档描述：<br>• 用于保护持卡人数据的所有算法、协议和密钥的详情，包括密钥强度和到期日<br>• 每个密钥主要用途的说明。<br>• 用于进行密钥管理的任何 HSM 和其他 SCD 的清单<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | | | | 5 | |
| **3.5.2** 仅极少数必需的保管人有密钥访问权。 | | | | | 5 | |
| **3.5.3** 存储用于始终以下列一种（或多种）形式加密/解密持卡人数据的机密密钥和私人密钥：<br>• 使用至少与数据加密密钥一样强效且与数据加密密钥分开存储的密钥加密密钥进行加密<br>• 在安全加密设备（例如，硬件（主机）安全模块 (HSM) 或 PTS 批准的交互点设备）内<br>• 根据行业认可的方法，作为至少两个全长密钥组分或密钥共享<br>*注：公共密钥不要求以这些形式存储。* | | | | | 5 | |
| **3.5.4** 尽量减少密钥存储的地方。 | | | | | 5 | |
| ***3.6*** 充分记录并实施用于持卡人数据加密的所有密钥管理流程和程序，包括：<br>*注：包括 NIST（可在 http://csrc.nist.gov 找到）在内的各种资源均提供有大量密钥管理方面的行业标准。* | | | | | | |
| **3.6.1** 生成强效密钥 | | | | | 5 | |
| **3.6.2** 安全的密钥分配 | | | | | 5 | |
| **3.6.3** 安全的密钥存储 | | | | | 5 | |
| **3.6.4** 根据相关应用程序供应商或密钥所有人的规定并基于行业最优方法和指南（例如，《NIST 特别出版物 800-57》），在密钥周期结束时（例如，指定期限过后和/或给定密钥产生一定量的密文后）对密钥进行的变更。 | | | | | 5 | |
| **3.6.5** 密钥的完整性变弱（例如，知道明文密钥部分的员工离职）或怀疑密码遭受威胁时，认为有必要注销或替换（例如，存档、销毁和/或撤销）密钥。<br>注：如果需要保留注销或替换的密钥，则必须对其进行安全存档（例如，使用密钥加密密钥进行存档）。存档的密钥只能用于解密/验证。 | | | | | 5 | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **3.6.6** 若使用手动明文密钥管理操作，则必须使用分割知识和双重控制来管理这些操作。<br>注：手动密钥管理操作示例包括但不限于：密钥生成、传输、加载、存储和销毁。 | | | | | 5 | |
| **3.6.7** 防止密钥的非授权替换。 | | | | | 5 | |
| **3.6.8** 有关密钥保管人正式确认理解并接受密钥保管责任的要求。 | | | | | 5 | |
| **3.7** 确保已记录、正在使用且所有相关方了解用于保护已存储的持卡人数据的安全政策和操作程序。 | | | | | 5 | |
| **要求 4：加密持卡人数据在开放式公共网络中的传输** | | | | | | |
| **4.1** 使用强效加密法和安全协议来保护经由公开、公共网络传输的敏感持卡人数据，包括：<br>• 只接受可信的密钥和证书。<br>• 使用的协议只支持安全的版本或配置。<br>• 加密强度适合所使用的加密方法。<br>*注：若要使用 SSL/早期 TLS，须完成附录 A2 中的要求。开放式公共网络包括但不限于：*<br>• *互联网*<br>• *无线技术，包括 802.11 和蓝牙*<br>• *蜂窝技术，例如，全球移动通信系统 (GSM)、码分多址 (CDMA)*<br>• *通用分组无线业务 (GPRS)。*<br>• *卫星通信。* | | 2 | | | | |
| **4.1.1** 确保传输持卡人数据或连接到持卡人数据环境的无线网络使用行业最优方法，以对验证和传输实施强效加密。 | | 2 | | | | |
| **4.2** 不要使用终端用户通讯技术（例如，电子邮件、即时通讯、短信、聊天等）来传送不受保护的 PAN。 | | 2 | | | | |
| **4.3** 确保已记录、正在使用且所有相关方了解用于加密持卡人数据传输的安全政策和操作程序。 | | 2 | | | | |
| **要求 5：使用并定期更新杀毒软件或程序** | | | | | | |
| **5.1** 在经常受恶意软件影响的所有系统（特别是个人电脑和服务器）中部署杀毒软件。 | | 2 | | | | |
| **5.1.1** 确保杀毒程序能检测、删除并阻止所有已知类型的恶意软件。 | | 2 | | | | |
| **5.1.2** 对于通常不受恶意软件影响的系统，需要执行定期评估以确定并评估不断进化的恶意软件威胁，从而确认这些系统是否仍不需要使用杀毒软件。 | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **5.2** 确保所有杀毒机制按如下方式维护：<br>• 保持为最新，<br>• 执行定期扫描<br>• 生成检查日志（PCI DSS 要求 10.7 规定保留）。 | | 2 | | | | |
| **5.3** 确保杀毒机制积极运行且无法被用户禁用或更改，除非管理人员根据具体情况做出有时间限制的明确授权。<br>*注：只有存在合理的技术需要且根据具体情况经管理人员批准时，才能暂时禁用杀毒解决方案。如果出于特定目的需要禁用杀毒保护，必须获得正式授权。杀毒保护禁用期间，可能还需要实施其他安全措施。* | | 2 | | | | |
| **5.4** 确保已记录、正在使用且所有相关方了解为系统提供恶意软件防护的安全政策和操作程序。 | | 2 | | | | |
| **要求 6：开发并维护安全的系统和应用程序** | | | | | | |
| **6.1** 制定相关流程，通过使用高声誉的外部源获取安全漏洞信息来识别安全漏洞，并为新发现的安全漏洞指定风险等级（例如“高”、“中”或“低”）。<br>*注：风险等级应以行业最优方法和潜在影响考虑为依据。例如，漏洞分级标准可能包括对 CVSS 基础得分的考虑及/或供应商的分类及/或相关系统的类型。*<br>*根据组织的环境和风险评估策略不同，评估漏洞和指定风险等级的方法也不尽相同。风险等级至少应标识出所有被视为对环境具有高风险的漏洞。除风险等级外，如果安全漏洞即将对环境造成威胁、影响关键系统且/或如果不解决可能会造成潜在危害，则可被视为重要。关键系统示例可能包括安全系统、面向公众的设备和系统、数据库以及其他存储、处理或传输持卡人数据的系统。* | | | 3 | | | |
| **6.2** 通过安装供应商提供的适用安全补丁，确保所有系统组件和软件均杜绝已知漏洞。在发布后一个月内安装关键的安全补丁。<br>*注：应按照要求 6.1 中规定的风险分级流程标识关键安全补丁。* | | | 3 | | | |
| **6.3** 遵照如下要求安全地开发内部和外部软件应用程序（包括基于 Web 的应用程序管理访问）：<br>• 按照 PCI DSS（例如安全验证和记录）<br>• 基于行业标准和/或最优方法。<br>• 信息安全并入整个软件开发生命周期 *注：*<br>*该要求适用于所有内部开发的软件以及由第三方开发的定制软件。* | | | 3 | | | |
| **6.3.1** 在激活或向客户发布应用程序前，删除开发、测试和/或自定义应用程序帐户、用户 ID 和密码。 | | | 3 | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **6.3.2** 为识别任何潜在的编码漏洞（采用人工或自动流程），请在投入生产或向客户发布前审核自定义代码，至少包括：<br>• 由代码原作者以外人员以及熟悉代码审核方法和安全编码实践的人员审核代码变更。<br>• 代码审核可确保代码的开发符合安全编码指南<br>• 发布前已进行适当修正。<br>• 代码审查结果在发布前已由管理人员审核并批准。*注：这项代码审核要求适用于所有自定义代码（内部代码和面向公众的代码），可作为系统开发生命周期的组成部分。代码审核可由经验丰富的内部人员或第三方执行。面向公众的 Web 应用程序还应受到附加控制措施的约束，以应对实施后不断出现的威胁和漏洞，具体规定请参见 PCI DSS 要求 6.6。* | | | 3 | | | |
| **6.4** 系统组件的所有变更均须遵守变更控制流程和程序。该流程必须包括如下内容： | | | 3 | | | |
| **6.4.1** 开发/测试环境独立于生产环境，并借助访问控制确保两者分离。 | | | 3 | | | |
| **6.4.2** 开发/测试环境与生产环境中的职责分离 | | | 3 | | | |
| **6.4.3** 在测试或开发过程中不使用生产数据（真实的 PAN） | | | 3 | | | |
| **6.4.4** 在激活系统/系统投入生产前，删除系统组件中的测试数据和帐户。 | | | 3 | | | |
| **6.4.5** 变更控制程序须包含： | | | | | | 6 |
| **6.4.5.1** 影响记录。 | | | | | | 6 |
| **6.4.5.2** 被授权方的变更审批记录。 | | | | | | 6 |
| **6.4.5.3** 功能测试，以确认该变更未对系统安全性造成不利影响。 | | | | | | 6 |
| **6.4.5.4** 取消程序。 | | | | | | 6 |
| **6.4.6** 完成重要变更后，须对所有新的或变更的系统和网络实施所有相关的 PCI DSS 要求，并在适当情况下更新文档记录。<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | | | | | 6 |
| **6.5** 按照以下方式处理软件开发流程中常见的编码漏洞：<br>• 至少每年对开发人员进行一次最新安全编码技术方面的培训，包括如何避免常见编码漏洞。<br>• 根据安全编码指南开发应用程序。<br>*注：在本版本 PCI DSS 发布时，已采用行业最优方法将 6.5.1 到 6.5.10 中列举的漏洞保持为最新。但当有关漏洞管理的行业最优方法（例如 OWASP 指南、前 25 大高危软件错误、CERT 安全编码等）出现更新时，这些要求必须采用当下最新的最优方法。* | | | 3 | | | |
| *注：下文的要求 6.5.1 至 6.5.6 适用于所有应用程序（内部或外部）。* | | | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **6.5.1** 注入攻击，特别是 SQL 注入。同时还须考虑 OS 命令注入、LDAP、XPath 等其他注入攻击。 | | | 3 | | | |
| **6.5.2** 缓冲区溢出 | | | 3 | | | |
| **6.5.3** 非安全加密存储 | | | 3 | | | |
| **6.5.4** 非安全通信 | | | 3 | | | |
| **6.5.5** 不正确的错误处理 | | | 3 | | | |
| **6.5.6** 漏洞识别流程中确认的所有“高风险”漏洞（具体规定请参阅 PCI DSS 要求 6.1）。 | | | 3 | | | |
| *注：要求 6.5.7 至下文的要求 6.5.10 适用于 Web 应用程序和应用程序接口（内部或外部）：* | | | | | | |
| **6.5.7** 跨站脚本 (XSS) | | | 3 | | | |
| **6.5.8** 不正确的访问控制（例如不安全的直接对象引用、未能限制网址访问、目录遍历和未能限制用户的功能访问）。 | | | 3 | | | |
| **6.5.9** 跨站请求伪造 (CSRF) | | | 3 | | | |
| **6.5.10** 失效的验证与会话管理 | | | 3 | | | |
| **6.6** 对于面向公众的网络应用程序，应不断解决新的威胁和漏洞，并通过以下任一方法确保这些应用程序不会受到已知攻击：<br>• 利用手动或自动应用程序漏洞安全评估工具或方法审核面向公众的网络应用程序，至少每年一次并在有任何变更后进行<br>*注：本评估与要求 11.2 中规定执行的漏洞扫描不同。*<br>• 在面向公众的 Web 应用程序前安装可检查和防范网页式攻击的自动化技术解决方案（例如 Web 应用程序防火墙），用以不断检查所有流量。 | | | 3 | | | |
| **6.7** 确保已记录、正在使用且所有相关方了解用于开发和维护安全系统和应用程序的安全政策和操作程序。 | | | 3 | | | |
| **要求 7：按业务知情需要限制对持卡人数据的访问** | | | | | | |
| **7.1** 仅有工作需要的个人才能访问系统组件和持卡人数据。 | | | | | | |
| **7.1.1** 为每个角色定义访问需要，包括：<br>• 每个角色依据工作职能需要访问的系统组件和数据资源<br>• 访问资源所需的权限级别 （例如，用户、管理员等）。 | | | | 4 | | |
| **7.1.2** 将特权用户 ID 的访问权限限制为执行工作职责所需的最小权限。 | | | | 4 | | |
| **7.1.3** 基于个人的工作分类和职能分配访问权限。 | | | | 4 | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **7.1.4** 需要指定所需权限的被授权方作出的书面批准。 | | | | 4 | | |
| **7.2** 为系统组件建立访问控制系统，以根据用户的知情需要限制访问，并将系统设为“全部拒绝”，特别允许访问时除外。该访问控制系统必须包含以下内容： | | | | | | |
| **7.2.1** 所有系统组件范围 | | | | 4 | | |
| **7.2.2** 基于工作分类和职能为个人分配权限。 | | | | 4 | | |
| **7.2.3** 将“全部拒绝”设为默认设置。 | | | | 4 | | |
| **7.3** 确保已记录、正在使用且所有相关方了解用于限制持卡人数据访问的安全政策和操作程序。 | | | | 4 | | |
| **要求 8：为有计算机访问权限的每个人分配唯一标识符 (ID)** | | | | | | |
| **8.1** 规定并实施政策和程序，确保对所有系统组件中的非消费者用户和管理员执行以下适当的用户识别管理： | | | | | | |
| **8.1.1** 允许用户访问系统组件或持卡人数据之前，为其分配唯一 ID。 | | 2 | | | | |
| **8.1.2** 控制添加、删除和修改用户 ID、凭证和其他标识符对象。 | | 2 | | | | |
| **8.1.3** 立即撤销到期用户的访问权限。 | | 2 | | | | |
| **8.1.4** 在 90 天内删除/禁用非活动的用户帐户。 | | 2 | | | | |
| **8.1.5** 通过如下远程访问管理第三方用于访问、支持或维护系统组件的 ID：<br>• 仅在需要的时间段启用并在不用时禁用。<br>• 使用时进行监控。 | | 2 | | | | |
| **8.1.6** 在不超过 6 次尝试后锁定用户 ID，从而限制反复的访问尝试。 | | 2 | | | | |
| **8.1.7** 将锁定时间设为最少 30 分钟或直到管理员启用用户 ID。 | | 2 | | | | |
| **8.1.8** 如果某会话空闲超过 15 分钟，则需要重新验证用户来重新激活终端或会话。 | | 2 | | | | |
| **8.2** 除了分配唯一 ID 以外，至少采用以下一种方法来验证所有用户，确保对所有系统组件中的非消费者用户和管理员执行恰当的用户验证管理：<br>• 所知，如密码或口令等<br>• 所有，如令牌设备或智能卡等<br>• 个人特征，如生物特征。 | | 2 | | | | |
| **8.2.1** 使用强效加密法以使所有验证凭证（例如密码/口令）在所有系统组件中传输和存储时均不可读。 | | 2 | | | | |
| **8.2.2** 在修改任何验证凭证（例如，执行密码重置、提供新令牌或生成新密钥）前验证用户身份。 | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **8.2.3** 密码/口令必须符合以下要求：<br>• 要求长度至少为 7 个字符。<br>• 同时包含数字和字母字符。<br>或者，密码/口令必须具有至少与上面指定参数相当的复杂度和强度。 | | 2 | | | | |
| **8.2.4** 至少每 90 天变更一次用户密码/口令。 | | 2 | | | | |
| **8.2.5** 不允许个人提交与最近所用的 4 个密码/口令中任何一个相同的新密码/口令。 | | 2 | | | | |
| **8.2.6** 将每个用户首次使用的密码/口令和重置密码/口令设为唯一值，并在首次使用后立即变更。 | | 2 | | | | |
| **8.3** 使用多因素验证保护对 CDE 的所有单独非控制台管理访问和所有远程访问。<br>*注：多因素验证要求在验证过程中至少使用三种验证方法中的两种（有关验证方法的说明，请参见要求 8.2）。使用一个因素两次（例如，使用两个不同的密码）不视为多因素验证。* | | | | | | |
| **8.3.1** 将针对所有非控制台访问的多因素验证融入针对具有管理访问权限的工作人员的 CDE。<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | 2 | | | | |
| **8.3.2** 针对来自该实体网络外部的所有远程网络访问（针对用户和管理员，并包括出于支持和维护目的的第三方访问）加入多因素验证。 | | 2 | | | | |
| **8.4** 为所有用户编写并传达验证政策和程序<br>包括：<br>• 选择强效验证凭证的指南<br>• 关于用户应如何保护其验证凭证的指南<br>• 关于不重用之前用过的密码的说明<br>• 在怀疑密码可能受到威胁的情况下更改密码的相关说明。 | | | | 4 | | |
| **8.5** 不要使用群组、共享或常规 ID、密码或其他验证方法，具体如下：<br>• 常规用户 ID 已禁用或删除。<br>• 用于系统管理和其他重要功能的共享用户 ID 不存在。<br>• 不使用共享和常规用户 ID 管理任何系统组件。 | | | | 4 | | |
| **8.5.1 仅针对服务提供商的附加要求：**可远程访问客户所在地的服务提供商（例如，为支持 POS 系统或服务器）须针对每位客户使用唯一的验证凭证（例如密码/口令）。<br>*注：本要求不适用于访问其本身托管环境（托管多个客户环境）的共享托管服务提供商。* | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **8.6** 在使用其他验证机制（例如物理或逻辑安全令牌、智能卡、证书等）的情形下，须按照下述要求分配这些机制的用法：<br>• 验证机制必须分配到单个帐户，不得在多个帐户之间共享。<br>• 必须要有物理和/或逻辑控制，以确保仅既定帐户可使用该机制获得访问权限。 | | | | 4 | | |
| **8.7** 按照下述要求限制对任何包含持卡人数据的数据库的所有访问（包括应用程序、管理员和其他所有用户的访问）：<br>• 用户对数据库的所有访问、查询和操作均通过编程方法完成。<br>• 仅数据库管理员能直接访问或查询数据库。<br>• 数据库应用程序的应用程序 ID 仅可由这些应用程序使用（个人用户或其他非应用程序流程不能使用）。 | | | | 4 | | |
| **8.8** 确保已记录，正在使用且所有相关方了解用于身份识别和验证的安全政策与操作程序。 | | | | 4 | | |
| **要求 9：限制对持卡人数据的物理访问** | | | | | | |
| **9.1** 采用适当的场所入口控制，对实际接触持卡人数据环境中的系统进行限制和监控。 | | 2 | | | | |
| **9.1.1** 利用摄像头和/或访问控制机制监控个人对敏感区域的物理访问。核查采集的数据并与其他条目关联。除非法律另有规定，否则至少存储三个月。<br>*注：“敏感区域”指任何数据中心、服务器室或任何存储、处理或传输持卡人数据的系统所在区域。这不包括仅有销售点终端的公共区域，例如零售店的收银区。* | | 2 | | | | |
| **9.1.2** 实施物理和/或逻辑控制，限制实际接触公共网络插座交换机。<br>例如，位于公共区域和访客可进入区域的网络插座交换机可能被禁用，并且仅在明确授权进行网络访问时才能启用。或者，也可以实施相应流程，以确保访客处在网络插座交换机正在运行的区域时始终有人陪同。 | | 2 | | | | |
| **9.1.3** 限制实际接触无线访问点、网关、手持式设备、网络/通信硬件和电信线路。 | | 2 | | | | |
| **9.2** 制定相关程序，以便轻松区分现场工作人员和访客，包括：<br>• 识别现场工作人员和访客（例如发放工卡）<br>• 修改访问要求<br>• 废除或取消现场工作人员和过期访客的身份证件（例如工卡）。 | | | | | 5 | |
| **9.3** 控制现场工作人员对敏感区域的物理访问，具体如下：<br>• 必须根据个人的工作职能获取使用权。<br>• 一旦离职，立即撤消使用权，所有物理访问机制（例如钥匙、访问卡等）均退回或禁用。 | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **9.4** 实施相关程序，识别并批准访客。<br>程序应包括以下方面： | | | | | | |
| **9.4.1** 访客进入前需获批准，并且在进入处理或维护持卡人数据的区域时始终有人陪同。 | | | | | 5 | |
| **9.4.2** 识别访客并给访客发放一张工卡或带有效期且能区分访客与现场工作人员的其他身份证件。 | | | | | 5 | |
| **9.4.3** 访客在离开经营场所前或证件到期时需上交工卡或身份证件。 | | | | | 5 | |
| **9.4.4** 使用访客日志，始终对访客进入经营场所、存储或传输持卡人数据的计算机房和数据中心后的活动作实际检查记录。<br>在日志上记录访客的姓名、代表的公司以及批准物理访问的现场工作人员。<br>除非法律另有规定，否则该日志至少应保留三个月。 | | | | | 5 | |
| **9.5** 保护所有媒介的实体安全。 | | | | | 5 | |
| **9.5.1** 将备份媒介存储在安全的地方，最好是外部场所，例如一个备选或备用场所，或一个商业存储设施。至少每年检查一次该场所的安全性。 | | | | | 5 | |
| **9.6** 严格控制任何媒介的内部或外部分发，包括： | | | | | | |
| **9.6.1** 对媒介进行分类，以便确定数据的敏感性。 | | | | | 5 | |
| **9.6.2** 通过可靠的快递公司或其他可准确跟踪的投递方法递送媒介。 | | | | | 5 | |
| **9.6.3** 凡自安全区域转移媒介时（包括将媒介分发给个人），确保经过管理层批准。 | | | | | 5 | |
| **9.7** 严格控制对媒介的存储和获取。 | | | | | | |
| **9.7.1** 适当维护所有媒介的盘存记录，至少每年盘点一次媒介。 | | | | | 5 | |
| **9.8** 当媒介因业务或法律原因不再需要时应予销毁，具体如下： | | | | | | |
| **9.8.1** 将硬拷贝材料粉碎、焚烧或打浆，以确保持卡人数据无法重建。确保待销毁材料所用存储容器的安全性。 | 1 | | | | | |
| **9.8.2** 使电子媒介上的持卡人数据不可恢复，以确保持卡人数据无法被重建。 | 1 | | | | | |
| **9.9** 保护通过直接接触卡本身便可捕获支付卡数据的设备，以避免设备被篡改和替换。<br>*注：这些要求适用于销售点实卡交易（即刷卡）中使用的读卡设备。本要求不适用于手动密钥输入组件，如计算机键盘和 POS 机键盘。* | | | | | | |
| **9.9.1** 保留一份最新的设备列表。该列表应包含如下信息：<br>• 设备的外形、型号<br>• 设备位置（例如安放设备的现场或设施的地址）<br>• 设备的序列号或其他独特验证方法。 | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **9.9.2** 定期检查设备的表面，以检查篡改（例如给设备增加读卡器）或替换（例如通过检查序列号或其他设备特征确认其未被欺诈性设备调换）迹象。<br>*注：设备可能被篡改或替换的迹象包括：不明附件或有线缆连接到设备，安全标签丢失或改变，外壳破损或颜色不同，序列号或其他外部标记改变。* | | 2 | | | | |
| **9.9.3** 培训工作人员，使其了解尝试篡改或替换设备的行为。培训应包括以下内容：<br>• 在允许对设备进行调整或修理之前，验证任何自称修理或维护人员的第三方人员的身份。<br>• 在未经验证的情况下，不要安装、替换或退还设备。<br>• 注意设备周围的可疑行为（例如，陌生人尝试拔掉设备插头或打开设备）。<br>• 向相关人员（例如，经理或安全人员）报告篡改或替换设备的可疑行为和迹象。 | | 2 | | | | |
| **9.10** 确保已记录、正在使用且所有相关方了解用于限制实际接触持卡人数据的安全政策和操作程序。 | | | | | 5 | |
| **要求 10：跟踪并监控对网络资源和持卡人数据的所有访问** | | | | | | |
| **10.1** 实施检查记录，将对系统组件的所有访问链接到个人用户。 | | | | 4 | | |
| **10.2** 对所有系统组件实施自动检查记录以重建以下事件： | | | | | | |
| **10.2.1** 对持卡人数据的所有个人用户访问 | | | | 4 | | |
| **10.2.2** 任何具有 root 或管理员权限的个人执行的所有操作 | | | | 4 | | |
| **10.2.3** 对所有检查记录的访问 | | | | 4 | | |
| **10.2.4** 无效的逻辑访问尝试 | | | | 4 | | |
| **10.2.5** 识别和验证机制的使用和变更（包括但不限于新建帐户和提升权限）以及具有 root 或管理员权限帐户的所有变更、添加或删除 | | | | 4 | | |
| **10.2.6** 检查日志的初始化、关闭或暂停 | | | | 4 | | |
| **10.2.7** 系统级对象的创建和删除 | | | | 4 | | |
| **10.3** 对于每次事件，至少记录所有系统组件的以下检查记录条目： | | | | | | |
| **10.3.1** 用户识别 | | | | 4 | | |
| **10.3.2** 事件类型 | | | | 4 | | |
| **10.3.3** 日期和时间 | | | | 4 | | |
| **10.3.4** 成功或失败指示 | | | | 4 | | |
| **10.3.5** 事件的起因 | | | | 4 | | |
| **10.3.6** 受影响的数据、系统组件或资源的特性或名称。 | | | | 4 | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **10.4** 使用时间同步技术来同步所有关键系统的时钟和时间，并确保实施以下各项以获取、分配并存储时间。<br>*注：网络时间协议 (NTP) 便是一种时间同步技术。* | | | | 4 | | |
| **10.4.1** 关键系统的时间正确且一致。 | | | | 4 | | |
| **10.4.2** 时间数据受保护。 | | | | 4 | | |
| **10.4.3** 时间设置来自行业认可的时间来源。 | | | | 4 | | |
| **10.5** 保护检查记录，禁止进行更改。 | | | | | | |
| **10.5.1** 只允许有工作需要的人查看检查记录。 | | | | 4 | | |
| **10.5.2** 防止检查记录文件受到非授权修改。 | | | | 4 | | |
| **10.5.3** 即时将检查记录文件备份到难以更改的中央日志服务器或媒介中。 | | | | 4 | | |
| **10.5.4** 将向外技术的日志写入安全的内部中央日志服务器或媒介设备。 | | | | 4 | | |
| **10.5.5** 对日志使用文件完整性监控或变更检测软件可确保未生成警报时无法变更现有日志数据（虽然新增数据不应生成警报）。 | | | | 4 | | |
| **10.6** 审核所有系统组件的日志和安全事件以识别异常情况或可疑活动。<br>*注：可使用日志搜集、分析和告警工具来满足本要求。* | | | | | | |
| **10.6.1** 至少每天审核一次以下内容：<br>• 所有安全事件<br>• 存储、处理或传输 CHD 和/或 SAD 的所有系统组件的日志<br>• 所有关键系统组件的日志<br>• 执行安全功能的所有服务器和系统组件（例如，防火墙、入侵检测系统/入侵防御系统 (IDS/IPS)、验证服务器、电子商务重定向服务器等）的日志。 | | | | 4 | | |
| **10.6.2** 根据组织的年度风险评估结果，基于组织的政策和风险管理策略定期审核所有其他系统组件的日志。 | | | | 4 | | |
| **10.6.3** 跟进审核过程中发现的例外和异常。 | | | | 4 | | |
| **10.7** 保留检查记录历史至少一年，其中最少 3 个月的记录可立即访问以供分析（例如，在线、存档或可从备份恢复）。 | | | | 4 | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **10.8 仅针对服务提供商的附加要求：**实施流程，以便及时检测和报告关键安全控制系统故障，包括但不限于以下方面故障：<br>• 防火墙<br>• IDS/IPS<br>• FIM<br>• 杀毒<br>• 物理访问控制<br>• 逻辑访问控制<br>• 检查日志机制<br>• 分段控制（如使用）<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | | | 4 | | |
| **10.8.1 仅针对服务提供商的附加要求：**及时响应任何关键安全控制故障。安全控制故障响应流程须包括：<br>• 恢复安全功能<br>• 识别并记录安全故障持续时间（日期以及从开始到结束的时间）<br>• 识别并记录故障原因（包括根本原因），并记录解决根本原因所需的补救措施<br>• 识别并解决故障期间引发的任何安全问题<br>• 执行风险评估，确定是否需要因安全故障执行进一步操作<br>• 实施控制，以防故障原因再次发生<br>• 恢复安全控制监控<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | | | 4 | | |
| **10.9** 确保已记录、正在使用且所有相关方了解用于监控所有网络资源和持卡人数据访问的安全政策和操作程序。 | | | | 4 | | |
| **要求 11：定期测试安全系统和流程** | | | | | | |
| **11.1** 实施流程以测试是否存在无线访问点 (802.11)，并按季度检车和识别所有授权和非授权的无线访问点。<br>*注：可用于该流程的方法包括但不限于无线网络扫描、系统组件和基础架构的物理/逻辑检查、网络访问控制 (NAC) 或无线 IDS/IPS。无论使用何种方法，都必须足以检测并识别授权和非授权设备。* | | | | 4 | | |
| **11.1.1** 保留一份授权的无线接入点清单，包括业务理由记录。 | | | | 4 | | |
| **11.1.2** 如果检测到非授权的无线接入点，则实施事故响应程序。 | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **11.2** 至少每个季度运行一次内部和外部网络漏洞扫描，并且在网络有任何重大变化（例如安装新的系统组件，更改网络拓扑，修改防火墙规则，产品升级）时也运行漏洞扫描。<br>*注：可在季度扫描流程中综合多次扫描报告，以表明所有系统均已扫描，且所有漏洞均已解决。可能需要其他文档记录来确认未修复的漏洞处于解决过程中。*<br>*如果评估商确认 1) 最近的扫描结果为通过，2) 实体具备要求每季度扫描一次的书面政策和程序，3) 扫描结果中指出的漏洞在重新扫描中显示为已修复，则不要求四次季度扫描均通过才能认定最初 PCI DSS 合规。在最初 PCI DSS 审核后的几年里，必须出现四次季度扫描结果均为通过的情况。* | | 2 | | | | |
| **11.2.1** 执行季度内部漏洞扫描。解决漏洞并执行重新扫描，确认已根据实体的漏洞等级解决了所有“高风险”漏洞（根据要求 6.1）。必须由合格人员执行扫描。 | | 2 | | | | |
| **11.2.2** 通过由支付卡行业安全标准委员会 (PCI SSC) 认证的授权扫描服务商 (ASV) 执行每季度一次的外部漏洞扫描。视需要执行重复扫描，直至获得扫描通过结果。<br>*注：季度外部漏洞扫描必须由支付卡行业安全标准委员会 (PCI SSC) 认证的授权扫描服务商 (ASV) 执行。如需了解扫描客户的责任、扫描准备等，请参阅 PCI SSC 网站上发布的《ASV 计划指南》。* | | 2 | | | | |
| **11.2.3** 在发生任何重大变更后执行内部和外部扫描，并视需要执行重新扫描。必须由合格人员执行扫描。 | | 2 | | | | |
| **11.3** 实施包含以下内容的穿透测试法：<br>• 以行业认可的穿透测试法为基础（例如 NIST SP800-115）<br>• 覆盖整个 CDE 环境和关键系统<br>• 来自网络内部和外部的测试<br>• 用于验证任何网段和范围缩小控制的测试<br>• 定义应用层穿透测试，至少包括要求 6.5 中列出的漏洞<br>• 定义网络层穿透测试，包括支持网络功能和操作系统的组件<br>• 审核并考虑过去 12 个月内遇到的威胁和漏洞<br>• 详细说明保留穿透测试结果和修复活动结果。 | | 2 | | | | |
| **11.3.1** 每年至少执行一次外部穿透测试，并且在基础架构或应用程序有任何重要升级或修改时（例如操作系统升级、环境新增子网络或环境新增 Web 服务器）也执行该测试。 | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **11.3.2** 至少每年执行一次内部穿透测试，并在基础架构或应用程序有任何重要升级或修改（例如操作系统升级、环境新增子网络或环境新增 Web 服务器）后也执行该测试。 | | 2 | | | | |
| **11.3.3** 在穿透测试中发现的可利用漏洞已得到修复，并通过重复执行的测试确认修复。 | | 2 | | | | |
| **11.3.4** 如果利用分段将 CDE 与其他网络隔离，应至少每年执行一次穿透测试，并在分段控制/方法有任何变更后执行测试，以确认该分段方法行之有效，并已将所有范围外系统与 CDE 中的系统进行隔离。 | | 2 | | | | |
| **11.3.4.1 仅针对服务提供商的附加要求：**如果使用了分段，请通过至少每半年执行一次穿透测试以及在分段控制/方法有任何变更后执行穿透测试，以确认 PCI DSS 范围。<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | 2 | | | | |
| **11.4** 使用入侵检测和/或入侵防御技术检测和/或防止入侵网络。监控持卡人数据环境周围以及持卡人数据环境中关键点的所有流量，并警示工作人员注意可疑威胁。<br>确保所有入侵检测和防御引擎、基线和签名均为最新。 | | 2 | | | | |
| **11.5** 部署变更检测机制（例如文件完整性监控工具），以便在关键系统文件、配置文件或内容文件发生非授权修改（包括变更、添加和删除）时警示工作人员；并将软件配置为至少每周执行一次关键文件对比。<br>*注：在变更检测中，重要文件通常指那些不经常变更但一旦变更即表示系统受到威胁或面临威胁风险的文件。变更检测机制（例如文件完整性监控产品）通常预先配置了相关操作系统的重要文件。其他重要文件（例如自定义应用程序的重要文件）必须由该实体（即商户或服务提供商）评估和定义。* | | | | 4 | | |
| **11.5.1** 实施流程，针对变更检测解决方案发出的任何警报作出响应。 | | | | 4 | | |
| **11.6** 确保已记录、正在使用且所有相关方均了解用于安全监控与测试的安全政策和操作程序。 | | | | 4 | | |
| **要求 12：维护针对所有工作人员的信息安全政策** | | | | | | |
| **12.1** 制定、发布、维护和宣传安全政策。 | | | | | | 6 |
| **12.1.1** 至少每年审核一次安全政策，并在环境变更时更新政策。 | | | | | | 6 |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.2** 实施风险评估流程，该流程：<br>• 至少每年执行一次，并在环境发生重大变更时（例如收购、合并、迁址等）执行，<br>• 确定重要资产、威胁和漏洞，并<br>• 形成正式的书面风险分析。<br>风险评估方法示例包括但不限于 OCTAVE、ISO 27005 和 NIST SP 800-30。 | 1 | | | | | |
| **12.3** 制定关键技术的使用政策，并规定这些技术的正确用法。<br>*注：关键技术包括但不限于，远程访问和无线技术、笔记本电脑、平板电脑、可移动电子媒介以及电子邮件和互联网的使用。*<br>确保这些使用政策要求： | | | | | | 6 |
| **12.3.1** 被授权方的明确许可 | | | | | | 6 |
| **12.3.2** 技术使用验证 | | | | | | 6 |
| **12.3.3** 一份列出所有此类设备和具有访问权的工作人员的列表 | | | | | | 6 |
| **12.3.4** 一种确定负责人、联系方式和用途的准确方便的方法（例如设备的贴标、编码和/或盘存） | | | | | | 6 |
| **12.3.5** 可接受的技术使用方式 | | | | | | 6 |
| **12.3.6** 技术可接受的网络位置 | | | | | | 6 |
| **12.3.7** 公司批准的产品列表 | | | | | | 6 |
| **12.3.8** 非活跃状态持续一定时间后自动中断远程访问技术的会话 | | | | | | 6 |
| **12.3.9** 仅在供应商和业务合作伙伴需要时为其激活远程访问技术，并在使用后立即停用 | | | | | | 6 |
| **12.3.10** 对于通过远程访问技术访问持卡人数据的工作人员，除非因规定的业务需要获得明确许可，否则禁止将持卡人数据复制、移动和存储到本地硬盘及可移动电子媒介上。<br>如果有经批准的业务需要，使用政策必须规定应按照所有适用的 PCI DSS 要求保护数据。 | | | | | | 6 |
| **12.4** 确保安全政策和程序明确规定所有工作人员的信息安全责任。 | | | | | | 6 |
| **12.4.1 仅针对服务提供商的附加要求：**行政管理人员应明确保护持卡人数据和 PCI DSS 遵从性计划的责任，包括：<br>• 全面负责维护 PCI DSS 遵从性<br>• 规定 PCI DSS 遵从性计划以及与行政管理人员进行沟通的相关章程<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | | | | | 6 |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.5** 将下列信息安全管理职责分配给个人或团队： | | | | | | 6 |
| **12.5.1** 制定、记录和分发安全政策与程序。 | | | | | | 6 |
| **12.5.2** 监控和分析安全警报与信息，并分发给相应人员。 | | | | | | 6 |
| **12.5.3** 建立、记录并分发安全事故响应和逐级上报程序，确保及时有效地处理所有情况。 | | 2 | | | | |
| **12.5.4** 管理用户帐户，包括添加、删除和修改。 | | | | | | 6 |
| **12.5.5** 监控并控制所有数据访问。 | | | | | | 6 |
| **12.6** 实施了正式的安全意识计划，以使所有工作人员了解持卡人数据安全政策和程序。 | | | | | | 6 |
| **12.6.1** 人员一经录用即进行培训，此后每年至少培训一次。<br>注：根据工作人员的角色及其对持卡人数据的访问级别，可采用不同的方法。 | | | | | | 6 |
| **12.6.2** 要求工作人员每年至少确认一次自己已阅读并了解安全政策和程序。 | | | | | | 6 |
| **12.7** 在录用人员前筛选应征者，以最大程度地降低内部攻击的风险。（背景调查包括以往的工作经历、犯罪记录、信用记录以及证明人调查。）<br>*注：对于门店收银员这样的职位，本要求仅作为建议，因为他们在交易时一次只能访问一个卡号。* | | | | | | 6 |
| **12.8** 维护并实施政策和程序，以管理共享持卡人数据或可影响持卡人数据安全的服务提供商，具体方式如下： | | 2 | | | | |
| **12.8.1** 维护服务提供商列表（包括所提供服务的说明）。 | | 2 | | | | |
| **12.8.2** 维护书面协议，其中包括确认服务提供商负责其处理或者代表客户以其他方式存储、处理或传输的持卡人数据的安全性，或对客户持卡人数据环境安全性的影响程度。<br>*注：“确认”的确切措辞取决于双方协议、所提供服务的详情以及分配给每一方的责任。“确认”不一定要包含与本要求完全相同的措辞。* | | 2 | | | | |
| **12.8.3** 确保已建立雇用服务提供商的流程（包括雇用前相应的尽职调查）。 | | 2 | | | | |
| **12.8.4** 通过维护一项计划来监控（至少每年一次）服务提供商的 PCI DSS 遵从性状态。 | | 2 | | | | |
| **12.8.5** 维护关于每个服务提供商所管理的 PCI DSS 要求，以及实体所管理的 PCI DSS 要求的信息。 | | 2 | | | | |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.9 仅针对服务提供商的附加要求：**服务提供商以手写方式向客户确认负责其处理或以其他方式代表客户存储、处理或传输的持卡人数据的安全性，或对客户持卡人数据环境安全性的影响程度。<br>*注：“确认”的确切措辞取决于双方协议、所提供服务的详情以及分配给每一方的责任。“确认”不一定要包含与本要求完全相同的措辞。* | | 2 | | | | |
| **12.10** 实施事故响应计划。随时准备立即响应系统漏洞。 | | | | | | |
| **12.10.1** 建立在出现系统漏洞时实施的事故响应计划。确保该计划至少包括以下内容：<br>• 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<br>• 详细的事故响应程序<br>• 业务恢复和继续程序<br>• 数据备份流程<br>• 报告威胁的法律要求分析<br>• 所有关键系统组件的范围和响应<br>• 支付品牌对事故响应程序的参考或应用。 | | 2 | | | | |
| **12.10.2** 审核并测试计划，包括要求 12.10.1 中列出的所有要素，至少一年一次。 | | 2 | | | | |
| **12.10.3** 指定可全天候响应警报的特定人员。 | | 2 | | | | |
| **12.10.4** 为具有安全漏洞响应责任的员工提供恰当的培训。 | | 2 | | | | |
| **12.10.5** 包含来自安全监控系统（包括但不限于入侵检测系统、入侵防御系统、防火墙和文件完整性监控系统）的警报。 | | 2 | | | | |
| **12.10.6** 根据以往的经验教训并结合行业发展情况，制定修改并改进事故响应计划的流程。 | | 2 | | | | |
| **12.11 仅针对服务提供商的附加要求：**至少每季度进行一次审查，以确认工作人员遵守安全政策和操作程序。审查须涵盖以下流程：<br>• 日常日志审查<br>• 防火墙规则集审查<br>• 将配置标准应用于新系统<br>• 响应安全警报<br>• 更改管理流程<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | | | | | 6 |

| PCI DSS 要求 3.2 版 | 里程碑 | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| **12.11.1 仅针对服务提供商的附加要求：**维护季度审查流程文档记录，使其包括：<br>• 记录审查结果<br>• 由指定负责 PCI DSS 遵从性计划的工作人员审查并签核结果<br>*注：本要求在 2018 年 1 月 31 日前属于最优方法，此后成为一项要求。* | | | | | | 6 |
| **附录 A1：针对共享托管服务提供商的 PCI DSS 附加要求** | | | | | | |
| **A1** 根据 A1.1 至 A1.4，保护每个实体（即商户、服务提供商或其他实体）的托管环境和数据：<br>托管服务提供商必须满足这些要求以及 PCI DSS 中所有其他相关章节的要求。<br>*注：即使托管服务提供商满足这些要求，也不能保证雇用该托管服务提供商的实体的遵从性。每个实体均必须遵从 PCI DSS 并验证其遵从性（如果适用）。* | | | 3 | | | |
| **A1.1** 确保每个实体仅运行可访问自身持卡人数据环境的流程。 | | | 3 | | | |
| **A1.2** 每个实体的访问权限和特权仅限其自身的持卡人数据环境。 | | | 3 | | | |
| **A1.3** 确保日志记录和检查记录已启用、对于每个实体的持卡人数据环境唯一且符合 PCI DSS 要求 10。 | | | 3 | | | |
| **A1.4** 启用相关流程，确保在任何托管商户或服务提供商受到威胁时提供及时的取证调查。 | | | 3 | | | |
| **附录 A2：针对使用 SSL/早期 TLS 的实体的 PCI DSS 附加要求**<br>*注：本附录适用于将 SSL/早期 TLS 用作安全控制以保护 CDE 和/或 CHD 的实体* | | | | | | |
| **A2.1** 针对使用 SSL 和/或早期 TLS 的 POS POI 终端（及其连接到的 SSL/TLS 终端点），实体须：<br>• 确认设备不易受上述协议已知漏洞的影响。或者：<br>• 采用了正式的风险降低和迁移计划。 | | 2 | | | | |
| **A2.2** 拥有使用 SSL 和/或早期 TLS 的现有实施项目（A2.1 允许的内容除外）的实体须采用正式的风险降低和迁移计划。 | | 2 | | | | |
| **A2.3 仅针对服务提供商的附加要求：**所有服务提供商均须在 2016 年 6 月 30 日前提供安全服务产品。<br>*注：在 2016 年 6 月 30 日前，服务提供商须在其提供的服务中增加安全协议选项，或者建立已存档的风险降低和迁移计划（根据要求 A2.2），其中包含提供安全协议选项的目标日期，该日期不晚于 2016 年 6 月 30 日。该日期之后，所有服务提供商均须提供适用于其服务的安全协议选项。* | | 2 | | | | |