支付卡行业 (PCI)
数据安全标准

要求和安全评估程序

3.0 版

2013 年 11 月

文档变更记录

日期	版本	描述	页码
2008 年 10 月	*1.2*	*将 PCI DSS 1.2 版改称“PCI DSS 要求和安全评估程序”，避免文档之间的重复，并对* PCI DSS 安全审核程序 1.1 版做了综合和具体变更。*如需完整信息，请参阅* PCI DSS 1.1 版到 1.2 版的 PCI 数据安全标准变更汇总。	
2009 年 7 月	*1.2.1*	*增补 PCI DSS 1.1 版和 1.2 版之间被误删的句子。*	*5*
		将测试程序 6.3.7.a 和 6.3.7.b 中的“随后”更正为“比”。	*32*
		删除测试程序 6.5.b 中“到位”和“未到位”栏的灰色标记。	*33*
		在“补偿性控制工作表 - 完整示例”中，修正页面顶部的用语，改为“利用本工作表为通过补偿性控制备注为‘到位’的任何要求定义补偿性控制”。	*64*
2010 年 10 月	*2.0*	*更新并实施 1.2.1 版的变更。请参阅*“PCI DSS - PCI DSS 1.2.1 版到 2.0 版的变更汇总”。	
2013 年 11 月	*3.0*	*更新 2.0 版。请参阅*“PCI DSS - PCI DSS 2.0 版到 3.0 版的变更汇总”。	

目录

简介和 PCI 数据安全标准概述

本支付卡行业数据安全标准 (PCI DSS) 旨在促进并增强持卡人的数据安全，便于统一的数据安全措施在全球范围内的广泛应用。PCI DSS 为意在保护持卡人数据的技术和操作要求提供了一个基准。PCI DSS 适用于所有涉及支付卡处理的实体，包括商户、处理机构、收单机构、发卡机构、服务提供商以及所有其他存储、处理或传输持卡人数据 (CHD) 和/或敏感验证数据 (SAD) 的实体。以下是对 12 条 PCI DSS 要求的主要概述。

PCI 数据安全标准–主要概述

建立并维护安全的网络和系统	**1.** 安装并维护防火墙配置以保护持卡人数据 **2.** 不要使用供应商提供的默认系统密码和其他安全参数
保护持卡人数据	**3.** 保护存储的持卡人数据 **4.** 加密持卡人数据在开放式公共网络中的传输
维护漏洞管理计划	**5.** 为所有系统提供恶意软件防护并定期更新杀毒软件或程序 **6.** 开发并维护安全的系统和应用程序
实施强效访问控制措施	**7.** 按业务知情需要限制对持卡人数据的访问 **8.** 识别并验证对系统组件的访问 **9.** 限制对持卡人数据的物理访问
定期监控并测试网络	**10.** 跟踪并监控对网络资源和持卡人数据的所有访问 **11.** 定期测试安全系统和流程
维护信息安全政策	**12.** 维护针对所有工作人员的信息安全政策

本文档*《PCI 数据安全标准要求和安全评估程序》*将 12 条 PCI DSS 要求和相应的测试程序合并为一个安全评估工具。该工具在 PCI DSS 遵从性评估期间专门用作实体验证程序的组成部分。以下提供的详细指南和最优方法可协助实体准备、执行 PCI DSS 评估并汇报评估结果。PCI DSS 要求和测试程序自第 14 页开始。

除当地、地区和行业法律法规外，PCI DSS 至少要包含一组持卡人数据保护要求，并通过制定附加控制措施和操作规程加以完善，以进一步规避风险。另外，立法或监管规定可能会要求对个人可识别信息或其他数据元素（例如持卡人姓名）施以特别保护。PCI DSS 不能取代当地或地区法律、政府法规或其他法律要求。

PCI DSS 资源

PCI 安全标准委员会 (PCI SSC) 网站 (www.pcisecuritystandards.org) 上提供有很多补充资源，可用于协助组织完成 PCI DSS 评估和验证，其中包括：

- 文档库，包括：
  - PCI DSS – PCI DSS 2.0 版到 3.0 版的变更汇总
  - PCI DSS 快速参考指南
  - PCI DSS 和 PA-DSS 术语、缩写词和首字母缩略词词汇表
  - 增补信息和指南
  - PCI DSS 的优先方法
  - 遵从性报告 (ROC) 的报告模板和报告说明
  - 自我评估调查问卷 (SAQ) 以及 SAQ 说明和指南
  - 遵从性证明书 (AOC)
- 常见问题 (FAQ)
- 小商户网站中的 PCI
- PCI 培训课程和信息网络会议
- 合格的安全性评估商 (QSA) 和授权扫描服务商 (ASV) 列表
- PTS 批准设备和 PA-DSS 认证支付应用程序列表

注：增补信息对 PCI DSS 进行补充，并明确规定要满足 PCI DSS 要求的其他考虑因素和建议（不能取代、代替或扩充 PCI DSS 或其中任何一项要求）。

有关这些及其他资源的信息，请参阅 www.pcisecuritystandards.org。

PCI DSS 适用性信息

PCI DSS 适用于所有涉及支付卡处理的实体，包括商户、处理机构、收单机构、发卡机构、服务提供商以及所有其他存储、处理或传输持卡人数据和/或敏感验证数据的实体。

持卡人数据和敏感验证数据的定义如下：

帐户数据	
持卡人数据包括：	***敏感验证数据包括：***
▪ 主帐户 (PAN) ▪ 持卡人姓名 ▪ 失效日 ▪ 业务码	▪ 全磁道数据（磁条数据或芯片上的等效数据） ▪ CAV2/CVC2/CVV2/CID ▪ PIN/PIN 数据块

主帐户是持卡人数据的决定性因素。 如果持卡人姓名、业务码和/或失效日与 PAN 一起存储、处理或传输，或以其他方式出现在持卡人数据环境中，则必须按照所有适用的 PCI DSS 要求予以保护。

PCI DSS 要求适用于可存储、处理或传输帐户数据（持卡人数据和/或敏感验证数据）的组织和环境。部分 PCI DSS 要求也可能适用于外包其支付操作或 CDE 管理的组织 [1]。此外，将 CDE 或支付操作外包给第三方的组织有责任确保第三方按照适用的 PCI DSS 要求保护帐户数据。

下页中的表格列举了持卡人数据和敏感验证数据的常用元素、是否允许存储各数据元素，以及是否必须保护各数据元素。该表格的内容并非详尽无遗，只用于列举适用于每种数据元素的不同类型的要求。

		数据元素	允许存储	按照要求 3.4 实现存储数据的不可读性
帐户数据	持卡人数据	主帐户 (PAN)	是	是
		持卡人姓名	是	否

[1] 遵循个人支付品牌遵从性计划

		业务码	是	否
		失效日	是	否
	敏感验证数据 [2]	全磁道数据 [3]	否	要求 3.2 规定不能存储
		CAV2/CVC2/CVV2/CID[4]	否	要求 3.2 规定不能存储
		PIN/PIN 数据块 [5]	否	要求 3.2 规定不能存储

PCI DSS 要求 3.3 和 3.4 仅适用于 PAN。如果 PAN 与持卡人数据的其他元素一起存储，仅 PAN 必须按照 PCI DSS 要求 3.4 实现不可读性。

授权之后，即使已加密，也不允许存储敏感验证数据。即使环境中没有 PAN，该规定仍适用。组织应直接联系其收单机构或个人支付品牌，了解是否允许在授权前存储 SAD、可存储时间以及任何相关用法和保护要求。

2 *授权之后，不允许存储敏感验证数据（即使已加密）*
3 *磁条上的全磁道数据，芯片或其他地方上的等效数据*
4 *印在支付卡正面或背面的三位或四位数值*
5 *数据持卡人在有卡交易时输入的个人识别码，和/或出现在交易信息中已加密的 PIN 数据块*

PCI DSS 与 PA-DSS 的关系

PCI DSS 对 PA-DSS 应用程序的适用性

实体使用符合支付应用程序数据安全标准 (PA-DSS) 的应用程序本身并不表示其遵从 PCI DSS 要求，这是因为应用程序必须应用于符合 PCI DSS 的环境，并遵守支付应用程序供应商提供的 PA-DSS 实施指南。

凡存储、处理或传输持卡人数据的应用程序均属于实体的 PCI DSS 评估范围，包括已按照 PA-DSS 验证的应用程序。PCI DSS 评估应确认经 PA-DSS 验证的支付应用程序已按照 PCI DSS 的要求正确配置并安全应用。如果支付应用程序已经过任何定制，在 PCI DSS 评估期间则需开展更深入的审核，因为该应用程序可能已经不能代表经 PA-DSS 验证的版本。

PA-DSS 要求出自*《PCI DSS 要求和安全评估程序》*（详见本文档）。PA-DSS 详细规定了支付应用程序必须满足的要求，以促使客户遵守 PCI DSS。

在符合 PCI DSS 的环境中使用安全支付应用程序，可最大限度减少潜在的安全漏洞，从而防止 PAN、全磁道数据、卡片验证码与验证值 (CAV2、CID、CVC2、CVV2)、PIN 和 PIN 数据块遭受威胁，并避免因安全漏洞所造成的严重欺诈行为。

要确定 PA-DSS 是否适用于指定的支付应用程序，请参阅《PA-DSS 程序指南》，该《指南》可在 www.pcisecuritystandards.org 上获取。

PCI DSS 对支付应用程序供应商的适用性

如果支付应用程序供应商可存储、处理或传输持卡人数据或有权访问其客户的持卡人数据（例如充当服务提供商的角色），则 PCI DSS 适用于该供应商。

PCI DSS 要求的范围

本 PCI DSS 安全要求适用于持卡人数据环境中包含或与之连接的所有系统组件。持卡人数据环境 (CDE) 包含存储、处理或传输持卡人数据或敏感验证数据的人员、流程和技术。“系统组件”包括网络设备、服务器、计算设备和应用程序。系统组件包括但不限于：

- 提供安全服务（例如验证服务器）、方便分段（例如内部防火墙）或可能影响 CDE 安全性（例如名称解析或 web 跳转服务器）的系统。
- 虚拟化组件，例如虚拟机、虚拟交换机/路由器、虚拟设备、虚拟应用程序/桌面和虚拟机监控程序。
- 网络组件，包括但不限于防火墙、交换机、路由器、无线接入点、网络设备和其他安全设备。
- 服务器类型，包括但不限于 web、应用程序、数据库、验证、邮件、代理、网络时间协议 (NTP) 和域名系统 (DNS)。
- 应用程序，包括所有购买和自定义的应用程序以及内部和外部（例如互联网）应用程序。
- 位于 CDE 内或连接到 CDE 的任何其他组件或设备。

PCI DSS 评估的第一步是准确确定审核范围。评估至少每年进行一次，接受评估的实体应在年度评估前查找持卡人数据的所有位置和数据流并确保其包含在 PCI DSS 的范围内，从而确定实体 PCI DSS 范围的准确性。要确定 PCI DSS 范围的准确性和适宜性，可执行下列步骤：

- 接受评估的实体查找并记录其环境中存在的所有持卡人数据，确认所有持卡人数据均包含在当前规定的 CDE 之内。
- 在确定并记录持卡人数据的所有位置后，实体可利用相关结果确认 PCI DSS 的范围是否适宜（例如，结果可能是一个关于持卡人数据位置的图表或目录）。
- 实体应考虑任何属于 PCI DSS 评估范围和 CDE 组成部分的持卡人数据。如果实体发现当前未纳入 CDE 的数据，应将这些数据安全地删除、迁移到当前规定的 CDE 内，或重新界定 CDE 以纳入该数据。
- 实体将保留有关说明如何确定 PCI DSS 范围的文档记录。这些文档记录留待评估商审核以及/或留作下一次年度 PCI DSS 范围确认活动的参考。

对于每一次 PCI DSS 评估，评估商都必须验证评估范围是准确界定并有文档记录的。

网络分段

持卡人数据环境的网络分段或将持卡人数据环境与实体网络的剩余部分隔离（分段）并非 PCI DSS 的一项要求。但这种方法值得大力推荐，因为它可以：

- 缩小 PCI DSS 的评估范围

- 减少 PCI DSS 的评估费用
- 降低实施和维护 PCI DSS 控制的成本和难度
- 降低组织面临的风险（通过将持卡人数据合并到更少、更易控制的位置来降低风险）

如果没有足够的网络分段（有时也称为“扁平网络”），则整个网络均属于 PCI DSS 的评估范围。网络分段可通过若干物理或逻辑方法来实现，例如正确配置的内部网络防火墙、带有严格访问控制列表的路由器或其他限制访问特定网络分段的技术。如果被视为不属于 PCI DSS 的评估范围，则系统组件必须与 CDE 正确隔离（分段），这样即便该范围外系统组件受到威胁，也无法影响 CDE 的安全性。

要缩小持卡人数据环境的范围需满足一个重要的前提条件，即清楚了解与持卡人数据的存储、处理或传输有关的业务需求和流程。通过消除不必要的数据和合并必要的数据将持卡人数据限制尽量少的位置，这可能需要对长期业务实践进行重建。

通过数据流程图记录持卡人数据流有助于全面了解所有的持卡人数据流，并确保任意网络分段在隔离持卡人数据环境时均有效。

如果已设置网络分段并将其用于缩小 PCI DSS 的评估范围，则评估商必须确认该分段足以缩小评估范围。处于高层级时，充足的网络分段可将存储、处理或传输持卡人数据的系统与其他无法执行此类操作的系统隔离开来。然而，就具体实施的网络分段而言，其充足性非常多变并且取决于多种因素，例如特定网络的配置、部署的技术以及可能已实施的其他控制措施。

*附录 D：网络分段与企业设施/系统组件抽样*提供了更多关于网络分段和抽样对 PCI DSS 评估范围所产生影响的信息。

无线

如果采用无线技术存储、处理或传输持卡人数据（例如销售点交易、“快速结帐”），或者如果无线局域网 (WLAN) 是持卡人数据环境的一部分或与之连接，则面向无线环境的 PCI DSS 要求和测试程序适用且必须执行（例如要求 1.2.3、2.1.1 和 4.1.1）。在实施无线技术前，实体应根据风险认真评估该技术的必要性。仅针对非敏感数据传输考虑部署无线技术。

采用第三方服务提供商 / 外包

对需要接受年度现场评估的服务提供商而言，必须对持卡人数据环境中的所有系统组件执行遵从性验证。

服务提供商或商户可通过第三方服务提供商代为存储、处理或传输持卡人数据，或管理路由器、防火墙、数据库、物理安全和/或服务器等组件。在此情况下，持卡人数据环境的安全性可能会受影响。

各方应清楚确定服务提供商的 PCI DSS 评估范围内所包含的服务和系统组件、服务提供商规定的具体 PCI DSS 要求以及服务提供商的客户有责任纳入各自 PCI DSS 审核的任何要求。例如，托管管理供应商应明确规定哪些 IP 地址应作为其季度安全漏洞扫描过程的一部分进行扫描，哪些 IP 地址由客户负责纳入各自的季度扫描。

第三方服务提供商验证遵从性时有两种选择：

1) 他们可自行接受 PCI DSS 评估并向客户提供证据证明其遵从性；或
2) 如果未自行接受 PCI DSS 评估，则需在每位客户的 PCI DSS 评估中接受服务审核。

如果第三方自行接受 PCI DSS 评估，则应向客户提供充分证据，证明该服务提供商的 PCI DSS 评估范围涵盖客户适用的服务，且相关 PCI DSS 要求已检查完毕并认定现已到位。服务提供商向客户提供的具体证据类型将取决于双方的现有协议/合同。例如，提供 AOC 和/或服务提供商 ROC（为保护任何机密信息而编写）的相关部分有助于提供全部或部分信息。

此外，商户和服务提供商必须管理并监督所有有权访问持卡人数据的相关第三方服务提供商的 PCI DSS 遵从性。*请参阅本文档中的要求 12.8 了解详情。*

在常规业务流程中实施 PCI DSS 的最优方法

为确保安全控制继续得以妥善实施，实体应在常规业务 (BAU) 活动中实施 PCI DSS，作为整个安全策略的一部分。实体可借此持续监控其安全控制的有效性，并在两次 PCI DSS 评估之间维护 PCI DSS 遵从性环境。

关于应如何将 PCI DSS 纳入常规业务活动的方式包括但不限于：

1. 监控安全控制（例如防火墙、入侵检测系统/入侵防御系统 (IDS/IPS)，文件完整性监控 (FIM)、反病毒、访问控制等） – 以确保其按计划有效地运作。
2. 确保及时发现所有安全控制故障并作出响应。安全控制故障响应流程应包括：
   - 恢复安全控制
   - 找出故障原因
   - 发现并解决安全控制故障期间出现的任何安全问题
   - 实施防范措施（例如过程或技术控制），防止故障原因再次出现
   - 恢复对安全控制的监控，或在一段时间内加强监控力度，以确认控制正在有效运行
3. 在完成环境变更（例如增加新系统、变更系统或网络配置）前审查这些变更，并执行下列操作：
   - 确定对 PCI DSS 范围的潜在影响（例如允许 CDE 中的某个系统与另一系统连接的一条防火墙新规则可能会将额外的系统或网络纳入 PCI DSS 的范围）
   - 确定 PCI DSS 要求适用于受变更影响的系统和网络（例如，如果一个新系统属于 PCI DSS 的范围，则可能需要按照系统配置标准进行配置，包括 FIM、AV、补丁和检查日志等，并需添加进季度漏洞扫描计划）
   - 更新 PCI DSS 范围并视情况实施安全控制
4. 组织结构如有变化（例如公司合并或收购），应正式审核其对 PCI DSS 范围和要求的影响。

5. 应定期进行审核和沟通，以确保 PCI DSS 要求继续有效并且工作人员均遵守安全流程。此类定期审核应涵盖所有设施和位置（包括零售店、数据中心等）并应包括系统组件（或系统组件样本）审核，以确认 PCI DSS 要求继续有效，例如配置标准已应用，补丁和 AV 已更新，检查日志已审核等。定期审核的频度应由实体根据其环境的规模和复杂性确定。

   此类审核还可用于确认已保留适当证据（例如检查日志、漏洞扫描报告、防火墙检查等），从而帮助实体为下一次遵从性评估做准备。

6. 至少每年审核一次硬件和软件技术，确认其继续获得供应商的支持，并能满足实体的安全要求（包括 PCI DSS）。如果发现这些技术未继续获得供应商的支持或不能满足实体的安全需求，实体则应制定补救方案、更新或者甚至在必要时替换该技术。

除了上述方法外，组织还可以考虑实现安全功能的职责分离，以便将安全性和/或审计功能与操作功能分开。在单人承担多重职责的环境中（例如管理和安全操作），可以转让职责，确保没有任何个人拥有流程的端到端控制，而缺少一个独立的检查点。例如，可以将配置工作和变更审批工作分配给不同的人。

注意：这些在常规业务流程中实施 PCI DSS 的最优方法仅为提供建议和指导，并不能代替或扩展任何 PCI DSS 要求。

对于评估商：企业设施/系统组件抽样

如果企业设施和/或系统组件的数量很多，评估商可选择采取抽样的方式简化评估流程。

评估商可以对企业设施/系统组件进行抽样，作为对实体 PCI DSS 遵从性审核的一部分，但实体不可将 PCI DSS 要求仅应用于其环境的样本部分（例如，有关季度漏洞扫描的要求适用于所有系统组件）。同样，评估商也不可只审核样本部分的 PCI DSS 遵从性要求。

在考虑被评估环境的整体范围和复杂性后，评估商可独立选择有代表性的企业设施/系统组件样本，以评估实体对 PCI DSS 要求的遵从情况。必须首先明确企业设施样本，然后明确每个选定的企业设施中的系统组件样本。样本必须选择所有企业设施类型和位置中以及所选企业设施内所有系统组件类型中具有代表性的部分。样本必须足够大，这样才能让评估商确信控制措施已按预期实施。

企业设施包括但不限于：公司办公室、商店、加盟店、处理机构、数据中心及处于不同位置的其他设施类型。抽样应包括每个所选企业设施内的系统组件。例如，对于每个选定的企业设施，均包括适用于受审核区域的各种操作系统、功能和应用程序。

例如，评估商可选定企业设施中的一个样本，包括运行 Apache 的 Sun 服务器、运行 Oracle 的 Windows 服务器、运行遗留卡处理应用程序的大型机系统、运行 HP-UX 的数据传输服务器和运行 MySQL 的 Linux 服务器。如果所有应用程序均从一个版本的操作系统（例如 Windows 7 或 Solaris 10）运行，该样本仍应包含各种应用程序（例如数据库服务器、web 服务器、数据传输服务器）。

在独立选择企业设施/系统组件样本时，评估商应考虑以下方面：

- 如果现有可确保一致性且每个企业设施/系统组件必须遵守的标准化、集中式的 PCI DSS 安全与操作流程和控制，则样本总量可比没有标准流程/控制时小。样本必须足够大，这样才能让评估商合理确信所有企业设施/系统组件均按照标准流程配置。评估商必须确认此类标准化、集中式控制均已实施并有效运作。
- 如果现有一种以上的标准安全和/或操作流程（例如针对不同类型的企业设施/系统组件），则样本必须足够大才能包含采用每种安全流程的企业设施/系统组件。
- 如果目前未采用任何 PCI DSS 标准流程/控制，并且每个企业设施/系统组件均通过非标准流程进行管理，则样本必须更大，这样评估商才能确信每个企业设施/系统组件均已适当执行 PCI DSS 要求。
- 系统组件的样本必须包含正在使用的每个类型和组合。例如，在对应用程序抽样时，样本必须包含每类应用程序的所有版本和平台。

对于使用抽样法的每种情形，评估商必须：

- 记录抽样方法和样本容量背后的依据，
- 记录并验证确定样本容量时使用的标准化 PCI DSS 流程和控制，以及
- 解释样本适宜且在整体中具有代表性的原因。

请同时参阅：附录 D：《网络分段与企业设施/系统组件抽样》。

评估商必须在每次评估中重复验证抽样依据。如果要采用抽样法，必须为每次评估选择不同的企业设施和系统组件样本。

补偿性控制

评估商每年均须记录、审核和验证补偿性控制一次，并同时提交遵从性报告，具体遵照*附录 B：《补偿性控制》*和*附录 C：《补偿性控制工作表》*。

对于每项补偿性控制，**必须**填写《补偿性控制工作表》*（附录 C）*。此外，应在遵从性报告相应的 PCI DSS 要求栏内记录补偿性控制结果。

如需了解更多关于"补偿性控制"的详情，请参阅上述*附录 B* 和 *C*。

遵从性报告的说明与内容

*PCI DSS ROC 报告模板*中现提供有遵从性报告 (ROC) 的说明与内容。

必须使用 *PCI DSS ROC 报告模板*作为创建*遵从性报告*的模板。接受评估的实体应遵守每个支付品牌各自的报告要求，以确保各支付品牌确认实体的遵从状态。请与各支付品牌或收单机构联系，确定报告要求和说明。

PCI DSS 评估流程

1. 确认 PCI DSS 的评估范围。
2. 根据每项要求的测试程序执行环境 PCI DSS 评估。
3. 如果需要，纠正任何不到位的项目。
4. 根据适用的 PCI 指南和说明，完成适用的评估报告（即自我评估调查问卷 (SAQ) 或遵从性报告 (ROC)），包括所有补偿性控制文档记录。
5. 如果适用，完成服务提供商或商户的遵从性证明书。遵从性证明书可从 PCI SSC 网站获取。
6. 向收单机构（商户）、支付品牌或其他申请机构（服务提供商）提交 SAQ 或 ROC、遵从性证明书以及任何其他要求的文档记录（例如 ASV 扫描报告）。

详细的 PCI DSS 要求和安全评估程序

以下提供了《*PCI DSS 要求和安全评估程序*》列标题的定义：

- **PCI DSS 要求** – 此列定义数据安全标准要求；根据这些要求对 PCI DSS 遵从性进行验证。
- **测试程序** – 此列展示评估商用来验证 PCI DSS 要求是否满足且“到位”的流程。
- **指南** – 此列说明每项 PCI DSS 要求的目的或安全目标。本列只包含指南，旨在帮助读者理解每项要求的目的。本列中的指南并不替代或扩充《PCI DSS 要求和测试程序》。

注：*如果未□施或□划在将来某个日期完成控制，□□□ PCI DSS 要求不到位。在实体纠正任何未完成或不到位的项目后，评估商会重新进行评估以验证是否完成纠正且满足所有要求。*

请参阅以下资源（位于 PCI SSC 网站），记录 PCI DSS 评估：

- *关于完成遵从性报告 (ROC) 的说明，请参阅《PCI DSS ROC 报告模板》。*
- *关于完成自我□估□□□卷 (SAQ) 的说明，请参阅《PCI DSS SAQ 说明和指南》。*
- *关于提交 PCI DSS 遵从性□□□告的□明，□参□《PCI DSS 遵从性□明□》。*

建立并维护安全的网络和系统

要求 1：　　安装并维护防火墙配置以保护持卡人数据

防火墙是一种用以控制实体网络（内部）和不可信网络（外部）之间允许的计算机访问流量，以及实体内部可信网络中较敏感区域的输入和输出流量的设备。例如，持卡人数据环境就是实体可信网络中的较敏感区域。

防火墙会检查所有网络流量并阻止不符合指定安全标准的传输。

无论是以电子商务方式通过互联网访问、员工经桌面浏览器访问互联网、员工电子邮件访问、专用连接（例如企业对企业连接）还是通过无线网络或其他来源进入系统，都应避免任何系统受到来自不可信网络的非授权访问。通常，连接到不可信网络和来自其的看似不显眼的路径会使关键系统遭受无保护的访问。防火墙是任何计算机网络的关键防护机制。

只要符合要求 1 中规定的防火墙最低要求，其他系统组件也能提供防火墙功能。如果在持卡人数据环境中使用其他系统组件来提供防火墙功能，则这些设备必须纳入要求 1 的范围和评估中。

PCI DSS 要求	测试程序	指南
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** 检查防火墙和路由器配置标准以及以下指定的其他文档记录，并确认已按如下方式完成并实施这些标准：	防火墙和路由器是控制网络输入和输出的架构的关键组件，是阻止非法访问并管理授权访问和退出网络的软硬件设备。 配置标准和程序有助于确保组织的第一道数据防线始终强大。
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	**1.1.1.a** 检查书面程序，确认存在测试和批准以下所有内容的正式流程： • 网络连接以及 • 防火墙和路由器配置变更	用于批准和测试所有连接以及防火墙和路由器变更的已记录和实施的流程有助于避免因网络、路由器或防火墙的错误配置导致的安全问题。 如果不正式批准和测试变更，变更记录可能无法得到更新，从而导致网络记录和实际配置不一致。
	1.1.1.b 针对网络连接样本，与负责人员面谈并检查记录，确认网络连接已得到批准和测试。	
	1.1.1.c 确定防火墙和路由器配置的实际变更样本，将其与变更记录对比并与负责人员面谈，以确认变更已得到批准和测试。	
1.1.2 标识持卡人数据环境和其他网络（含任何无线网络）间所有连接的当前网络图表	**1.1.2.a** 检查图表并查看网络配置，确认存在当前网络图且该图记录了持卡人数据的所有连接（包括任何无线网络）。	网络图说明了网络的配置方法，并标识出所有网络设备的位置。 如果没有当前网络图，设备可能遭到忽略并在无意中被排除在对 PCI DSS 实施的安全控制之外，因而容易受到威胁。
	1.1.2.b 与负责人员面谈，确认图表为最新。	
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。	**1.1.3.a** 检查数据流程图并与工作人员面谈，确认图表： • 显示整个系统和网络中所有持卡人数据流	持卡人数据流程图标识出网络内存储、处理或传输的所有持卡人数据的位置。

PCI DSS 要求	测试程序	指南
	• 为最新且在出现环境变更时根据需要更新	网络和持卡人数据流程图通过显示持卡人数据在网络间以及单个系统和设备间的流动方式，帮助组织了解并跟踪其环境的范围。
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	**1.1.4.a** 检查防火墙配置标准并确认其包含各互联网连接以及任何 DMZ 和内部网络区域间的防火墙要求。	通过在进入（和退出）网络的每个互联网连接以及任何 DMZ 和内部网络间使用防火墙，组织可监控和控制访问并将恶意个人通过不受保护的连接访问内部网络的机会降到最低。
	1.1.4.b 确认当前网络图与防火墙配置标准一致。	
	1.1.4.c 根据所记录的配置标准和网络图，查看网络配置，确认各互联网连接的防火墙以及任何非军事区 (DMZ) 和内部网络区域间的防火墙均已到位。	
1.1.5 网络组件管理群组、角色与责任的说明	**1.1.5.a** 确认防火墙和路由器配置标准包括网络组件管理群组、角色与责任的说明。	角色说明和责任分配可确保工作人员知道所有网络组件的安全负责人，且组件管理人员了解自己的责任。如果角色与责任未进行正式分配，则设备可能无人管理。
	1.1.5.b 与网络组件管理的负责人员面谈，确认已根据文档记录分配角色与责任。	
1.1.6 使用所有获准服务、协议和端口的文档记录和业务理由，包括对非安全协议实施安全功能的文档记录。 非安全服务、协议或端口包括但不限于 FTP、Telnet、POP3、IMAP 以及 SNMP 1 版和 2 版。	**1.1.6.a** 确认防火墙和路由器配置标准包含所有服务、协议和端口的文档记录列表，包括每一项（例如，超文本传输协议 (HTTP) 和安全套接层 (SSL)、安全外壳 (SSH) 和虚拟专用网络 (VPN) 协议）的业务理由。	威胁通常由不用或非安全的服务和端口导致，这是因为此类服务和端口一般都存在已知的漏洞而很多组织不会修补不修补其不使用的服务、协议和端口的漏洞（即使漏洞仍然存在）。通过明确界定和记录自身业务所需的服务、协议和端口，组织可以确保禁用或删除所有其他服务、协议和端口。 如果业务需要用到非安全的服务、协议或端口，则组织应清楚了解并接受使用这些协议会带来的风险，使用协议应有正当的理由，且应记录并实施允许安全使用这些协议的安全功能。如果业务不需要用到这些非安全的服务、协议或端口，则应加以禁用或删除。
	1.1.6.b 识别获准的非安全服务、协议和端口；确认已记录每个服务的安全功能。	
	1.1.6.c 检查防火墙和路由器配置，确认已对每个非安全服务、协议和端口实施有文档记录的安全功能。	
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	**1.1.7.a** 确认防火墙和路由器配置标准，规定至少每半年审核一次防火墙和路由器规则集。	通过该审核，组织能至少每半年清除一次不需要、过时或错误的规则，并确保所有规则集只允许使用与有文档记录的业务理由相符的授权服务和端口。 防火墙和路由器规则集出现大量变更的组织会希望通过实施更频繁的审核来确保规则集继续满足业务需要。
	1.1.7.b 检查与规则集审核相关的文档记录并与负责人员面谈，确认至少每半年审核一次规则集。	
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。 ***注：****"不可信网络"是指受审核实体所属网络之外的网络，和/或不受实体控制或管理的网络。*	**1.2** 检查防火墙和路由器配置并执行以下操作，确认不可信网络与持卡人数据环境中系统组件间的连接受限。	在内部可信网络以及任何外部和/或不受实体控制或管理的不可信网络之间安装网络防护很重要。如果无法正确实施本措施，实体将容易遭受恶意个人或软件的非授权访问。 要使防火墙功能生效，则必须进行正确配置，从而

PCI DSS 要求	测试程序	指南
		控制和/或限制进出实体网络的流量。
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。	**1.2.1.a** 检查防火墙和路由器配置标准，确认其规定了持卡人数据环境所需的输入和输出流量。	本要求旨在防止恶意个人通过非授权的 IP 地址访问实体网络或以非授权的方式使用服务、协议或端口（例如，将从您的网络中获取的数据发送到不可信服务器）。 实施规则以拒绝任何非特别所需的输入和输出流量有助于避免因疏忽造成的漏洞，防止输入或输出意料之外和可能有害的流量。
	1.2.1.b 检查防火墙和路由器配置，确认输入和输出流量限制在持卡人数据环境所需的范围。	
	1.2.1.c 检查防火墙和路由器配置，确认已明确拒绝所有其他输入和输出流量，例如，使用明确的“拒绝所有”或在允许声明后含蓄地表达拒绝之意。	
1.2.2 保护并同步路由器配置文件。	**1.2.2.a** 检查路由器配置文件，确认其不会遭受非授权访问。	当运行（或活动）中的路由器配置文件包含当前安全设置时，启动文件（重启或启动路由器时使用）必须更新为相同的安全设置，才能确保在启动配置运行时应用这些设置。 由于启动配置文件只是偶尔运行，因此通常会被遗忘且不进行更新。当路由器重启并且加载的启动配置未更新为与运行配置相同的安全设置时，可能会导致规则减弱，进而允许恶意个人访问网络。
	1.2.2.b 检查路由器配置并确认其已同步，例如，运行（或活动）配置与启动配置（启动电脑时使用）匹配。	
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。	**1.2.3.a** 检查防火墙和路由器配置，确认所有无线网络和持卡人数据环境间均已安装外围防火墙。	采用已知（或未知）的方法来执行和利用网络中的无线技术是恶意个人访问网络和持卡人数据的常用方法。如果在实体不知情时安装了无线设备或网络，则恶意个人可“悄无声息”地轻松进入网络。如果防火墙不限制无线网络对 CDE 的访问，则非授权访问无线网络的恶意个人可轻松连接到 CDE 并威胁帐户信息的安全性。 无论无线网络连接到的环境有何用途，所有无线网络和 CDE 之间都必须安装防火墙。其中包括但不限于公司网络、零售店、客户网络、仓库环境等。
	1.2.3.b 确认防火墙拒绝流量或（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。	
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** 检查防火墙和路由器配置（包括但不限于互联网中的阻塞路由器、DMZ 路由器和防火墙、DMZ 持卡人分段、外围路由器以及内部持卡人网段）并执行以下操作，以确定互联网和内部持卡人网段中的系统组件之间并无直接访问：	防火墙主要用于管理并控制公共系统和内部系统（特别是存储、处理或传输持卡人数据的系统）之间的所有连接。如果允许公共系统和 CDE 之间进行直接访问，则恶意个人会跳过防火墙提供的保护，并使存储持卡人数据的系统组件受到威胁。

PCI DSS 要求	测试程序	指南
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。	**1.3.1** 检查防火墙和路由器配置，确认已实施 DMZ 以仅向提供授权服务、协议和端口（支持公共访问）的系统组件输入流量。	DMZ 属于网络的一部分，管理着互联网（或其他不可信网络）与组织需向公众提供的服务（如 web 服务器）之间的连接。 该功能旨在阻止恶意个人通过互联网访问组织的内部网络或以非授权的方式使用服务、协议或端口。
1.3.2 仅向 DMZ 内的 IP 地址输入互联网流量。	**1.3.2** 检查防火墙和路由器配置，确认仅向 DMZ 内的 IP 地址输入互联网流量。	
1.3.3 禁止任何直接的入站和出站连接在互联网和持卡人数据环境之间产生流量。	**1.3.3** 检查防火墙和路由器配置，确认已禁止直接的入站和出站连接在互联网和持卡人数据环境之间产生流量。	通过检查所有入站和出站的连接，可根据源地址和/或目标地址检查并限制流量，同时检查并阻止不需要的内容，从而避免不可信和可信环境之间未过滤的访问。这有助于防止恶意个人将从您的网络获取的数据发送到不可信网络的外部不可信服务器。
1.3.4 执行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）	**1.3.4** 检查防火墙和路由器配置，确认已执行反欺骗措施，例如内部地址无法从互联网进入 DMZ。	通常，数据包包含最初发送它的计算机的 IP 地址，因此网络中的其他计算机知道数据包的来源。恶意个人经常会试图假冒（或模仿）发送的 IP 地址，以使目标系统相信数据包来自可信来源。 过滤进入网络的数据包的作用之一是确保数据包不会遭到“假冒”，而看似来自组织自身内部的网络。
1.3.5 禁止从持卡人数据环境到互联网的非授权输出流量。	**1.3.5** 检查防火墙和路由器配置，确认从持卡人数据环境输出到互联网的流量有明确授权。	从持卡人数据环境输出的所有流量都应进行评估以确保其遵守已制定和授权的规则。应检查连接，仅允许授权通信的流量（例如，通过限制源/目标地址/端口，和/或阻止内容）。
1.3.6 实施状态检查，也称动态数据包过滤。（即只有“已建立的”连接才能进入网络。）	**1.3.6** 检查防火墙和路由器配置，确认防火墙执行状态检查（动态数据包过滤）。（只有与之前建立的会话关联的已建立连接才能进入网络。）	执行状态数据包检查的防火墙可维持通过防火墙实现的每个连接的“状态”。通过维持“状态”，防火墙可知道对之前连接作出的明显响应是有效的授权响应（因为防火墙会保存每个连接的状态）还是尝试骗取防火墙连接许可的恶意流量。
1.3.7 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。	**1.3.7** 检查防火墙和路由器配置，确认存储持卡人数据的系统组件放置在与 DMZ 以及其他不可信网络隔离的内部网络区域中。	如果持卡人数据位于 DMZ 中，则外部攻击者更容易访问此信息，这是因为要穿透的层数更少。将存储持卡人数据的系统组件放置于通过防火墙与 DMZ 以及其他不可信网络隔离的内部网络区域中，可防止非授权网络流量到达系统组件。 ***注：****本要求不适用于易失性存储器中暂时存储的持卡人数据。*

PCI DSS 要求	测试程序	指南
1.3.8 不要将私人 IP 地址和路由信息泄露给非授权方。 ***注：****掩盖 IP 地址的方法包括但不限于：* ▪ *网络地址转换 (NAT)* ▪ *将包含持卡人数据的服务器放置在代理服务器/防火墙中，* ▪ *删除或过滤针对采用注册地址的专用网络的路由器广告，* ▪ *在内部使用 RFC1918 地址空间而非注册地址。*	**1.3.8.a** 检查防火墙和路由器配置，确认防止私人 IP 地址和路由信息从内部网络泄漏到互联网的方法到位。	限制内部或私人 IP 地址的泄漏对于防止黑客“得知”内部网络的 IP 地址并使用该信息访问网络很关键。 根据所使用的特定网络技术，可采用不同的方法来实现本要求的目的。例如，IPv4 和 IPv6 网络可使用不同的控制措施来满足本要求。
	1.3.8.b 与工作人员面谈并检查记录，确认针对外部实体的任何私人 IP 地址和路由信息的泄漏都经过授权。	
1.4 在位于外网时仍连接到互联网且可用以访问网络的任意移动设备和/或员工自有设备（例如，员工使用的笔记本电脑）上安装个人防火墙软件。防火墙配置包括： • 个人防火墙软件设有特定的配置设置 • 个人防火墙软件正在积极运行 • 移动设备用户和/或员工自有设备用户无法更改个人防火墙软件。	**1.4.a** 检查政策和配置标准，确认： • 处于外网时仍连接到互联网且可用以访问网络的所有移动设备和/或员工自有设备（例如，员工使用的笔记本电脑）均要求安装个人防火墙软件 • 已为个人防火墙软件定义特定的配置设置 • 个人防火墙软件配置为积极运行 • 个人防火墙软件配置为无法由移动设备用户和/或员工自有设备用户更改。	可以在公司防火墙外连接到互联网的移动计算设备更容易受到攻击。使用个人防火墙有助于保护设备免受网络攻击。这些攻击会在设备重新连接到网络后，利用该设备来访问组织内的系统和数据。 ***注：****本要求适用于员工自有和公司所有的计算机。无法通过公司政策管理的系统会带来外围漏洞并为恶意个人提供可利用的机会。允许不可信系统连接到组织的网络，可能会导致攻击者和其他恶意用户获得访问权限。*
	1.4.b 检查移动设备和/或员工自有设备样本，确认： • 个人防火墙软件已根据组织的特定配置设置进行安装和配置 • 个人防火墙软件正在积极运行 • 移动设备用户和/或员工自有设备用户无法更改个人防火墙软件	
1.5 确保已记录、正在使用且所有相关方了解用于防火墙管理的安全政策和操作程序。	**1.5** 检查文档记录并与工作人员面谈，确认用于防火墙管理的安全政策和操作程序： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守安全政策和操作程序，确保始终对防火墙和路由器进行管理，从而防止对网络的非授权访问。

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

恶意个人（实体的外部和内部）经常使用供应商默认密码和其他供应商默认设置来威胁系统安全。黑客团体十分了解并可通过公共信息轻松确定这些密码和设置。

PCI DSS 要求	测试程序	指南
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。 该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、简单网络管理协议 (SNMP) 社区字符串等使用的默认密码。	**2.1.a** 选择系统组件样本并尝试使用供应商提供的默认帐户和密码登录（在系统管理员的帮助下）设备和应用程序，以确认所有默认密码（包括操作系统、提供安全服务的软件、应用程序和系统帐户、POS 终端以及简单网络管理协议 (SNMP) 社区字符串使用的默认密码）均已修改。（使用供应商手册和互联网资源找到供应商提供的帐户/密码。）	恶意个人（组织外部和内部）经常使用供应商默认设置、帐户名和密码来破坏操作系统软件、应用程序以及安装这些软件和程序的系统。由于这些默认设置通常会对外发布且黑客团体对此十分了解，因此更改这些设置会降低系统受到攻击的可能性。 即使不打算使用默认帐户，将默认密码修改为独一无二的强效密码并禁用帐户也能防止恶意个人重新启用帐户并用默认密码进行访问。
	2.1.b 针对系统组件样本，确认所有不必要的默认帐户（包括操作系统、安全软件、应用程序、系统、POS 终端、SNMP 等使用的帐户） 均已删除或禁用。	
	2.1.c 与工作人员面谈并检查支持文档记录，确认： • 在网络中安装系统前，已更改所有供应商默认值（包括操作系统、提供安全服务的软件、应用程序和系统帐户、POS 终端、简单网络管理协议 (SNMP) 社区字符串等使用的默认密码）。 • 在网络中安装系统前，已删除或禁用不必要的默认帐户 （包括操作系统、安全软件、应用程序、系统、POS 终端、SNMP 等使用的帐户）。	
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。		如果无线网络未实施充分的安全配置（包括更改默认设置），则无线嗅探器可窃听流量、轻松捕获数据和密码并轻易进入并攻击网络。 另外，用于旧版本 802.11x 加密（有线等效加密或 WEP）的关键交换协议已失效且会导致加密无效。应更新设备固件以支持更多安全协议。
	2.1.1.a 与负责人员面谈并检查支持文档记录，确认： • 密钥默认值在安装时已更改 • 知道密钥的任何人离职或更换岗位时即更改密钥。	
	2.1.1.b 与工作人员面谈并检查政策和程序，确认 • 默认的 SNMP 社区字符串必须在安装时更改。 • 访问点的默认密码/口令必须在安装时更改。	
	2.1.1.c 在系统管理员的帮助下检查供应商文档记录并登录无线设备，确认： • 未使用默认的 SNMP 社区字符串 • 未使用访问点的默认密码/口令。	
	2.1.1.d 检查供应商文档记录并查看无线配置设置，确认已更新无线设备的固件以支持以下操作的强效加密：	

PCI DSS 要求	测试程序	指南
	• 无线网络验证 • 无线网络传输。	
	2.1.1.e 检查供应商文档记录并查看无线配置设置，确认其他与安全有关的无线供应商默认值均已更改（如果适用）。	
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。 行业认可的系统强化标准来源包括但不限于： ▪ 互联网安全中心 (CIS) ▪ 国际标准化组织 (ISO) ▪ 美国系统网络安全协会 (SANS) ▪ 国家标准与技术研究所 (NIST)	**2.2.a** 检查组织所有类型系统组件的系统配置标准，确认系统配置标准与行业认可的系统强化标准一致。	很多操作系统、数据库和企业应用程序都存在已知的漏洞，同时也拥有已知的方法可用于配置这些系统，从而修补安全漏洞。为帮助非安全专家人士，很多安全组织提出了系统强化指南和建议，就如何修复此类漏洞提供指导建议。 有关配置标准的指南来源包括但不限于：www.nist.gov、www.sans.org、www.cisecurity.org、www.iso.org 和产品供应商。 系统配置标准必须保持最新状态，以确保在网络上安装系统前已修复新发现的漏洞。
	2.2.b 检查政策并与工作人员面谈，确认在发现新的安全漏洞问题时系统配置标准已经更新，具体规定请参阅要求 6.2。	
	2.2.c 检查政策并与工作人员面谈，确认在配置新系统时已应用系统配置标准，并且在网络上安装系统前已确认到位。	
	2.2.d 确认系统配置标准包含以下适合所有类型系统组件的程序： • 更改供应商提供的所有默认值，并清除非必要的默认帐户 • 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 • 仅启用系统功能所需的必要服务、协议、守护进程等 • 对于任何被视为不安全的必要服务、协议或守护进程，均执行附加安全功能 • 配置系统安全参数，以防滥用 • 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	
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。） ***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。*	**2.2.1.a** 选择系统组件样本，并检查系统配置，确认每台服务器仅执行一项主要功能。	如果需要不同安全级别的服务器功能位于同一台服务器上，由于存在安全性较低的功能，需要较高安全性的功能其安全级别将因此而降低。此外，安全级别较低的服务器功能可能会给同一台服务器上的其他功能带来安全漏洞。作为系统配置标准和相关流程的一部分，通过考虑不同服务器功能的安全需求，组织可以确保需要不同安全级别的功能不会并存于同一台服务器上。
	2.2.1.b 如果采用虚拟化技术，检查系统配置，确认每个虚拟系统组件或设备仅执行一项主要功能。	
2.2.2 仅启用系统功能所需的必要服务、协议、守护进程等。	**2.2.2.a** 选择系统组件样本，并检查已启用的系统服务、守护进程和协议，确认仅启用了必要的服务或协议。	正如要求 1.1.6 所述，企业需要（或已通过默认值启用）的很多协议常被恶意个人利用，对网络造成威胁。本要求应成为组织配置标准和相关流程的一部分，以确保仅启用必要的服务和协议。
	2.2.2.b 找出任何已启用的不安全服务、守护进程或协议，并与工作人员面谈，确认已根据书面配置标准判断其实属合理。	
2.2.3 对于任何被视为不安全的服务、协议	**2.2.3.a** 检查配置设置，确认已针对所有不安全的服务、守护进	在部署新服务器前启用安全功能将防止服务器被

PCI DSS 要求	测试程序	指南
或守护进程，均执行附加安全功能 — 例如，采用 SSH、S-FTP、SSL 或 IPSec VPN 等安全技术保护 NetBIOS、文件共享、Telnet、FTP 等不安全的服务	程或协议记录并执行安全功能。	安装在具有不安全配置的环境中。 确保所有不安全的服务、协议和守护进程均通过相应的安全功能得到充分的安全保护，令恶意个人难以利用网络内常用的威胁点。
2.2.4 配置系统安全参数，以防滥用。	**2.2.4.a** 与系统管理员和/或安全经理面谈，确认其了解系统组件的常用安全参数设置。	系统配置标准和相关流程应特别针对常用安全设置和参数（了解使用中的每类系统的安全隐患）。 为实现安全的系统配置，负责配置和/或系统管理的工作人员必须了解适用于该系统的具体安全参数和设置。
	2.2.4.b 检查系统配置标准，确认其中包含常用的安全参数设置。	
	2.2.4.c 选择系统组件样本，并检查常用安全参数，确认已按照配置标准对其进行适当设置。	
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。	**2.2.5.a** 选择系统组件样本，并检查此类配置，确认所有非必要功能（例如脚本、驱动程序、特性、子系统、文件系统等） 均已删除。	非必要功能可为恶意个人提供更多访问系统的机会。在删除非必要功能后，组织可专注于必要功能的安全，降低未知功能被利用的风险。 将此要求纳入服务器强化标准和流程可解决涉及非必要功能的具体安全隐患（例如，如果服务器不执行这些功能，可通过删除/禁用 FTP 或 web 服务器来解决）。
	2.2.5.b 检查文档记录和安全参数，确认已启用的功能具有文档记录并且支持安全配置。	
	2.2.5.c 检查文档记录和安全参数，确认抽选的系统组件样本上仅出现具有文档记录的功能。	
2.3 使用强效加密法对所有非控制台管理访问进行加密。对于基于 web 的管理和其他非控制台管理访问，可采用 SSH、VPN 或 SSL/TLS 等技术。	**2.3** 选择系统组件样本，并确认已通过执行以下方式对非控制台管理访问进行加密：	如果非控制台（包括远程）管理未采用安全认证和加密通信，敏感管理或操作级信息（例如管理员的 ID 和密码）便可能泄露给窃听者。恶意个人可利用这些信息访问网络，变身为管理员，然后窃取数据。 明文协议（例如 HTTP、telnet 等） 不会对流量或登录详情加密，所以窃听者很容易便能截取这类信息。 要称得上“强效加密”，应在所使用技术类型适用的情况下具备行业认可的具有适当关键优势和密钥管理的协议。（请参阅 *《PCI DSS 和 PA-DSS 术语、缩略词和首字母缩略词词汇表》* 中“强效加密”一词的定义。）
	2.3.a 在管理员登录到每个系统时进行查看，并检查系统配置，确认在要求提供管理员密码前已调用强效加密法。	
	2.3.b 审核系统上的服务和参数文件，确定不存在可访问非控制台的 Telnet 及其他不安全的远程登录命令。	
	2.3.c 在管理员登录到每个系统时进行查看，确认已采用强效加密法对管理员访问任何基于 web 的管理界面的权限进行加密。	
	2.3.d 检查供应商文档记录并与工作人员面谈，确认已按照行业最优方法和/或供应商建议对所使用的技术实施强效加密	
2.4 保留一份 PCI DSS 范围内系统组件的清单	2.4.a 检查系统清单，确认已保留一份软硬件组件列表，并包含各自的功能/用途描述：	保留一份所有系统组件的最新列表能使组织准确有效地界定其实施 PCI DSS 控制的环境范围。没有这份清单，某些系统组件可能会被遗漏，并被不小心排除在组织的配置标准之外。
	2.4.b 与工作人员面谈，确认书面清单保持为最新。	
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	**2.5** 检查文档记录并与工作人员面谈，确认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均：	工作人员需了解并遵守安全政策和日常操作程序，确保始终对供应商默认设置及其他安全参数

PCI DSS 要求	测试程序	指南
全政策和操作程序。	• 已记录， • 正在使用，且 • 为所有相关方所了解	进行管理，从而避免不安全的配置。
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 A：《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。*	**2.6** 对于共享托管服务提供商的 PCI DSS 评估，需执行*附录 A《针对共享托管服务提供商的 PCI DSS 附加要求》中详述的测试程序* ***A.1.1*** *至* ***A.1.4***，以确认共享托管服务提供商确实会保护其实体（商户和服务提供商）的托管环境和数据。	本要求适用于在同一台服务器上为多个客户提供共享托管环境的托管服务提供商。当所有数据都位于同一台服务器上且处于单一环境控制下时，这些共享服务器的设置通常不由单个客户管理。这样会使客户添加可影响所有其他客户环境安全的不安全功能和脚本，从而让恶意个人能轻易破坏某个客户的数据，并访问所有其他客户的数据。请参阅*附录 A* 了解详细要求。

保护持卡人数据

要求 3：　　保护存储的持卡人数据

诸如加密、截词、掩盖和散列等保护方法都是持卡人数据保护的重要组成部分。即使入侵者绕过其他安全控制并获得加密数据的访问权险，但如果没有正确的加密密钥，仍不能读取或使用这些数据。此外，也应考虑使用其他保护已存储数据的有效方法，以降低潜在风险。例如，最大限度地降低风险的方法包括：如非绝对必要则不存储持卡人数据，如不需要完整 PAN 则截词持卡人数据，不使用终端用户消息传递技术（例如电子邮件和即时消息）发送未受保护的 PAN。

请参阅*《PCI DSS 和 PA-DSS 术语、缩略词和首字母缩略词词汇表》*中"强效加密"和其他 PCI DSS 术语的定义。

PCI DSS 要求	测试程序	指南
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： ▪ 将数据存储量和保留时间限制在法律、法规和业务要求的范围内 ▪ 不再需要时安全删除数据的流程 ▪ 持卡人数据的具体保留要求 ▪ 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。	**3.1.a** 检查数据保留和处理政策、程序与流程，确认其至少包含以下方面： • 关于数据保留的法律、法规和业务要求，包括 • 保留持卡人数据的具体要求（例如因 Y 业务原因，需将持卡人数据保留 X 的时间）。 • 因法律、法规或业务原因而不再需要时安全删除持卡人数据 • 涵盖持卡人数据存储的所有方面 • 按季度查找并安全删除所存储的超过规定保留期限要求的持卡人数据的流程。	正式的数据保留政策明确规定了需要保留的数据和数据存储的地方，以便能在不再需要这些数据时将其安全地销毁或删除。 授权后可存储的唯一持卡人数据为主帐户或 PAN（令其不可读取）、失效日、持卡人姓名和业务码。 必须了解持卡人数据的存储位置，以便能适当保留或在不再需要时予以适当处理。要对保留要求作适当规定，实体首先需要了解自己的业务需求、适用于其行业以及/或被保留的数据类型的所有法律或法规义务。 查找并删除已超过指定保留期限的存储数据可防止不必要地保留不再需要的数据。该过程可以自动或由人工完成，或二者相结合。例如，可以执行程控程序（自动或手动）来查找和删除数据，以及/或人工审核数据存储区。 采用安全删除方法可确保当不再需要时无法检索到数据。 ***记住，如果不需要，则不存储！***
	3.1.b 与工作人员面谈，确认： • 数据保留和处理流程中包含所有位置的已存储持卡人数据。 • 现有按季度执行的自动或人工流程可用于识别并安全删除存储的持卡人数据。 • 针对所有位置的持卡人数据按季度执行自动或人工流程。	

PCI DSS 要求	测试程序	指南
	3.1.c 对于存储持卡人数据的系统组件样本， • 检查文件和系统记录，确认存储的数据未超出数据保留政策中的要求 • 查看删除机制，确认数据已安全删除。	
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。 *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：* • *有正当的业务理由且* • *数据存储安全。* 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：	**3.2.a** 对于发卡机构和/或支持发卡服务并存储敏感验证数据的公司，需审核政策并与工作人员面谈，确认具备存储敏感验证数据的有文档记录的正当业务理由。	敏感验证数据包括全磁道数据、卡验证代码或值以及 PIN 数据。禁止在授权后存储敏感验证数据！这类数据对恶意个人非常重要，因为他们可借此生成假冒支付卡，进行欺诈性交易。
	3.2.b 对于发卡机构和/或支持发卡服务并存储敏感验证数据的公司，需检查数据存储和系统配置，以确认敏感验证数据的安全性。	发行支付卡的实体或者提供或支持发行服务的实体通常会将创建和控制敏感验证数据作为发行功能的一部分。提供、促进或支持发行服务的公司仅在有存储敏感验证数据的合理业务需求时方可存储此类数据。应当注意，所有 PCI DSS 要求均适用于发卡机构，对发卡机构和发卡机构处理商而言，唯一的例外就是在有正当理由时方可保留敏感验证数据。正当理由指发卡机构履行职能时必需的理由，而非因便所需理由。凡此类数据均须安全存储，并且遵守所有 PCI DSS 要求和具体的支付品牌要求。 非发卡实体不得在授权后保留敏感验证数据。
	3.2.c 对于所有其他实体，如果收到敏感验证数据，需审核政策和程序，并检查系统配置，以确认这些数据并非在授权后保留。	
	3.2.d 对于所有其他实体，如果收到敏感验证数据，需审核程序并检查安全删除数据的流程，以确认这些数据不可恢复。	
3.2.1 切勿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。此类数据也可称为全磁道、磁道、磁道 1、磁道 2 和磁条数据。 ***注：****在正常业务过程中，以下磁条数据元素可能需要保留：* ▪ *持卡人的姓名* ▪ *主帐户 (PAN)* ▪ *失效日* ▪ *业务码* *为将风险降至最低，只存储业务所需的数据元素。*	**3.2.1** 对于系统组件样本，需检查包括但不限于以下方面的数据源，并确认在授权之后并未存储卡片背面磁条上任何磁道的完整内容或芯片上的等效数据： ▪ 输入的交易数据 ▪ 所有日志（例如交易、历史、除错、错误） ▪ 存档文件 ▪ 跟踪文件 ▪ 几种数据库架构 ▪ 数据库内容	如果已存储全磁道数据，恶意个人在获得这些数据后便可借此复制支付卡，完成欺诈性交易。

PCI DSS 要求	测试程序	指南
3.2.2 切勿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）。	**3.2.2** 对于系统组件样本，需检查包括但不限于以下方面的数据源，并确认在授权之后并未存储印在卡片正面或签名栏上的三或四位卡验证代码或值（CVV2、CVC2、CID、CAV2 数据）： ▪ 输入的交易数据 ▪ 所有日志（例如交易、历史、除错、错误） ▪ 存档文件 ▪ 跟踪文件 ▪ 几种数据库架构 ▪ 数据库内容	卡验证代码主要用于保护消费者和卡都不在交易现场的“无实卡”交易 — 互联网或邮件命令/电话命令 (MO/TO) 交易。 如果这些数据被盗，恶意个人便能实施互联网和 MO/TO 欺诈交易。
3.2.3 切勿存储个人识别码 (PIN) 或已加密的 PIN 数据块。	**3.2.3** 对于系统组件样本，需检查包括但不限于以下方面的数据源，并确认在授权之后并未存储 PIN 和已加密的 PIN 数据块： ▪ 输入的交易数据 ▪ 所有日志（例如交易、历史、除错、错误） ▪ 存档文件 ▪ 跟踪文件 ▪ 几种数据库架构 ▪ 数据库内容	仅持卡人或发卡银行可知道这些数值。如果这些数据被盗，恶意个人便能实施基于 PIN 的欺诈性借方交易（例如 ATM 取款）。
3.3 显示 PAN 时予以掩盖（最多显示前六位和后四位数字），这样仅具有正当业务需要者方可看到完整的 PAN。 ***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。*	**3.3.a** 检查关于掩盖 PAN 显示的书面政策和程序，确认： • 已记录需要访问完整 PAN 显示的角色列表，以及每个角色拥有该访问权的正当业务需要 • 显示 PAN 时必须予以掩盖，这样仅具有正当业务需要者方可看到完整的 PAN • 未特别授权可见完整 PAN 的所有其他角色仅可看到被掩盖的 PAN。	在计算机显示屏、支付卡收据、传真或纸质报告等物品上显示完整的 PAN 可能导致此类数据被无授权个人获取并用于欺诈。确保仅对出于正当业务理由需要查看完整 PAN 的人员显示完整的 PAN，可以将未授权人员访问 PAN 数据的风险降到最低。 该要求涉及保护在显示屏、纸质收据、打印材料等上面***显示***的 PAN，切勿与要求 3.4 中在文件、数据库等内***存储***时保护 PAN 的要求相混淆。
	3.3.b 检查系统配置，确认仅向具有书面业务需求的用户/角色显示完整的 PAN，对所有其他请求均掩盖 PAN。	
	3.3.c 检查 PAN 的显示（例如显示在显示屏、纸质收据上），确认在显示持卡人数据时 PAN 被掩盖，且仅有正当业务需要者方可看到完整的 PAN。	

PCI DSS 要求	测试程序	指南
3.4 通过采取下列任一方法使所有位置（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： ▪ 基于强效加密法的单向散列函数（散列必须要有完整的 PAN） ▪ 截词（不能用散列代替 PAN 被截词的部分） ▪ 索引记号与索引簿（索引簿必须安全地存储） ▪ 具有相关密钥管理流程和程序的强效加密法 ***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，则应采取额外控制措施，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。*	**3.4.a** 检查关于 PAN 保护系统的文件记录，包括供应商、系统/流程类型以及加密算法（若适用），确认已通过使用下列任一方法令 PAN 不可读取： ▪ 基于强效加密法的单向散列函数 ▪ 截词 ▪ 索引记号与索引簿（索引簿存储安全） ▪ 具有相关密钥管理流程和程序的强效加密法	存储在主要存储区（数据库或诸如文本文件和电子表格等平面文件）和非主要存储区（备份、检查日志、异常或故障排除日志）的 PAN 均须得到保护。 可采用基于强效加密法的单向散列函数令持卡人数据不可读取。在无需检索原始数字时适于采用散列函数（单向散列不可逆）。在进行散列前，建议（当前并不要求）向持卡人数据另增一个随机输入值，以降低攻击者将这些数据与预先计算的散列值表相比较并从中推算出 PAN 的可能性。 截词的目的在于仅存储部分 PAN（最多前六位和后四位数字）。 索引记号是根据特定索引用一个不可预测的值替代 PAN 的密码符号。一次性索引簿是一个系统，在这个系统中，使用（只可使用一次）随机生成的私人密钥为消息加密，然后使用匹配的一次性索引簿和密钥为消息解密。 强效加密法（请参阅*《PCI DSS 和 PA-DSS 术语、缩略词和首字母缩略词词汇表》*中的定义）的目的是根据经行业测试并认可的算法（非专有或“自行开发”的算法）采用强效加密密钥进行加密 。 通过关联特定 PAN 的散列版和截词版，恶意个人可轻易推算出 PAN 的原始值。防范此类数据相互关联的控制措施有助于确保原始 PAN 始终不可读。
	3.4.b 检查数据储存库样本中的几个表格或文件，确认 PAN 不可读（即，未以纯文本形式存储）。	
	3.4.c 检查可移动媒介（例如备份磁带）样本，确认 PAN 不可读。	
	3.4.d 审查检查日志样本，确认 PAN 不可读或已从日志中删除。	
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）。解密密匙决不能与用户帐户关联。	**3.4.1.a** 如果采用磁盘加密，需检查配置并查看验证过程，确认实现加密文件系统逻辑访问所使用的机制与本地操作系统的验证机制分离（例如不使用本地用户帐户数据库或普通网络登录凭证）。	本要求旨在实现磁盘级加密对于实现持卡人数据不可读的可接受性。磁盘级加密可对计算机上的整个磁盘/分区加密，并在授权用户请求时自动解密信息。许多磁盘加密解决方案会拦截操作系统的读/写操作，并且无需用户执行任何特殊操作便可实施相应的加密转换，而不是在系统启动或会话开始时提供密码或口令。根据磁盘级加密的这些特点，如要
	3.4.1.b 查看流程并与工作人员面谈，确认加密密钥存储安全（例如存储在通过严格访问控制提供充分保护的可移动媒介上）。	

PCI DSS 要求	测试程序	指南
	3.4.1.c 检查配置并查看流程，确认存储在可移动媒介上任何位置的持卡人数据均已加密。 ***注：****如果未使用磁盘加密法对可移动媒介加密，则需通过一些其他方法让存储在该媒介上的数据实现不可读。*	符合本要求，则不能： 1) 使用与操作系统相同的用户帐户验证器，或 2) 使用与系统本地用户帐户数据库或普通网络登录凭证相关联或源于此的解密密钥。 全盘加密有助于在磁盘丢失时保护数据，因此可能适用于存储持卡人数据的便携设备。
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： ***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。*	**3.5** 检查密钥管理政策和程序，确认已针对保护用于为持卡人数据加密以防泄露和滥用的密钥制定专门的流程，这些流程至少应包括以下方面： • 密钥访问权限仅限极少数必需的保管人 • 密钥加密密钥至少要与其保护的数据加密密钥一样强效 • 密钥加密密钥与数据加密密钥单独存储 • 尽量减少密钥安全存储的地方和形式	必须大力保护加密密钥，因为获得密钥访问权者能够解密数据。为确保适当保护为数据加密的密钥和用该密钥加密的数据，密钥加密密钥（如使用）至少须与数据加密密钥一样强效。 本要求旨在防止密钥泄露和滥用，适用于数据加密密钥和密钥加密密钥。由于一个密钥加密密钥可允许访问很多数据加密密钥，所以需要对密钥加密密钥实施强效的保护措施。
3.5.1 仅极少数必需的保管人有密钥访问权限。	**3.5.1** 检查用户访问列表，确认密钥访问权限仅限极少数必需的保管人。	应只有极少数人有权访问密钥（降低非授权方可见持卡人数据的可能性），通常仅限具有密钥保管责任的人员。
3.5.2 始终以下面的一种（或多种）形式存储用于加密/解密持卡人数据的机密密钥和私人密钥： • 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 • 在安全加密设备（例如，主机安全模块 (HSM) 或 PTS 批准的交互点设备）内 • 根据行业认可的方法，采用至少两个全长密钥组分或密钥共享 ***注：****公共密钥不要求以这些形式存储。*	**3.5.2.a** 检查书面程序，确认用于加密/解密持卡人数据的密钥始终以下面的一种（或多种）形式存在。 • 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 • 在安全加密设备（例如，主机安全模块 (HSM) 或 PTS 批准的交互点设备）内 • 根据行业认可的方法，采用多个密钥组分或密钥共享 **3.5.2.b** 检查系统配置和密钥存储位置，确认用于加密/解密持卡人数据的密钥始终以下面的一种（或多种）形式存在。 • 用密钥加密密钥进行加密 • 在安全加密设备（例如，主机安全模块 (HSM) 或 PTS 批准的交互点设备）内 • 根据行业认可的方法，采用多个密钥组分或密钥共享 **3.5.2.c** 无论密钥加密密钥用于何处，均需检查系统配置和密钥存储位置以确认： • 密钥加密密钥至少要与其保护的数据加密密钥一样强效 • 密钥加密密钥与数据加密密钥单独存储。	密钥必须安全存储，以防止非授权或不必要的访问，它们可能会导致持卡人数据的泄露。密钥加密密钥无需加密，但应根据要求 3.5 的规定避免泄露和滥用。若使用密钥加密密钥，在与数据加密密钥有物理和/或逻辑区别的位置存储密钥加密密钥可降低对两种密钥的非授权访问风险。

PCI DSS 要求	测试程序	指南
3.5.3 尽量减少密钥存储的地方。	**3.5.3** 检查密钥存储位置并查看流程，确认已尽量减少密钥存储的地方。	尽量减少密钥存储的地方有助于组织跟踪并监控所有密钥位置，并将非授权方获取密钥的可能性降到最低。
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： ***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.a** 针对服务提供商的附加程序：如果服务提供商与客户共享传输或存储持卡人数据的密钥，则需要检查服务提供商向客户提供的文档记录，以确认已根据下文要求 3.6.1 至 3.6.8 在文档记录中提供了安全传输、存储并更新客户密钥的指南。 **3.6.b** 检查用于持卡人数据加密的密钥管理程序和流程并执行以下操作：	密钥的管理方式是确保加密解决方案持续安全的关键部分。良好的密钥管理流程作为加密产品的一部分，无论是手动或自动均以行业标准为基础并涵盖要求 3.6.1 至 3.6.8 中的所有密钥要素。 指导客户如何安全地传输、存储并更新密钥有助于防止密钥管理不善或泄露给非授权实体。 本要求适用于用来加密所存储持卡人数据的密钥以及任何相关的密钥加密密钥。
3.6.1 生成强效密钥	**3.6.1.a** 确认密钥管理程序详细列明强效密钥的生成方式。 **3.6.1.b** 查看密钥生成方法，确认已生成强效密钥。	必须根据《PCI DSS 和 PA-DSS 术语、缩写词和首字母缩略词词汇表》中“强效加密”的定义，使加密解决方案生成强效密钥。使用强效密钥可显著提高已加密持卡人数据的安全级别。
3.6.2 安全的密钥分配	**3.6.2.a** 确认密钥管理程序详细列明如何安全分配密钥。 **3.6.2.b** 查看密钥的分配方法，确认密钥已安全分配。	加密解决方案必须对密钥进行安全分配，这表示密钥只会以掩盖的方式分配给要求 3.5.1 中指定的保管人。
3.6.3 安全的密钥存储	**3.6.3.a** 确认密钥管理程序详细列明如何安全存储密钥。 **3.6.3.b** 查看密钥存储方法，确认密钥已安全存储。	加密解决方案必须对密钥进行安全存储，例如，使用密钥加密密钥对其进行加密。密钥存储未得到适当保护时会为攻击者提供访问通道，进而导致解密并暴露持卡人数据。
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。	**3.6.4.a** 确认密钥管理程序包含使用中的每种密钥的指定密钥周期并定义密钥在指定密钥周期结束时的变更流程。 **3.6.4.b** 与工作人员面谈，确认已在指定密钥周期结束时更改密钥。	密钥周期是指特定密钥用于指定目的的时间段。定义密钥周期要考虑的因素包括但不限于基础算法的强度、密钥的大小或长度、密钥遭受威胁的风险以及被加密数据的敏感性。 加密密钥必须在加密周期结束后定期更改，这样可将他人获取加密密钥并用其解密数据的风险降到最低。
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。	**3.6.5.a** 确认密钥管理程序详细列明以下各方面的流程： • 当密钥的完整性减弱时，注销或替换密钥。 • 替换确定或怀疑受到威胁的密钥。 • 注销或替换后保留的任何密钥均不用于加密。	不再使用或需要的密钥或者确定或怀疑受到威胁的密钥应予以撤销和/或销毁，以确保不再使用。若需要保留这种密钥（例如，用来支持已存档的加密数据），则应为其提供强效保护。

PCI DSS 要求	测试程序	指南
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。*	**3.6.5.b** 与工作人员面谈，确认已实施以下流程： • 密钥的完整性变弱时（包括知道密钥的人离职时），根据需要注销或替换密钥。 • 确定或怀疑密钥受到威胁时替换密钥。 • 注销或替换后保留的任何密钥均不用于加密。	加密解决方案应规定并简化已到期或者确定或怀疑受到威胁的密钥的替换流程。
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。 ***注：****手动密钥管理操作包括但不限于：密钥生成、传输、加载、存储和销毁。*	**3.6.6.a** 确认手动明文密钥管理程序详细列明使用以下管理方法的流程： • 密钥的分割知识，即密钥的组成部分至少由两个人控制，每个人只知道自己那部分的密钥，以及 • 密钥的双重控制，即至少需要两个人执行密钥管理操作且他们无法访问对方的验证材料（例如，密码或密钥）。	密钥的分割知识和双重控制确保没人知道完整的密钥。此控制适用于手动密钥管理操作或加密产品未实施密钥管理的情况。 分割知识是由两个或更多人分别掌握部分密钥的方法；每个人只知道自己的密钥部分，且根据单个密钥部分无法得知整个密钥）。 双重控制需要两个或更多的人共同完成且他们无法访问或使用对方的验证材料。
	3.6.6 b 与工作人员面谈和/或查看流程，确认使用以下方法管理手动明文密钥： • 分割知识和 • 双重控制	
3.6.7 防止密钥的非授权替换。	**3.6.7.a** 确认密钥管理程序详细列明防止对密钥进行非授权替换的流程。	加密解决方案不允许或接受来自非授权来源或意外流程的密钥替换。
	3.6.7.b 与工作人员面谈和/或查看流程，确认已防止密钥的非授权替换。	
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。	**3.6.8.a** 确认密钥管理程序详细列明密钥保管人确认（以书面或电子形式）理解并接受密钥保管责任的流程。	该流程有助于确保密钥保管人承诺担任该角色并且理解和接受其责任。
	3.6.8.b 查看表明密钥保管人已确认（以书面或电子形式）理解并接受密钥保管责任的文档记录或其他证据。	
3.7 确保已记录、正在使用且所有相关方了解用于保护所存储持卡人数据的安全政策和操作程序。	**3.7** 检查文档记录并与工作人员面谈，确认用于保护所存储持卡人数据的安全政策和操作程序均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守用于持续管理持卡人数据安全存储的安全政策和书面操作程序。

要求 4：　　加密持卡人数据在开放式公共网络中的传输

在恶意个人可轻松访问的网络中传输敏感信息时必须进行加密。错误配置的无线网络和旧版加密及验证协议中的漏洞仍然是恶意个人攻击的目标，他们利用这些漏洞来获取持卡人数据环境的访问特权。

PCI DSS 要求	测试程序	指南
4.1 使用强效加密法和安全协议（例如，SSL/TLS、IPSEC、SSH 等） 来保护在开放式公共网络中传输的敏感持卡人数据，包括： • 只接受可信的密钥和证书 • 使用的协议只支持安全的版本或配置 • 加密强度适合所使用的加密方法 *开放式公共网络包括但不限于：* ▪ 互联网 ▪ 无线技术，包括 802.11 和蓝牙 ▪ 蜂窝技术，例如，全球移动通信系统 (GSM)、码分多址 (CDMA) ▪ 通用分组无线业务 (GPRS)。 ▪ 卫星通信	**4.1** 识别通过开放式公共网络传输或接收的持卡人数据的所有位置，检查书面标准并与系统配置对比，确认在所有位置均已使用安全协议和强效加密法。	在公共网络中传输的敏感信息必须予以加密，这是因为恶意个人通常会在数据传输过程中轻松拦截和/或转移数据。 要实现持卡人数据的安全传输需使用可信密钥/证书、安全传输协议以及用于持卡人数据加密的合适加密强度。对于不支持所需加密强度以及会导致非安全连接的系统发出的连接请求不予以接受。 注意：有些协议的实施（例如 SSL v2.0、SSH v1.0 和 TLS 1.0）存在攻击者可用于控制相关系统的已知漏洞。无论使用哪项安全协议，均需确保将其配置为仅使用安全的版本和配置，从而防止使用非安全连接。例如，可以考虑从公认的公共证书授权中心获取仅支持强效加密的 TLS 1.1 版证书或更高版本。 确认证书可信（例如，未过期且由可信来源发布）有助于确保安全连接的完整性。
	4.1.a 审查书面政策和程序，确认已详细列明以下方面的流程： • 只接受可信密钥和/或证书。 • 所使用的协议仅支持安全的版本和配置（不支持非安全版本和配置）。 • 根据所使用的加密方法实施适当的加密强度	
	4.1.b 在出现入站和出站传输时选择并查看其样本部分，以确认所有持卡人数据均在传输时使用强效加密法加密。	
	4.1.c 检查密钥和证书，确认仅接受可信密钥和/或证书。	
	4.1.d 检查系统配置，确认实施的协议仅使用安全的配置且不支持非安全版本或配置。	
	4.1.e 检查系统配置，确认已针对所使用的加密方法采用合适的加密强度。（核对供应商建议/最优方法。）	
	4.1.f 对于 SSL/TLS 的实施：检查系统配置，确认传输或接收持卡人数据时始终启用 SSL/TLS。 例如，对于基于浏览器的实施： ▪ HTTPS 作为浏览器统一记录定位器 (URL) 协议，且 ▪ 仅当 HTTPS 作为 URL 的一部分时才需要持卡人数据。	通常，网页 URL 应以“https”开始和/或 web 浏览器会在其窗口的某个位置显示挂锁图标。很多 SSL 证书供应商还会提供高度可见的验证标记（有时称为“安全标记”、“安全站点标记”或“安全信任标记”），并且可能提供点击标记后即显示网站信息的功能。

PCI DSS 要求	测试程序	指南
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（例如，IEEE 802.11i），以对验证和传输实施强效加密。 ***注：****禁止将 WEP 用作安全控制。*	**4.1.1** 识别传输持卡人数据或连接到持卡人数据环境的所有无线网络。检查书面标准并与系统配置设置对比，确认找到所有无线网络的以下内容： • 使用行业最优方法（例如，IEEE 802.11i）以对验证和传输实施强效加密。 • 弱加密（例如，WEP、SSL 2.0 版或之前版本）未用作验证或传输的安全控制。	恶意用户使用可轻松获取的免费工具来窃听无线通信。使用强效加密法可限制无线网络中敏感信息的泄漏。 对于持卡人数据的验证和传输，必须使用强效加密法来防止恶意用户访问无线网络或利用无线网络访问其他内部网络或数据。
4.2 不要使用终端用户通讯技术（例如，电子邮件、即时通讯、聊天等）来传送不受保护的 PAN。	**4.2.a** 如果使用终端用户通讯技术来发送持卡人数据，则应查看发送 PAN 的流程，并在出现出站传输时抽样查看，确认只要通过终端用户通讯技术传送，PAN 便不可读或受强效加密保护。	电子邮件、即时通讯和聊天在内部和公共网络中传送时，可通过包嗅探轻松拦截。除非这些通讯工具配置后可提供强效加密，否则勿用其传送 PAN。
	4.2.b 审查书面政策，确认已有不会通过终端用户通讯技术传送不受保护的 PAN 方面的政策规定。	
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。	**4.3** 检查文档记录并与工作人员面谈，确认用于加密持卡人数据传输的安全政策和操作程序均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守用于持续管理持卡人数据安全传输的安全政策和操作程序。

维护漏洞管理计划

要求 5：　　为所有系统提供恶意软件防护并定期更新杀毒软件或程序

恶意的软件通常称为“恶意软件”（包括病毒、蠕虫病毒和特洛伊木马），可在很多业务许可活动（包括员工电子邮件以及互联网、移动计算机和存储设备的使用）中进入网络，从而利用系统漏洞。经常受恶意软件影响的所有系统均必须使用杀毒软件，以避免系统经受当前和不断进化的恶意软件的威胁。除杀毒软件以外，也可以考虑其他反恶意软件解决方案；但此类反恶意软件解决方案无法代替杀毒软件。

PCI DSS 要求	测试程序	指南
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。	**5.1** 对于系统组件样本（包括经常受恶意软件影响的所有操作系统类型），确认如果存在适用的杀毒技术则部署杀毒软件。	目前存在利用广泛发布的威胁持续攻击其他安全系统的情况，通常称为“零日漏洞攻击”（利用之前未知的漏洞进行的攻击）。如果没有定期更新的杀毒解决方案，这些新型恶意软件便会攻击系统、禁用网络或威胁数据。
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。	**5.1.1** 审查供应商文档记录并检查杀毒配置，确认杀毒程序能： • 检测所有已知类型的恶意软件， • 删除所有已知类型的恶意软件，并 • 阻止所有已知类型的恶意软件 *恶意软件类型包括病毒、特洛伊木马、蠕虫病毒、间谍软件、广告软件和 rootkit 内核型病毒。*	阻止**所有**类型和形式的恶意软件很重要。
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	**5.1.2.b** 与工作人员面谈，确认已针对目前认为通常不受恶意软件影响的系统，监控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。	通常，主机、中端电脑（例如 AS/400）和类似系统目前不是恶意软件攻击的目标或不受其影响。然而，恶意软件的行业趋势变化迅速，因此组织需要了解会影响其系统的新的恶意软件，例如，通过密切关注供应商安全公告和杀毒新闻组，确定其系统是否会受到不断进化的新恶意软件的威胁。 恶意软件的发展趋势应包含在新安全漏洞的识别流程中，而处理新趋势的方法应根据需要并入公司的配置标准和保护机制中

PCI DSS 要求	测试程序	指南
5.2 确保所有杀毒机制按如下方式维护： • 保持为最新， • 执行定期扫描 • 生成检查日志（PCI DSS 要求 10.7 规定保留）	**5.2.a** 检查政策和程序，确认已规定杀毒软件和相关定义需要保持为最新。	如果不用最新的安全更新、签名文件或恶意软件防护进行维护并保持为最新，则即使是最佳杀毒解决方案的效力也会受限。 检查日志可监控病毒和恶意软件活动以及反恶意软件的效果。因此，反恶意软件解决方案必须配置为可生成检查日志且这些日志必须根据要求 10 进行管理。
	5.2.b 检查杀毒配置（包括软件的主体安装），确认杀毒机制： • 配置为执行自动更新，且 • 配置为执行定期扫描	
	5.2.c 检查系统组件样本（包括经常受恶意软件影响的所有操作系统类型），确认： • 杀毒软件和相关定义为最新 • 已执行定期扫描	
	5.2.d 检查杀毒配置（包括软件的主体安装和系统组件的样本部分），确认： • 已启用杀毒软件日志生成功能，且 • 日志根据 PCI DSS 要求 10.7 进行保留	
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。 ***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。若出于特定目的需要禁用杀毒软件保护，必须获得正式授权。杀毒软件保护禁用期间，需要实施其他安全措施。*	**5.3.a** 检查杀毒配置（包括软件的主体安装和系统组件的样本部分），确认杀毒软件正在积极运行	持续运行且无法更改的杀毒软件可提供持久的恶意软件防护。 根据政策对所有系统实施控制，可确保反恶意软件保护无法更改或禁用，从而防止系统漏洞被恶意软件利用。 病毒防护禁用期间，需要实施其他安全措施，例如，在禁用杀毒保护时断开不受保护的系统与互联网间的连接并在重新启用 AV 后运行全盘扫描。
	5.3.b 检查杀毒配置（包括软件的主体安装和系统组件的样本部分），确认用户无法禁用或更改杀毒软件。	
	5.3.c 与负责人员面谈并查看流程，确认除非管理人员根据具体情况做出有时间限制的明确授权，否则用户无法禁用或更改杀毒软件。	
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。	**5.4** 检查文档记录并与工作人员面谈，确认为系统提供恶意软件防护的安全政策和操作程序均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守安全政策和操作程序，确保始终为系统提供恶意软件防护

要求 6：　　开发并维护安全的系统和应用程序

恶意个人会利用安全漏洞获得系统访问特权。很多此类漏洞可通过供应商提供的安全补丁修复，而负责管理系统的实体必须安装这些补丁。所有系统均须具备所有适当的软件补丁，以防恶意个人和恶意软件利用、破坏持卡人数据。

注：*适当的软件补丁指已通过充分评估和测试确定不会与现有安全配置相冲突的补丁。对于内部开发的应用程序，很多漏洞均可通过采用标准系统开发流程和安全编码技术加以避免。*

PCI DSS 要求	测试程序	指南
6.1 制定相关流程，通过使用外部信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”）。 ***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。* . *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。*	**6.1.a** 检查政策和程序，确认已规定以下流程： • 识别新的安全漏洞。 • 为漏洞指定风险等级，包括识别所有“高”风险和“重要”漏洞。 • 使用外部信源获取安全漏洞信息。 **6.1.b** 与负责人员面谈并查看流程，确认： • 已识别新的安全漏洞。 • 已为漏洞指定风险等级，包括对所有“高”风险和“重要”漏洞的识别。 • 用于识别新安全漏洞的流程包含使用可信外源获取安全漏洞信息。	本要求旨在让组织能及时更新可能影响其环境的新漏洞。 漏洞信息来源应当可信，并且通常包含供应商网址、行业新闻组、邮件列表或 RSS 反馈。 当组织发现可能影响其环境的漏洞后，必须评估该漏洞产生的风险并确定风险等级。因此，组织必须有适当的方法可对漏洞进行持续评估并为这些漏洞指定风险等级。这并非通过一次 ASV 扫描或内部漏洞扫描就能实现，而是需要制定积极监控漏洞信息行业来源的流程。 组织能够通过风险分类（例如“高”、“中”或“低”）更快地识别和优先解决风险最高的项目，降低风险最大的漏洞被利用的可能性。
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。 ***注：****应按照要求 6.1 中规定的风险分级流*	**6.2.a** 检查与安全补丁安装相关的政策和程序，确认已规定以下流程： • 在发布后一个月内安装供应商提供的适用关键安全补丁。 • 在适当的时间范围内（例如三个月内）安装供应商提供的所有适用安全补丁。	目前存在利用广泛发布的威胁持续攻击其他安全系统的情况，通常称为“零日漏洞攻击”（利用之前未知的漏洞进行的攻击）。如未尽快在关键系统上应用最新补丁，恶意个人便可能利用这些漏洞攻击或禁用系统，或获得敏感数据的访问权限。

PCI DSS 要求	测试程序	指南
程标识关键安全补丁。	**6.2.b** 对于系统组件和相关软件样本，对照各系统上已安装的安全补丁列表与最新的供应商安全补丁列表，确认： • 供应商提供的适用关键安全补丁已在发布后一个月内安装。 • 供应商提供的所有适用安全补丁已在适当的时间范围内（例如三个月内）安装。	为关键基础架构确定补丁优先次序可确保高优先级系统和设备在补丁发布后尽快得到漏洞防护。考虑确定补丁安装的优先次序，以便关键系统或高危系统的安全补丁能在 30 天内安装，其他风险较低的补丁在 2-3 个月内安装。 本要求适用于所有已安装软件的适用补丁。
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）： • 按照 PCI DSS（例如安全验证和记录） • 基于行业标准和/或最优方法。 • 将信息安全纳入软件开发的整个生命周期。 ***注：****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*	**6.3.a** 检查书面软件开发流程，确认这些流程以行业标准和/或最优方法为基础。 **6.3.b** 检查书面软件开发流程，确认信息安全已纳入软件开发的整个生命周期。 **6.3.c** 检查书面软件开发流程，确认软件应用程序的开发符合 PCI DSS。 **6.3.d** 与软件开发人员面谈，确认已实施书面软件开发流程。	如果未在软件开发的要求定义、设计、分析和测试阶段纳入安全考虑，安全漏洞则会被无意或恶意地带入生产环境。 理解应用程序处理敏感数据的方式，包括何时存储、何时传输、何时在内存中，有助于确定哪里的数据需要受到保护。
6.3.1 在应用程序启动前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	**6.3.1** 检查书面软件开发程序并与负责人员面谈，确认在应用程序投入生产前或向客户发布前已删除预生产和/或自定义应用程序帐户、用户 ID 和/或密码。	在应用程序启动前或向客户发布前，应自生产代码中删除开发、测试和/或自定义应用程序帐户、用户 ID 和密码，因为这些项目可能泄露有关该应用程序功能的信息。持有这类信息会让应用程序和相关持卡人数据更易遭受威胁。
6.3.2 为识别任何潜在的编码漏洞（采用人工或自动流程），在发布到产品前或向客户发布前检查自定义代码时至少应包括以下方面： ▪ 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。 ▪ 代码审核可确保代码的开发符合安全编码指南 ▪ 发布前已进行适当修正。 ▪ 代码审查结果在发布前已由管理人	**6.3.2.a** 检查书面软件开发程序并与负责人员面谈，确认所有自定义应用程序代码变更均必须按照以下要求进行审核（采用人工或自动流程）： ▪ 代码变更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进行审核。 ▪ 代码审核可确保代码的开发符合安全编码指南（请参阅 PCI DSS 要求 6.5）。 ▪ 发布前已进行适当修正。 ▪ 代码审查结果在发布前已由管理人员审核并批准。	恶意个人经常利用自定义代码中的安全漏洞获取网络访问权限并威胁持卡人数据。 审核流程应有一名熟悉代码审核方法并具备相关经验的人员参与。为确保进行独立客观的审核，代码审核应由代码开发人员以外的人员执行。也可采用自动化工具或流程代替人工审核，但要记住，自动化工具可能难以甚至不可能发现某些编码问题。 在将代码部署到生产环境或发布给客户之前修正编码错误可避免代码暴露在可能被利用的环境下。另外，在部署或发布到生产环境后处理错误

PCI DSS 要求	测试程序	指南
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。* *代码审核可由熟悉这方面工作的内部人员或第三方负责。Web 应用程序如果面向公众，也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，具体规定请参阅 PCI DSS 要求 6.6。*	**6.3.2.b** 选择最近的一批自定义应用程序更改样本，确认已根据上述要求 6.3.2.a 审核自定义应用程序代码。	代码的难度会更大，花费也更高。 管理人员在发布前进行正式审核并签字有助于确保代码通过审批，并已按政策与程序进行开发。
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：	**6.4** 检查政策和程序，确认已规定下列内容： • 开发/测试环境独立于生产环境，并设置访问控制，确保两者的分离 • 对分配到开发/测试环境与生产环境中的人员的职责进行分离 • 在测试或开发过程中不使用生产数据（真实的 PAN） • 在生产系统启动前，已经删除测试数据与帐户 • 有关应用安全补丁和软件修改的变更控制程序已用文档记录。	如果没有适当记录和实施的变更控制措施，安全属性则可能被无意或有意忽略或者被设定为不可操作，而且可能发生违规处理情形或引入恶意代码。
6.4.1 开发/测试环境独立于生产环境，并设置访问控制，确保两者分离	**6.4.1.a** 检查网络文档记录和网络设备配置，确认开发/测试环境独立于生产环境。	由于开发和测试环境会不断变化，所以其安全性往往低于生产环境。如果环境之间没有充分分离，则生产环境和持卡人数据可能会因测试或开发环境中不够严格的安全配置和可能存在的漏洞而受到威胁。
	6.4.1.b 检查访问控制设置，确认已实施访问控制来确保开发/测试环境与生产环境已分离。	
6.4.2 开发/测试环境与生产环境中的职责分离	**6.4.2** 查看流程，并与分配到开发/测试环境的人员和分配到生产环境的人员面谈，确认开发/测试环境与生产环境之间已实现职责分离。	减少有权访问生产环境和持卡人数据的人数可最大限度地降低风险，有助于确保访问权仅限于有业务知情需要的个人。 本要求旨在确保开发和测试职能与生产职能相分离。例如，开发人员可使用在开发环境中享有较高特权的管理员级帐户，并同时拥有可对生产环境进行用户级访问的独立帐户。
6.4.3 在测试或开发过程中不使用生产数据（真实的 PAN）	**6.4.3.a** 查看测试流程，并与工作人员面谈，确认现已实施相关程序，确保在测试或开发过程中不使用生产数据（真实的 PAN）。	测试或开发环境中的安全控制措施通常不够严格。使用生产数据会为恶意个人提供非法访问生产数据（持卡人数据）的机会。
	6.4.3.b 检查一批测试数据样本，确认测试或开发过程中未使用生产数据（真实的 PAN）。	
6.4.4 在生产系统启动前，删除测试数据与帐户	**6.4.4.a** 查看测试流程，并与工作人员面谈，确认在生产系统启动前已删除测试数据和帐户。	在应用程序启动前，应自生产代码中删除测试数据和帐户，因为这些项目可能会泄露有关该应用程序或系统功能的信息。持有这类信息会让系统

PCI DSS 要求	测试程序	指南
	6.4.4.b 检查一批来自最近安装或更新的生产系统的数据和帐户样本，确认在系统启动前已删除测试数据和帐户。	和相关持卡人数据更易遭受威胁。
6.4.5 应用安全补丁和软件修改的变更控制程序必须包括以下方面：	**6.4.5.a** 检查有关应用安全补丁和软件修改的书面变更控制程序，确认已规定以下方面的程序： • 影响记录 • 被授权方的变更审批记录 • 功能测试，以确认该变更未对系统安全造成不利影响 • 取消程序	如果管理不当，软件升级和安全补丁的效果可能得不到完全实现，并且可能造成无法预料的后果。
	6.4.5.b 对于系统组件样本，与负责人员面谈以确定最新的变更/安全补丁，并根据这些变更追溯到相关的变更控制记录。每次检查变更时，执行下列步骤：	
6.4.5.1 影响记录。	**6.4.5.1** 确认每次抽取的变更样本的变更控制文档记录已包含影响记录。	应记录变更影响，以便所有相关方能针对任何处理中的变更制定相应计划。
6.4.5.2 被授权方的变更审批记录。	**6.4.5.2** 确认每次抽取的变更样本都有被授权方的审批记录。	获被授权方批准表明该变更是组织认可的经批准的合法变更。
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。	**6.4.5.3.a** 对于每次抽取的变更样本，确认已执行功能测试，以证实该变更未对系统安全性造成不利影响。	通过执行全面的测试，确认环境的安全性未因实施变更而降低。应通过测试确认在环境发生任何变更后，所有现行安全控制措施仍然有效、为同样有力的控制措施取代或得到加强。
	6.4.5.3.b 对于自定义代码变更，确认在将其部署到生产环境前，所有更新均经过测试符合 PCI DSS 要求 6.5。	
6.4.5.4 取消程序。	**6.4.5.4** 确认每次抽取的变更样本都有取消程序。	每次变更都应有取消程序的书面记录，如果变更失败或对某个应用程序或系统的安全产生不利影响，即可将系统恢复到之前的状态。
6.5 按照以下操作解决软件开发流程中常见的编码漏洞： • 为开发人员提供关于安全编码技术的培训，包括如何避免常见的编码漏洞，并理解敏感数据在内存中的处理方式。 • 根据安全编码指南开发应用程序 ***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*	**6.5.a** 检查软件开发政策与程序，确认已要求开发人员必须参加安全编码技术培训，且培训以行业最优方法和指南为基础。	应用层是高风险层，可能成为内部和外部威胁的目标。 要求 6.5.1 至 6.5.10 属于应具备的最低控制要求，组织还应纳入其环境中特定技术适用的相关安全编码实践。 应用程序开发人员应经过适当培训，从而识别并解决与这些（及其他）常见编码漏洞相关的问题。拥有熟悉安全编码指南的员工能够最大限度地减少通过拙劣编码实践引入的安全漏洞数量。
	6.5.b 抽取部分开发人员进行面谈，确认他们熟悉安全编码技术。	
	6.5.c 检查培训记录，确认软件开发人员已接受关于安全编码技术的培训，包括如何避免常见的编码漏洞，并理解敏感数据在内存中的处理方式。	

PCI DSS 要求	测试程序	指南
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。	**6.5.d.** 确认已具备相应流程，可确保应用程序至少在以下方面没有漏洞：	对开发人员的培训可由内部或第三方提供，且应适用于所采用的技术。 当行业认可的安全编码实践改变时，组织的编码实践和开发人员的培训也应相应更新，以防范新的威胁，例如内存残留数据攻击。 要求 6.5.1 至 6.5.10 所指出的漏洞提供了最低的底线。组织有责任跟上最新的漏洞发展趋势，并在安全编码实践当中纳入适当的措施。
	***注：** 下文的要求 6.5.1 至要求 6.5.6 适用于所有应用程序（内部或外部）。*	
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。	**6.5.1** 检查软件开发政策与程序，并与负责人员面谈，以确认注入攻击可通过以下编码技术解决： • 验证输入，以确认用户数据无法修改命令和查询的意思 • 利用参数化查询	注入攻击，特别是 SQL 注入，是破坏应用程序的一种常用方法。当用户提供的数据作为命令或查询的一部分被发送到解释器时，就发生了注入。攻击者的恶意数据会诱导解释器执行非计划的命令或修改数据，并允许攻击者通过应用程序攻击网络内的组件，以发起攻击（例如缓冲区溢出），或泄露机密信息和服务器应用程序的功能。 信息在发送到应用程序前应经过验证 — 例如通过检查所有字母字符、字母与数字混合字符等。
6.5.2 缓冲区溢出	**6.5.2** 检查软件开发政策与程序，并与负责人员面谈，以确认缓冲区溢出可通过以下编码技术解决： • 验证缓冲区边界 • 截取输入字符串	当应用程序在其缓冲区空间上没有适当的检查范围时，则发生缓冲区溢出。这可能造成缓冲区内的信息被挤出缓冲区存储空间，而进入可执行的存储空间。当发生这种情形时，攻击者能在缓冲区的末端插入恶意代码，并通过促使缓冲区溢出将该恶意代码推入可执行的存储空间。随后，攻击者将执行该恶意代码并经常借机远程访问该应用程序和/或被感染的系统。
6.5.3 非安全加密存储	**6.5.3** 检查软件开发政策与程序，并与负责人员面谈，以确认非安全加密存储可通过以下编码技术解决： • 防止密码攻击 • 采用强效加密算法和密钥	未适当利用强效加密功能存储数据的应用程序受到威胁、泄露验证凭证和/或持卡人数据的风险会增大。如果攻击者能够利用薄弱的加密流程，他们便能获得加密数据的明文访问权限。
6.5.4 非安全通信	**6.5.4** 检查软件开发政策与程序，并与负责人员面谈，以确认非安全通信可通过正确验证和加密所有敏感通信的编码技术来解决	未采用强效加密法对网络流量进行充分加密的应用程序受到威胁和泄露持卡人数据的风险会增加。如果攻击者能利用薄弱的加密流程，他们或许便能控制应用程序，甚至获得加密数据的明文访问权限。

PCI DSS 要求	测试程序	指南
6.5.5 不正确的错误处理	**6.5.5** 检查软件开发政策与程序，并与负责人员面谈，以确认不正确的错误处理可采用不会通过错误消息泄露信息的编码技术解决（例如通过返回一般而非具体的错误详情）	应用程序可能会无意中泄露关于其配置和内部工作方式的信息，或通过不正确的错误处理方法泄露专用信息。攻击者会利用这一漏洞窃取敏感数据，或破坏整个系统。如果恶意个人能够创建应用程序未正确处理的错误，他们便能获得详细的系统信息、创建拒绝服务中断、引起安全故障，或导致服务器崩溃。例如，“提供的密码不正确”这一消息就在告诉攻击者其提供的用户 ID 是正确的，他们应该只关注攻击密码。使用较通用的错误消息，例如“数据无法验证”。
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）。	**6.5.6** 检查软件开发政策与程序，并与负责人员面谈，以确认编码技术可解决任何可能影响应用程序的“高风险”漏洞，具体规定请参阅 PCI DSS 要求 6.1。	所有通过组织漏洞风险分级流程（具体规定请参阅要求 6.1）确定为“高风险”的漏洞以及可能影响应用程序的漏洞均应在应用程序开发期间找到并解决。
***注：** 下文的要求 6.5.7 至要求 6.5.10 适用于 web 应用程序和应用程序接口（内部或外部）：*		面向内部和外部（公众）的 Web 应用程序因其架构特性具有独特的安全风险，较易受到威胁。
6.5.7 跨站点脚本 (XSS)	**6.5.7** 检查软件开发政策与程序，并与负责人员面谈，以确认跨站点脚本 (XSS) 可通过以下编码技术解决： • 所有参数在应用前均进行验证 • 利用上下文相关的转义	只要应用程序接收用户提供的数据并在未首先验证或编译内容的情况下将其发送到一个 web 浏览器，则发生 XSS 攻击。攻击者可通过 XSS 在受害人的浏览器中执行脚本，从而劫持用户会话、破坏网站外观，并可能引入蠕虫等。
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 URL 访问、目录遍历和未能限制用户的功能访问）	**6.5.8** 检查软件开发政策与程序，并与负责人员面谈，以确认不正确的访问控制（例如不安全的直接对象引用、未能限制 URL 访问和目录遍历）可通过以下编码技术解决： • 正确的用户验证 • 净化输入 • 不向用户暴露内部对象引用。 • 用户界面不允许访问未授权的功能	当开发人员将引用作为 URL 或形式参数暴露给内部执行对象（例如文件、目录、数据库记录或密钥）时，则发生直接对象引用。攻击者可利用这些引用在未授权的情况下访问其他对象。 始终对所有 URL 执行表示层和业务逻辑的访问控制。通常，应用程序保护敏感功能的唯一方式是防止向未授权用户显示链接或 URL。攻击者可利用这一漏洞，通过直接访问此类 URL 来访问和执行未授权的操作。 攻击者或许能列举并导航一个网站的目录结构（目录遍历），从而获得未授权信息的访问权限并进一步洞悉网站的运行方式，以供以后利用。 如果用户界面允许访问未授权的功能，则该访问可能导致未经授权的个人获得专用凭证或持卡人数据的访问权限。仅允许授权用户获取对敏感资源的直接对象引用。限制数据资源的访问权限有

PCI DSS 要求	测试程序	指南
		助于防止向未授权资源显示持卡人数据
6.5.9 跨站点请求伪造 (CSRF)	**6.5.9** 检查软件开发政策与程序，并与负责人员面谈，以确认跨站点请求伪造 (CSRF) 可通过确保应用程序不信任由浏览器自动提交的授权凭证和令牌的编码技术来解决。	CSRF 攻击会迫使已登录的受害者浏览器向一个存在漏洞的 web 应用程序发送预先验证的请求，随后攻击者便能执行受害人获准执行的任何状态变更操作（例如更新帐户明细、买入，甚至验证该应用程序）。
6.5.10 失效的验证与会话管理 ***注：****要求 6.5.10 在 2015 年 6 月 30 日前属于最优方法，此后将成为一项要求。*	**6.5.10** 检查软件开发政策与程序，并与负责人员面谈，以确认失效的验证与会话管理可通过一系列编码技术解决，通常包括： • 将会话令牌（如 cookie）标记为“安全” • 不要暴露 URL 中的会话 ID • 成功登录后采用适当超时和轮换会话 ID	安全验证和会话管理可防止未授权个人破坏合法的帐户凭证、密钥或会话令牌，如若不然，入侵者可能会占用授权用户的身份。
6.6 对于面向公众的 web 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： ▪ 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 web 应用程序，至少每年一次或在有任何变更后进行 ***注：****该评估与要求 11.2 中执行的漏洞扫描不同* ▪ 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。	**6.6** 对于*面向公众的* web 应用程序，确保已采用下面两种方法之一： ▪ 检查流程文档记录、与工作人员面谈并检查应用程序安全评估记录，确认面向公众的 web 应用程序已按以下方式审核（采用手动或自动漏洞安全评估工具或方法）： - 至少每年执行一次 - 在任意变更之后 - 由专注于应用程序安全的组织进行 - 至少要求 6.5 中的所有漏洞均包含在评估中 - 所有漏洞均已修复 - 修复漏洞后重新评估应用程序 ▪ 检查系统配置设置并与负责人员面谈，确认已按如下方式采用可检查并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）： - 位于面向公众的 web 应用程序之前，用以检查并防范网页式攻击。 - 积极运行且为最新（若适用） - 可生成检查日志 - 配置为阻止网页式攻击，或生成警报	面向公众的 web 应用程序是攻击者的主要目标，而编码不良的 web 应用程序使攻击者能轻松访问敏感数据和系统。要求审核应用程序或安装 web 应用程序防火墙的目的在于减少不良编码或应用程序管理实践对面向公众的 web 应用程序造成的威胁数量。 ▪ 手动或自动漏洞安全评估工具或方法可用于审核和/或测试应用程序中的漏洞 ▪ Web 应用程序防火墙可过滤并阻止应用层的非关键流量。正确配置的 web 应用程序防火墙与基于网络的防火墙配合使用，可防止应用程序编码不当或配置不当时的应用层攻击。 ***注：****“专注于应用程序安全的组织”可以是第三方公司或是内部组织，只要审核者专注于应用程序安全并表现出不依赖开发团队的独立工作能力即可。*

PCI DSS 要求	测试程序	指南
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。	**6.7** 检查文档记录并与工作人员面谈，确认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均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守安全政策和操作程序，始终确保系统和应用程序的安全开发和漏洞防护。

实施强效访问控制措施

要求 7： 按业务知情需要限制对持卡人数据的访问

为确保仅被授权人员能访问关键数据，必须根据知情需要和工作职责，通过适当的系统和流程来限制访问。

“知情需要”只授权访问执行工作所需的最低限度的数据量和权限。

PCI DSS 要求	测试程序	指南
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.a** 检查访问控制的书面政策，并确认其中包含下面的 7.1.1 至 7.1.4： • 为每个角色定义访问需要和权限分配 • 将特权用户 ID 的访问权限限制为执行工作所需的最小权限， • 基于个人的工作分类和职能分配访问权限 • 被授权方对所有访问的审批记录（电子或书面形式），包括获批的特定权限列表	访问持卡人数据的人越多，用户帐户遭受恶意使用的风险便越高。只为具有合理业务理由的人提供访问权限有助于组织避免因经验不足或恶意企图导致的持卡人数据错误处理。
7.1.1 为每个角色定义访问需要，包括： • 每个角色依据工作职能需要访问的系统组件和数据资源 • 访问资源所需的权限级别（例如，用户、管理员等）	**7.1.1** 选择角色样本，并确认已定义每个角色的访问需要，包括： • 每个角色依据工作职能需要访问的系统组件和数据资源 • 确定每个角色执行工作职能所需的权限	为了保证只允许有需要的个人访问持卡人数据，首先要定义每个角色（例如，系统管理员、呼叫中心人员、店员）的访问需要、每个角色需要访问的系统/设备/数据，以及每个角色有效执行所分配任务所需的权限级别。定义角色和相应的访问需要之后，可为个人授予相应的访问权限。
7.1.2 将特权用户 ID 的访问权限限制为执行工作所需的最小权限。	**7.1.2.a** 与负责分配访问权限的工作人员面谈，确认对特权用户 ID 的访问权限： • 只分配给明确需要此类特权访问的角色 • 限制为执行工作所需的最小权限	分配特权 ID 时，应仅为个人分配执行工作所需的权限（即“最小权限”）。例如，不得为数据库管理员或备份管理员分配与整体系统管理员一样的权限。分配最小权限有助于防止不熟悉应用程序的用户错误

PCI DSS 要求	测试程序	指南
	7.1.2.b 抽样选择具有特权访问权限的用户 ID 并与相关管理人员面谈，确认所分配的权限： • 为其工作职能所需 • 限制为执行工作所需的最小权限。	或无意中变更应用程序配置或更改其安全设置。执行最小权限还能在非授权人员访问用户 ID 时最大限度地缩小损失范围。
7.1.3 基于个人的工作分类和职能分配访问权限。	**7.1.3** 抽样选择用户 ID 并与相关管理人员面谈，确认已基于个人的工作分类和职能分配权限。	为用户角色定义访问需要（根据 PCI DSS 要求 7.1.1）之后，可根据工作分类和职能，使用已创建的角色轻松授予个人访问权限。
7.1.4 要求由指定所需权限的被授权方作出书面批准。	**7.1.4** 抽样选择用户 ID 并对比书面批准文档记录，确认： • 已分配权限具备书面批准文档记录 • 由被授权方进行批准 • 指定的权限与分配给个人的角色匹配	书面批准文档记录（例如以手写或电子形式）可确保有访问权限的人员被管理人员知晓并授权，且其访问为工作职能所需。
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，并且将系统设为“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** 检查系统设置和供应商文档记录，确认访问控制系统如下实施：	如果没有根据用户知情需要限制访问的机制，则可能会在无意中授权用户访问持卡人数据。访问控制系统自动执行限制访问和分配权限的流程。另外，默认的“全部拒绝”设置可以确保除非建立特别授权访问的规则，否则无人能获得访问授权。 ***注：****有些访问控制系统默认设为“全部允许”，因此除非建立特别拒绝访问的规则，否则会允许访问。*
7.2.1 所有系统组件范围	**7.2.1** 确认所有系统组件的访问控制系统均已到位。	
7.2.2 基于工作分类和职能为个人分配权限	**7.2.2** 确认访问控制系统配置为基于工作分类和职能执行个人权限分配。	
7.2.3 默认的“全部拒绝”设置	**7.2.3** 确认访问控制系统具备默认的“全部拒绝”设置。	
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。	**7.3** 检查文档记录并与工作人员面谈，确认用于限制持卡人数据访问的安全政策和操作程序均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守安全政策和操作程序，始终确保访问得以控制并以知情需要和最小权限为依据。

要求 8：识别并验证对系统组件的访问

为有访问权限的每个人分配唯一标识符 (ID)，确保每个人都能对自己的操作负责。实施这种责任制后，由已知被授权用户和流程对关键数据和系统执行操作和跟踪。

密码的有效性主要取决于验证系统的设计和实施，尤其是允许攻击者尝试密码的频率以及在输入点、传输过程和存储中保护用户密码的安全方法。

注：*这些要求适用于所有帐户，包括有管理功能的销售点终端帐户以及用来查看或访问持卡人数据或者访问含持卡人数据系统的所有帐户。还包括供应商和其他第三方（例如，进行支持或维护）使用的帐户。*

但是，要求 8.1.1、8.2、8.5、8.2.3-8.2.5 以及 8.1.6-8.1.8 不适用于销售点终端支付应用程序中的用户帐户，为了促成单笔交易，这些帐户一次只能访问一个卡号（例如出纳帐户）。

PCI DSS 要求	测试程序	指南
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.a** 审核程序并确认其已为下文 8.1.1 至 8.1.8 中的每一项制定流程	通过确保为每位用户分配唯一 ID 而非多位员工共用一个 ID，组织可保持个人对操作负责并维护每个员工的有效审核跟踪。这有助于在出现误用或恶意目的时加快问题的解决和控制。
	8.1.b 通过执行以下操作，确认已实施用户识别管理程序：	
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。	**8.1.1** 与管理人员面谈，确认所有用户均已分配访问系统组件或持卡人数据所需的唯一 ID。	
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。	**8.1.2** 对于特权用户 ID 和普通用户 ID 样本，检查相关授权并查看系统设置，确认每个普通用户 ID 和特权用户 ID 都只通过书面批准指定的权限实施。	为确保授予系统访问权限的用户帐户均为经过验证的有效用户，必须使用强有力的流程来管理用户 ID 和其他验证凭证的所有变更（包括新增、修改或删除）。
8.1.3 立即撤销到期用户的访问权限。	**8.1.3.a** 抽样选择在过去半年中过期的用户并审核当前用户访问权限列表（包括本地和远程访问），确认其 ID 已停用或从访问权限列表中删除。	若离职员工仍能通过用户帐户访问网络，则可能会导致对持卡人数据的不必要或恶意访问。这种访问可能来自前员工或利用旧帐户和/或不用帐户的恶意用户。因此，为了防止对网络的非授权访问，应在员工离职后，及时撤销其用户凭证及其他身份验证方法（越快越好）。
	8.1.3.b 确认所有物理验证方法（例如，智能卡、令牌等） 已退还或停用。	
8.1.4 至少每 90 天删除/禁用一次非活动的用户帐户。	**8.1.4** 查看用户帐户，确认已删除或禁用任何超过 90 天的非活动帐户。	不常用的帐户经常会成为攻击目标，因为用户不太会注意到此类帐户的任何变更（例如：密码的修改）。因此，利用或使用这些帐户来访问持卡人数据会更容易。
8.1.5 对供应商通过远程访问用于访问、支持或维护系统组件的用户 ID 进行如下管理： • 仅在需要的时间段启用并在不用时禁	**8.1.5.a** 与工作人员面谈并查看供应商用来访问、支持或维护系统组件的帐户管理流程，确认供应商用以进行远程访问的帐户： • 在不用时禁用 • 仅在供应商需要时启用，并在不用时禁用	如果为了方便供应商支持您的系统，便允许其随时访问您的网络，这样会增加供应商环境中的用户或恶意个人（他们会找到并使用这个始终可用的外部入口点进入您的网络）进行非授权访问的

PCI DSS 要求	测试程序	指南
用。 • 使用时进行监控。	**8.1.5.b** 与工作人员面谈并查看流程，确认供应商远程访问帐户在使用时被监控。	可能性。仅在所需时限内启用访问，用完后立即禁用，有助于防止滥用这些连接。 监控供应商的访问，可保证供应商仅访问所需的系统，并仅在批准的时限内进行访问。
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。	**8.1.6.a** 对于系统组件样本，检查系统配置设置，确认验证参数设为在不超过 6 次的无效登录尝试后锁定用户帐户。	如果不采用帐户锁定机制，攻击者可通过手动或自动工具（例如，密码破解）不断尝试猜测密码，直到成功猜出密码并访问用户帐户。
	8.1.6.b 针对服务提供商的附加程序：审核内部流程和客户/用户文档记录并查看所实施的流程，确认非消费者用户帐户在不超过 6 次的无效访问尝试后暂时锁定。	
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。	**8.1.7** 对于系统组件样本，检查系统配置设置，确认密码参数设为一旦用户帐户锁定，锁定时间为至少 30 分钟或直到系统管理员重置帐户。	如果帐户因有人不断尝试猜测密码而锁定，对这些已锁定帐户的延时再激活控制可阻止恶意个人不断猜测密码（在帐户重新激活之前，他们必须停止至少 30 分钟）。另外，如果必须申请重新激活，则管理员或技术支持人员可验证重新激活的请求者是否为实际的帐户所有人。
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。	**8.1.8** 对于系统组件样本，检查系统配置设置，确认系统/会话空闲超时功能设为不超过 15 分钟。	如果用户离开正在访问关键系统组件或持卡人数据的计算机，其他人可能会在用户不在时使用该计算机，从而导致非授权的帐户访问和/或误用。 重新认证既可以应用在系统级，以保护在机器上运行的所有会话，也可以应用在应用程序级。
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： • 所知，如密码或口令等 • 所有，如令牌设备或智能卡等 • 个人特征，如生物特征等	**8.2** 要确认已使用唯一 ID 和其他验证方法（例如，密码/口令）验证用户对持卡人数据环境的访问，请执行以下操作： • 检查描述所用验证方法的文档记录。 • 对于使用的每种验证方法和每种系统组件，查看验证以确认其与书面验证方法一致。	当与唯一 ID 配合使用时，这些验证方法有助于防止用户 ID 受到威胁，因为尝试威胁用户 ID 的人必须同时知晓唯一 ID 和密码（或使用的其他验证）。请注意，只要数字证书对特定用户来说唯一的，那它也是“所有”用户验证方法的有效选择。 由于恶意个人威胁系统的其中一个优先步骤是利用弱密码或不存在的密码，因此实施良好的验证管理流程很重要。
8.2.1 使用强效加密法使所有验证证书（例如密码/口令）在所有系统组件中传输和存储时均不可读。	**8.2.1.a** 检查供应商文档记录和系统配置设置，确认在传输和存储过程中用强效加密法保护密码。	很多网络设备和应用程序会在网络中传输未加密的可读密码和/或存储未加密的密码。恶意个人可在传输过程中使用“嗅探器”轻松拦截未加密的密码，或直接访问存储在文件中的未加密密码，并使用该数据来进行非授权访问。
	8.2.1.b 对于系统组件样本，检查密码文件以确认密码在存储过程中不可读。	
	8.2.1.c 对于系统组件样本，检查数据传输以确认密码在传输过程中不可读。	

PCI DSS 要求	测试程序	指南
	8.2.1.d 针对服务提供商的附加程序：查看密码文件以确认客户密码在存储过程中不可读。	
	8.2.1.e 针对服务提供商的附加程序：查看数据传输以确认客户密码在传输过程中不可读。	
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。	**8.2.2** 检查修改验证凭证的验证程序并监控安全人员，确认如果用户通过电话、电子邮件、网络或其他非面对面的方法请求重置验证凭证，则在修改验证凭证前已验证用户身份。	很多恶意个人会使用“社会工程”（例如，呼叫技术支持人员并充当合法用户）来变更密码，从而使用用户 ID。重置或修改验证凭证之前，可以使用只有真正的用户才能回答的“保密问题”来帮助管理员识别用户。
8.2.3 密码/口令必须符合以下要求： • 至少为 7 个字符。 • 同时包含数字和字母字符。 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。	**8.2.3a** 对于系统组件样本，检查系统配置设置，确认用户密码参数设为至少具有以下强度/复杂度： • 至少为 7 个字符。 • 同时包含数字和字母字符。	强效密码/口令是进入网络的第一道防线，因为恶意个人通常会首先尝试找到密码较弱或不存在密码的帐户。如果密码简短或易猜，则恶意个人相对更容易找到这些脆弱帐户并在有效用户 ID 的伪装下威胁网络。 本要求明确规定密码/口令应至少为 7 个字符且同时包含数字和字母字符。如果由于技术限制无法满足这个最低要求，实体可使用“等效强度”来评估其替代选择。NIST SP 800-63-1 将熵定义为“猜测或确定密码或密钥的难度衡量指标”。您可以参阅本文档和探讨“密码熵”的其他文档，以了解适用熵值的更多信息，以及不同格式的密码/口令其等效口令强度的变化性。
	8.2.3.b 针对服务提供商的附加程序：审核内部流程和客户/用户文档记录，确认非消费者用户密码需要符合至少以下强度/复杂度： • 要求至少为 7 个字符。 • 同时包含数字和字母字符。	
8.2.4 至少每 90 天变更一次用户密码/口令。	**8.2.4.a** 对于系统组件样本，检查系统配置设置，确认用户密码参数设为要求用户至少每 90 天变更一次密码。	长时间不更改的密码/口令会为恶意个人提供更多时间来破译密码/口令。
	8.2.4.b 针对服务提供商的附加程序：审核内部流程和客户/用户文档记录，确认： • 非消费者用户密码需要定期更改，且 • 指导非消费者用户在何时以及何种情况下必须更改密码。	
8.2.5 不允许个人提交与最近 4 个所用密码/口令相同的新密码/口令。	**8.2.5.a** 对于系统组件样本，获取并检查系统配置设置，确认密码参数设为新口令不得与最近用过的 4 个密码相同。	如果未维护密码历史记录，则会降低更改密码的效力，因为之前使用的密码可能被反复重用。要求一段时间内不得重用密码，这可降低在日后使用已猜出或强制获取的密码的可能性。
	8.2.5.b 针对服务提供商的附加程序：审核内部流程和客户/用户文档记录，确认非消费者用户的新密码不得与之前的 4 个密码相同。	
8.2.6 将每个用户的首次密码/口令和重置密码/口令设为唯一值，并在首次使用	**8.2.6** 检查密码程序并监视安全人员，确认所有新用户的首次密码	若每个新用户都使用相同的密码，则内部用户、前员工或恶意个人可能会知道或轻松发现密码并

PCI DSS 要求	测试程序	指南
后立即变更。	和现有用户的重置密码均设为唯一值并在首次使用后变更。	用其访问帐户。
8.3 对来自网络外部人员（包括用户和管理员）以及所有第三方的远程网络访问（包括基于支持或维护目的的供应商访问）使用双因素验证。 ***注：****双因素验证要求使用三种验证方法中的两种（请参阅要求 8.2 验证方法的说明）进行验证。使用一个因素两次（例如，使用两个不同的密码）不视为双因素验证。* 双因素技术包括带令牌的远程认证拨号用户服务 (RADIUS)、带令牌的终端访问控制器访问控制系统 (TACACS) 以及便于双因素验证的其他技术。	**8.3.a** 检查远程访问服务器和系统的系统配置，确认以下访问必须进行双因素验证： • 工作人员的所有远程访问 • 所有第三方/供应商远程访问（包括基于支持或维护目的对应用程序和系统组件进行的访问） **8.3.b** 监控远程连接到网络的人员（例如，用户和管理员）样本并确认至少使用了三种验证方法中的两种。	双因素验证要求对风险较高的访问（例如来自网络外部的访问）实施两种验证。 本要求适用于所有人员，包括远程访问网络的普通用户、管理员和供应商（进行支持和维护），而通过该远程访问会导致对持卡人数据环境的访问。 如果远程访问所针对的实体网络拥有适当的分割，使远程用户无法访问或影响持卡人数据环境，那么无需对该网络的远程访问实施双因素验证。但是，如果远程访问所针对的网络可以访问持卡人数据环境，则需要进行双因素验证，而且推荐对实体网络的所有远程访问均采用双因素验证。
8.4 记录并向所有用户传达验证程序和政策，包括： • 选择强效验证凭证的指南 • 关于用户应如何保护其验证凭证的指南 • 关于不重用之前用过密码的说明 • 用户如怀疑密码可能暴露则应修改密码	**8.4.a** 检查程序并与工作人员面谈，确认已为所有用户分配验证程序和政策。 **8.4.b** 审核分发给用户的验证程序和政策，确认其中包括： • 选择强效验证凭证的指南 • 关于用户应如何保护其验证凭证的指南。 • 关于用户不重用之前用过密码的说明 • 用户如怀疑密码可能暴露则应修改密码 **8.4.c** 抽样选取部分用户进行面谈，确认其熟悉验证程序和政策。	向所有用户传达密码/验证程序可帮助其理解并遵守政策。 例如，选择强效密码的指南可能包括帮助工作人员选择难猜密码的建议，这种密码不包含词典中的词汇，也不包含用户的个人信息（例如，用户 ID、家人姓名、生日等）。保护验证凭证的指南可能包括不要记录密码或将其保存在非安全文件中，以及警惕会尝试利用密码的恶意个人（例如，以“解决问题”为由打电话给员工询问密码）。 当密码可能不再安全时指导用户变更密码可防止恶意用户使用合法密码来进行非授权访问。
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： • 常规用户 ID 已禁用或删除 • 用于系统管理和其他重要功能的共享用户 ID 不存在 • 不使用共享和常规用户 ID 管理任何系统组件	**8.5.a** 对于系统组件样本，检查用户 ID 列表，确认下列各项： • 常规用户 ID 已禁用或删除 • 用于系统管理活动和其他重要功能的共享用户 ID 不存在 • 不使用共享和常规用户 ID 管理任何系统组件 **8.5.b** 检查验证政策/程序，确认已明确禁止使用群组和共享 ID 及/或密码或其他验证方法。 **8.5.c** 与系统管理员面谈，确认未分配群组和共享 ID 及/或密码或其他验证方法（即使有请求）。	如果多个用户共享一个验证凭证（例如用户帐户和密码），系统访问和活动便不可能追溯到个人。反过来则会妨碍实体为个人行为指定责任或有效记录个人行为，因为某个特定行为可能由群组内任何知道验证凭证者执行。

PCI DSS 要求	测试程序	指南
8.5.1 针对服务提供商的额外要求：有权远程进入客户经营场所的服务提供商（例如 POS 系统或服务器的维修商）必须使用每个客户经营场所独有的验证凭证（例如密码/口令）。 ***注：****本要求不适用于共享托管服务提供商访问自己的托管环境（其中托管有多个客户环境）。* ***注：****要求 8.5.1 在 2015 年 6 月 30 日前属于最优方法，此后将成为一项要求。*	**8.5.1** 针对服务提供商的额外程序：检查验证政策和程序，与工作人员面谈，确认访问每个客户时使用不同的验证凭证。	确保服务提供商使用不同的验证凭证访问每位客户，有助于避免使用同一组密码威胁到多位客户。 采用双因素机制等技术，为每个连接提供唯一的凭证（例如，通过一次性密码），也能达到本要求的目的。
8.6 如使用实物或逻辑安全令牌、智能卡和证书等其他验证机制，则必须按如下方法分配这些机制的使用： • 验证机制必须分配到单个帐户，不得在多个帐户之间共享 • 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权限	**8.6.a** 检查验证政策和程序，确认已制定实物安全令牌、智能卡和证书等验证机制的使用程序，并且包含以下方面： • 验证机制分配到单个帐户，而非在多个帐户之间共享 • 已定义物理和/或逻辑控制，以确保仅既定帐户可使用该机制获得权限	如果令牌、智能卡和证书等用户验证机制可以由多个账户共用，则可能无法使用验证机制识别个人的身份。使用物理和/或逻辑控制（例如 PIN、生物特征数据或密码）来唯一地识别账户用户，可防止未授权用户通过使用共享验证机制获得访问权限。
	8.6.b 与安全工作人员面谈，确认验证机制已分配到单个帐户，而非在多个帐户之间共享	
	8.6.c 检查系统配置设置和/或物理控制（如适用），确认已实施控制措施，确保仅既定帐户可利用该机制获得权限	
8.7 禁止对包含持卡人数据的任何数据库的 一切访问（包括应用程序、管理员和所有其他用户的访问），具体如下： • 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。 • 仅数据库管理员能直接访问或查询数据库 • 数据库应用程序的应用 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）	**8.7.a** 检查数据库和应用程序配置设置，确认所有用户在访问前均经过验证。	访问数据库和应用程序时如无用户验证，无授权或恶意访问的可能性便会增加，由于用户未经验证，所以系统无从知晓，也就无法记录此类访问。另外，仅应通过编程方法（例如通过存储的程序）授予数据库访问权，而非最终用户直接访问数据库（数据库管理员除外，他们可能需要直接访问数据库执行管理职责）。
	8.7.b 检查数据库和应用程序配置设置，确认用户对数据库的所有访问、查询和操作（例如移动、复制、删除）仅通过编程方法（例如通过存储的程序）完成。	
	8.7.c 检查数据库访问控制设置和数据库应用程序配置设置，确认用户直接访问或查询数据库的权限仅限于数据库管理员。	
	8.7.d 检查数据库访问控制设置、数据库应用程序配置设置和相关的应用程序 ID，确认应用程序 ID 仅可由这些应用程序使用（个人用户或其他流程不能使用）。	
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。	**8.8** 检查文档记录并与工作人员面谈，确认用于身份识别和验证的安全政策与操作程序均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守安全政策和操作程序，确保始终对身份识别和验证进行管理。

要求 9：　　限制对持卡人数据的物理访问

对数据或存储持卡人数据的系统的物理访问会让个人有机会访问设备或数据，删除系统或硬拷贝，所以应予以适当限制。在要求 9 中，“现场工作人员”指出现在实体经营场所的全职和兼职员工、临时工、承包商和顾问。“访客”指供应商、任何现场工作人员的客人、服务工人，或任何需要短时进入经营场所的人员，停留时间通常不超过一天。“媒介”指所有包含持卡人数据的纸质和电子媒介。

PCI DSS 要求	测试程序	指南
9.1 采用适当的场所入口控制，对持卡人数据环境中系统的物理访问进行限制和监控。	**9.1** 确认持卡人数据环境中的每个计算机房、数据中心和其他具备系统的实体区域均设有实体安全控制。 ▪ 确认已使用工卡读卡器或其他设备（包括经授权的工卡、锁和钥匙）控制接触。 ▪ 观察系统管理员在持卡人环境中试图登录随机选择的系统控制台时的操作，确认控制台已“锁定”，以防非授权使用。	如果没有物理访问控制，例如工卡系统和门禁控制，未授权人员便可能进入经营场所，窃取、禁用、干扰或破坏重要系统和持卡人数据。 锁定控制台登录屏可防止未授权人员访问敏感信息、更改系统配置，将漏洞引入网络或销毁记录。
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情况。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。 ***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。*	**9.1.1.a** 确认已使用摄像头和/或访问控制机制监控敏感区域的出入口。 **9.1.1.b** 确认摄像头和/或访问控制机制受到安全保护，免遭破坏或禁用。 **9.1.1.c** 确认已对摄像头和/或访问控制机制实施监控，并且来自摄像头或其他机制的数据至少保存三个月。	在调查实体漏洞时，这些控制措施能帮助识别曾对这些敏感区域进行物理访问的个人，以及他们进入和离开的时间。 试图获得敏感区域物理访问权的罪犯经常会尝试禁用或避开监控控制。为保护这些控制设备免遭破坏，可将摄像头安装在罪犯够不着和/或可监测到破坏行为的位置。同样地，可以监控访问控制机制或安装实体保护设备，以防被恶意个人破坏或禁用操作。 敏感区域包括企业数据库服务器室、零售店内存储持卡人数据的后端办公室，以及大量持卡人数据的存储区。每个组织都应确定敏感区域，以确保实施适当的物理监控控制措施。
9.1.2 实施物理和/或逻辑控制，限制对公共网络插座交换机的访问。 *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，也可以实施流程，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。*	**9.1.2** 与负责人员面谈并查看公共网络插座交换机的位置，确认现已实施物理和/或逻辑控制，以限制对公共网络插座交换机的访问。	限制对网络插座交换机（或网络端口）的访问可阻止恶意个人接入现有网络插座交换机并访问内部网络资源。 无论采用逻辑控制还是物理控制，或者二者相结合，都应有充足的控制措施来防止未经明确授权的个人或设备与网络连接。

PCI DSS 要求	测试程序	指南
9.1.3 限制对无线访问点、网关、手持式设备、网络/通信硬件和电信线路的物理访问。	**9.1.3** 确认已适当限制无线访问点、网关、手持式设备、网络/通信硬件和电信线路的物理访问。	如果不能确保无线组件和设备的使用安全，恶意用户便会利用组织无人值守的无线设备访问网络资源，甚至将自己的设备与无线网络连接，进行非授权访问。此外，确保网络和通信硬件安全也可防止恶意用户拦截网络流量或将自己的设备与有线网络资源进行物理连接。
9.2 制定相关程序，轻松识别现场工作人员和访客，包括： ▪ 识别新的现场工作人员或访客（例如发放工卡） ▪ 修改访问要求 ▪ 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）	**9.2.a** 检查流程文档记录，确认已制定用于识别和区分现场工作人员与访客的程序。 确认程序包括以下方面： • 识别新的现场工作人员或访客（例如发放工卡）， • 修改访问要求，以及 • 废除已离职现场工作人员和过期访客的身份证件（例如工卡）	识别授权访客，以便轻松区分授权访客与现场工作人员，防止允许未授权访客进入包含持卡人数据的区域。
	9.2.b 查看关于识别和区分现场工作人员与访客的流程，确认： • 访客的身份已清楚识别，并且 • 能轻松区分现场工作人员和访客	
	9.2.c 确认验证流程（如工卡系统）的查看权仅限于授权人员。	
	9.2.d 检查目前采用的身份识别方法（例如工卡），确认其能清楚识别访客，并能轻松区分现场工作人员和访客。	
9.3 控制现场工作人员对敏感区域的物理访问，具体如下： • 必须根据个人的工作职能获取使用权 • 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。	**9.3.a** 对于抽样选取的具有 CDE 物理访问权的现场工作人员，与负责人员面谈并查看访问控制列表，以确认： • 已授予 CDE 访问权 • 访问权系个人工作职能所必需	控制 CDE 的物理访问权有助于确保仅具有正当业务需求的授权人员获得访问权。 当工作人员离职时，所有物理访问机制均应及时退回或禁用（越快越好），以确保工作人员在离职后不能再进入 CDE。
	9.3.b 查看工作人员对 CDE 的访问，确认所有工作人员均在批准后方获得访问权	
	9.3.c 选择抽样选取的最近离职的员工，并检查访问控制列表，确认这些人员不具有 CDE 的物理访问权	
9.4 实施相关程序，识别并批准访客。 程序应包括以下方面：	**9.4** 确认现已实施访客授权和访问控制流程，具体如下：	要削弱未授权人员和恶意个人进入经营场所（以及可能访问持卡人数据）的能力，访客控制非常重要。 访客控制可确保访客身份被识别为访客，以便工作人员能监控其活动，且其访问权仅限于正
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	**9.4.1.a** 查看程序并与工作人员面谈，确认访客必须在获准后方可进入，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。	

PCI DSS 要求	测试程序	指南
	9.4.1.b 查看访客工卡或其他身份证件的使用情况，确认实体令牌工卡不允许在无人陪同的情况下进入处理或维护持卡人数据的现场区域	当访问期间。 确保在访问到期或结束时归还访客工卡，可阻止恶意个人在访问结束后利用之前获批的通行许可实地进入大楼。 访客日志记录关于访客的极少量信息，维护简单，费用不高，并可协助识别实际进入的大楼或房间，以及可能接触的持卡人数据。
9.4.2 识别访客并给访客发放一张工卡或有有效期且能明显区别访客与现场工作人员的其他身份证件。	**9.4.2.a** 查看经营场所内的人员，确认已使用访客工卡或其他身份证件，并能从现场工作人员中轻松分辨出访客。	
	9.4.2.b 确认访客工卡或其他身份证件的有效期。	
9.4.3 要求访客在离开经营场所前或在到期日交还工卡或身份证件	**9.4.3** 查看离开经营场所的访客，确认访客在离开或证件到期时被要求交还工卡或其他身份证件。	
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检查记录。 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。 除非法律另有规定，否则该日志至少应保留三个月。	**9.4. 4.a** 确认目前正在使用访客日志记录对经营场所以及存储或传输持卡人数据的计算机房和数据中心的物理访问。	
	9.4. 4.b 确认日志包含： • 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	
	9.4.4.c 确认该日志至少保留三个月。	
9.5 保护所有媒介的实体安全。	**9.5** 确认用于保护持卡人数据的程序包含关于保护所有媒介（包括但不限于计算机、可移动电子媒介、纸质收据、纸质报告和传真）实体安全的控制措施。	用于保护媒介实体安全的控制措施旨在阻止未授权个人访问任何类型媒介上的持卡人数据。当持卡人数据被存储在可移动或便携式媒介上、被打印出或留在某人的办公桌上时，如果未加保护，极易被非授权人员查看、复制或扫描。
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。	**9.5.1.a** 查看存储场所的实体安全性，确认备份媒介存储安全。	如果存储在不安全的场所，包含持卡人数据的备份可能会轻易丢失、被窃或被复制，用于恶意用途。
	9.5.1.b 确认至少每年检查一次存储场所的安全性。	定期检查存储场所可让组织及时解决发现的安全问题，最大限度地降低潜在风险。
9.6 严格控制任何媒介的内部或外部分发，包括：	**9.6** 确认现已制定控制媒介分发的政策，并且该政策涵盖所有被分发的媒介，包括分发给个人的媒介。	相关程序和流程有助于保护分发给内部和/或外部用户的媒介上存储的持卡人数据。如果没有这些程序，数据可能丢失或被盗，并用于欺诈行为。
9.6.1 对媒介进行分类，以便确定数据的敏感性。	**9.6.1** 确认所有媒介均已分类，以便确定数据的敏感性。	对媒介进行标识非常重要，这样便能轻松识别其分类状态。未标识为“机密”的媒介可能得不到充分保护，或可能丢失或被盗。 ***注：****这并不表示需要在媒介上贴一个标签，注明“机密”；目的是让组织识别包含敏感数据的媒介，以便加以保护。*

PCI DSS 要求	测试程序	指南
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。	**9.6.2.a** 与工作人员面谈并检查记录，确认对外递送的所有媒介均有记录，且通过可靠的快递公司或可跟踪的其他投递方法发出。	如果采用不可跟踪的方法（如普通邮件）递送媒介，媒介可能丢失或被盗。如果通过可靠的快递公司递送包含持卡人数据的媒介，组织便能利用其跟踪系统保留详细记录和运输地点。
	9.6.2.b 从最近几天所有媒介的非现场跟踪日志中抽样选择，确认已记录跟踪详情	
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。	**9.6.3** 从最近几天所有媒介的非现场跟踪日志中抽样选择。检查日志并与负责人员面谈，确认自安全区域转移媒介时（包括将媒介分发给个人）经过管理层的适当批准。	如果没有严格流程确保媒介自安全区域迁移前所有媒介移动均经过审批，便不能对这些媒介进行跟踪或适当保护，并且也无从知晓其位置，从而导致媒介丢失或被盗。
9.7 严格控制对媒介的存储和获取。	**9.7** 获取并检查所有媒介的存储和维护控制政策，确认该政策要求对媒介进行定期盘点。	如果没有细致的盘点方法和存储控制，被盗或丢失的媒介可能被人们无限期地忽视。
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。	**9.7.1** 检查媒介盘存记录，确认已保留记录，并且至少每年盘点一次媒介。	如果不对媒介进行盘点，被盗或丢失的媒介可能在很长时间内不被人注意，或根本不会引起注意。
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** 检查媒介定期销毁政策，确认该政策涵盖所有媒介，并具备以下要求： • 硬拷贝材料必须粉碎、焚烧或打浆，以合理保证这些硬拷贝材料无法重建。 • 用于存放待销毁材料的容器必须安全。 • 电子媒介上的持卡人数据必须通过安全擦除程序（符合行业认可的安全删除标准）或通过销毁媒介实体令其不可恢复。	处置前如未采取措施销毁硬盘、移动硬盘、CD/DVD或纸张上的信息，恶意个人或许能从被处置的媒介中找回信息，从而导致数据受到威胁。例如，恶意个人可利用一种称作“垃圾搜寻”的技术搜索垃圾桶和回收站，以查找其可用来发起攻击的信息。 确保待销毁材料所用存储容器的安全性，这样在材料被收集时即可阻止敏感信息被他人捕获。例如，“待粉碎”的容器可以上一把锁，阻止他人获取其中的内容或采用其他辅助物防止进入容器内部。 安全销毁电子媒介的方法包括安全擦除、消磁或实体销毁（如碾碎或粉碎硬盘）。
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。	**9.8.1.a** 与工作人员面谈并检查程序，确认硬拷贝材料被粉碎、焚烧或打浆，以合理保证硬拷贝材料无法重建。	
	9.8.1.b 检查包含待销毁信息的材料所使用的存储容器，确认容器的安全性。	
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。	**9.8.2** 利用符合行业认可的安全删除标准的安全擦除程序，让电子媒介上的持卡人数据不可恢复或以其他方式直接销毁该媒介。	

PCI DSS 要求	测试程序	指南
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。 ***注：****本要求适用于销售点有卡交易（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。* ***注：****要求 9.9 在 2015 年 6 月有 30 日前属于最优做法，此后将成为一项要求。*	**9.9** 检查政策和程序文档记录，确认其包含： • 保存一份设备列表 • 定期检查设备，查找篡改或替换迹象 • 培训工作人员，确保其了解可疑行为，并举报篡改或替换设备的行为	罪犯往往通过窃取和/操控读卡设备和终端盗取持卡人数据。例如，他们试图盗窃设备，以便了解进入方法，他们还经常试图用欺诈性设备取代合法设备，每次插入卡时，欺诈性设备都会向他们发送支付卡信息。罪犯还会试图在设备外部添加“浏览”组件，专用于在进入该设备前捕获支付卡详情，例如在合法读卡器的顶部另装一台读卡器，以便二次捕获支付卡详情；一次通过罪犯的组件捕获，另一次通过设备的合法组件捕获。这样，当罪犯在此过程中“浏览”支付卡信息时，交易仍可完成，不必中断。 对于手动密钥输入组件，例如计算机键盘和 POS 机键盘，这项要求属建议，非强制规定。 关于防范浏览的其他最优方法可在 PCI SSC 网站上获取。
9.9.1 保留一份最新的设备列表。该列表应包含如下信息： • 设备的外形、型号 • 设备的位置（例如设备所安放的现场或设施的地址） • 设备的序列号或其他独特验证方法	**9.9.1.a** 检查设备列表，确认其中包含： • 设备的外形、型号 • 设备的位置（例如设备所安放的现场或设施的地址） • 设备的序列号或其他独特验证方法 **9.9.1.b** 从列表中抽样选择设备并查看设备的位置，以确认该列表准确无误且为最新信息。 **9.9.1.c** 与工作人员面谈，确认设备在新增、更换位置、停用时该等设备列表也随之更新。	保留最新的设备列表有助于组织记录设备应位于的位置，从而快速识别某设备是否不见或已丢失。 保留设备列表时可采用自动方法（例如一个设备管理系统），也可采用手动方法（例如在电子或纸质记录中记载）。移动设备的位置可以是被指定人员的姓名。
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	**9.9.2.a** 检查书面程序，确认已规定包含以下内容的流程： • 设备的检查程序 • 检查频率	定期检查设备有助于组织更快速地检测设备是否被篡改或替换，从而最大程度地降低使用欺诈性设备的潜

PCI DSS 要求	测试程序	指南
调换）迹象。 ***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。*	**9.9.2.b** 与负责人员面谈并查看检查流程，确认： • 工作人员了解设备的检查程序 • 定期检查所有设备，查看是否存在篡改和替换现象	在影响。 检查类型取决于设备，例如，使用安全设备的图片来比较其当前外观与原来的外观，查看设备是否发生改变。另一个选择是使用安全记号笔（例如紫外线记号笔）在设备表面和开口处做标记，从而轻松判断设备是否被替换或篡改。罪犯经常会通过替换设备外壳来掩盖篡改行为，上述方法有助于检测这种做法。此外，设备供应商可提供安全指南以及“方法”指南，帮助确定设备是否被篡改。 检查频率取决于设备位置、设备是否有人看管等因素。例如，对于放在公共区域、不受组织人员监管的设备，其检查频率要比放在安全区域或公共可接触时受监管的设备高。检查的类型和频率由商户根据年度风险评估流程的规定来决定。
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： • 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 • 在未经验证的情况下，不要安装、替换或退还设备 • 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） • 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	**9.9.3.a** 审核销售点所在地工作人员的培训材料，确认其包含以下培训内容： • 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 • 在未经验证的情况下，不要安装、替换或退还设备 • 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） • 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 **9.9.3.b** 抽样选取部分销售点所在地工作人员进行面谈，确认他们已参加培训并了解以下程序： • 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 • 在未经验证的情况下，不要安装、替换或退还设备 • 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） • 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	罪犯经常会冒充授权维护人员来获取对 POS 设备的使用权。对于所有请求使用 POS 设备的第三方，始终在允许使用之前进行验证，例如，与管理人员确认或打电话给 POS 维护公司（例如供应商或收单机构）进行验证。很多罪犯会通过伪装外表（例如，身穿工作服且手提工具箱）来欺骗员工，他们也可能知道设备的位置，因此培训员工始终遵守程序很重要。 罪犯喜欢使用的另一个计谋是寄来一个“新的”POS 系统，要求与合法系统交换并将合法系统“寄回”指定地址。由于十分想获得这些设备，罪犯甚至会提供回寄邮费。安装设备或在工作中使用设备前，工作人员应始终与经理或供应商确认设备合法并来自可信来源。

PCI DSS 要求	测试程序	指南
9.10 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物理访问权的安全政策和操作程序。	**9.10** 检查文档记录并与工作人员面谈，确认用于限制持卡人数据物理访问权的安全政策和操作程序均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守安全政策和操作程序，始终限制持卡人数据和 CDE 系统的物理访问权。

定期监控并测试网络

要求 10：　　跟踪并监控对网络资源和持卡人数据的所有访问

记录机制和用户活动跟踪功能对防止、检测或最大程度降低数据威胁的影响很重要。如果所有环境中存在日志，则可在出错时执行彻底的跟踪、告警和分析。如果没有系统活动日志，则很难确定导致威胁的原因。

PCI DSS 要求	测试程序	指南
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。	**10.1** 通过查看并与系统管理员面谈，确认： • 系统组件的检查记录已启用并处于活动状态 • 对系统组件的访问已链接到个人用户	拥有一套将用户访问链接到所访问系统组件的流程或系统很重要。该系统会生成检查日志并能追溯特定用户的可疑活动。
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** 通过与负责人员面谈、查看检查日志并审查检查日志设置，执行以下操作：	通过生成可疑活动的检查记录，可向系统管理员发出警报、向其他监控机制（例如入侵检测系统）发送数据，并为事后跟进提供历史记录。组织能通过记录以下事件来识别并跟踪潜在的恶意活动
10.2.1 对持卡人数据的所有个人用户访问	**10.2.1** 确认已记录持卡人数据的所有个人访问。	恶意个人会获取可用于访问 CDE 中系统的用户帐户信息，或新建一个非授权帐户来访问持卡人数据。通过记录对持卡人数据的所有个人访问，可识别受到威胁或误用的帐户。
10.2.2 任何具有 root 或管理员权限的个人执行的所有操作	**10.2.2** 确认已记录任何具有 root 或管理员权限的个人执行的所有操作。	具有更高权限的帐户（例如“管理员”或“root”帐户）可能会对系统的安全性或操作功能产生巨大的影响。若不记录所执行的活动，则组织无法追踪到特定操作和个人产生的因管理员错误或权限误用导致的任何问题。
10.2.3 对所有检查记录的访问	**10.2.3** 确认已记录对所有检查记录的访问。	恶意用户经常会尝试通过更改检查日志来掩盖其操作，而组织可使用访问记录跟踪个人帐户日志的任何不一致或潜在篡改情况。访问可识别变更、添加和删除的日志有助于追溯非授权人员执行的操作步骤。
10.2.4 无效的逻辑访问尝试	**10.2.4** 确认已记录无效的逻辑访问尝试。	恶意个人经常会对目标系统执行多次访问尝试。多次无效的登录尝试可说明非授权用户尝试“强制获得”或猜测密码。
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	**10.2.5.a** 确认已记录识别和验证机制的使用情况。 **10.2.5.b** 确认已记录所有权限提升	如果不知道事件发生时的登录用户，便无法识别所使用的帐户。另外，恶意用户会尝试操纵验证控制来绕过控制或模仿有效帐户。

PCI DSS 要求	测试程序	指南
删除	**10.2.5.c** 确认已记录任何具有 root 或管理员权限的帐户的所有变更、添加或删除情况	
10.2.6 检查日志的初始化、关闭或暂停	**10.2.6** 确认已记录以下内容： • 检查日志的初始化 • 检查日志的关闭或暂停	在执行非法活动之前关闭（或暂停）检查日志是恶意用户避免检测的常用方法。检查日志的初始化说明用户通过禁用日志功能来掩盖其操作。
10.2.7 系统级对象的创建和删除	**10.2.7** 确认已记录系统级对象的创建和删除。	恶意软件经常在目标系统中创建或替换系统级对象，从而控制该系统中的特定功能或操作。通过在创建或删除系统级对象（例如数据库表或所存储的程序）时进行记录，可以更轻松地确定修改是否获得授权。
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** 通过访问并查看每个可检查事件（参阅 10.2）的检查日志，执行以下操作：	通过记录 10.2 中可检查事件的此类细节，可快速识别潜在威胁，并获得了解人物、事件、地点、时间和方式的足够详情。
10.3.1 用户识别	**10.3.1** 确认用户识别包含在日志条目中。	
10.3.2 事件类型	**10.3.2** 确认事件类型包含在日志条目中。	
10.3.3 日期和时间	**10.3.3** 确认日期和时间戳包含在日志条目中。	
10.3.4 成功或失败指示	**10.3.4** 确认成功或失败指示包含在日志条目中。	
10.3.5 事件的起因	**10.3.5** 确认事件的起因包含在日志条目中。	
10.3.6 受影响的数据、系统组件或资源的特性或名称。	**10.3.6** 确认受影响的数据、系统组件或资源的特性或名称包含在日志条目中。	
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。 ***注：****网络时间协议 (NTP) 便是一种时间同步技术。*	**10.4** 检查配置标准和流程，确认已根据 PCI DSS 要求 6.1 和 6.2 实施并更新时间同步技术。	时间同步技术可用于同步多个系统的时钟。在未正确同步时钟时，可能会难以比较不同系统中的日志文件、难以建立准确的事件序列（对出现漏洞时的取证分析很关键）。对于事后取证团队而言，所有系统中时间的准确性和一致性以及每个活动的时间对确定系统如何受到威胁很重要。

PCI DSS 要求	测试程序	指南
10.4.1 关键系统的时间正确且一致。	**10.4.1.a** 检查获取、分配和存储组织内部正确时间的流程，确认： • 只有指定的中央时间服务器能接收外来的时间信号，且外来的时间信号以国际原子时或 UTC 为基础。 • 当存在多个指定时间服务器时，这些时间服务器会相互同步以保持准确的时间。 • 系统只接收来自指定中央时间服务器的时间信息。	
	10.4.1.b 对于系统组件样本，查看与时间相关的系统参数设置，确认： • 只有指定的中央时间服务器能接收外来的时间信号，且外来的时间信号以国际原子时或 UTC 为基础。 • 当存在多个指定时间服务器时，这些指定的中央时间服务器会相互同步以保持准确的时间。 • 系统只接收来自指定中央时间服务器的时间。	
10.4.2 时间数据受保护。	**10.4.2.a** 检查系统配置和时间同步设置，确认仅有业务需要的人员才能访问时间数据。	
	10.4.2.b 检查系统配置、时间同步设置和日志以及流程，确认已记录、监控并审核关键系统中时间设置的任何变更。	
10.4.3 时间设置来自行业认可的时间来源。	**10.4.3** 检查系统配置，确认时间服务器接受来自行业认可的特定外部来源的时间更新（以防止恶意个人更改时钟）。可选择性地使用对称密钥加密此类更新，并创建访问控制列表指定客户端计算机（会接收时间更新）的 IP 地址（以防止内部时间服务器的非授权使用）。	
10.5 保护检查记录，禁止进行更改。	**10.5** 与系统管理员面谈并检查系统配置和许可，确认已按以下方式保护检查记录以防被更改：	通常，进入网络的恶意个人会通过尝试编辑检查日志来掩盖其活动。如果未对检查日志提供充分的保护，则无法保证其完整性和准确性，且检查日志会在遭受威胁后成为无用的调查工具。
10.5.1 只允许有工作需要的人查看检查记录。	**10.5.1** 仅有工作需要的个人才能查看检查记录文件。	检查日志的充分保护包括强效访问控制（仅基于“知情需要”限制对日志的访问），以及使用物理或网络隔离提高找到并修改日志的难度。 将日志及时备份到很难更改的集中日志服务器或媒体上，可以妥善地保护日志，即使生成日志的系统受到威胁，日志也不会受到影响。
10.5.2 防止检查记录文件受到非授权修改。	**10.5.2** 通过访问控制机制、物理隔离和/或网络隔离，防止当前检查记录文件受到非授权修改。	
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。	**10.5.3** 即时将当前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。	

PCI DSS 要求	测试程序	指南
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。	**10.5.4** 将向外技术（例如，无线电、防火墙、DNS、邮件）的日志写入安全的内部中央日志服务器或媒介。	写入向外技术（例如，无线电、防火墙、DNS 和邮件服务器）的日志，将降低日志被丢失或更改的风险，这是因为此类日志在内部网络更加安全。 日志可直接写入、卸载或从外部系统复制到安全的内部系统或媒介中。
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）。	**10.5.5** 检查系统设置、受监控的文件和监控活动的结果，确认对日志使用文件完整性监控或变更检测软件。	文件完整性监控或变更检测系统会检查关键文件的变更并在发现这种变更时发出通知。为了进行文件完整性监控，实体通常会监控不常变更但一旦变更即表示可能受到威胁的文件。
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。 ***注：****可使用日志搜集、分析和告警工具来满足本要求。*	**10.6** 执行以下操作：	很多漏洞在出现数天或数月后才能被检测到。每天检查日志可最大程度地减少潜在漏洞的存在时间和暴露量。 通过手动或自动方法定期审核日志，可识别并预先处理对持卡人数据环境的非授权访问。 日志审核流程不一定要手动执行。使用日志搜集、分析和告警工具可识别需要审核的日志事件，有助于简化流程。
10.6.1 至少每天审核一次以下内容： • 所有安全事件 • 可存储、处理或传输 CHD 和/或 SAD 或者影响 CHD 和/或 SAD 安全性的所有系统组件的日志 • 所有关键系统组件的日志 • 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	**10.6.1.a** 检查安全政策和程序，确认已规定程序，以手动或采用日志工具至少每天审核一次以下内容： • 所有安全事件 • 可存储、处理或传输 CHD 和/或 SAD 或者影响 CHD 和/或 SAD 安全性的所有系统组件的日志 • 所有关键系统组件的日志 • 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	很多漏洞在出现数天或数月后才能被检测到。每天检查日志可最大程度地减少潜在漏洞的存在时间和暴露量。 有必要每日审核安全事件（例如，在发现可疑或异常活动后发出通知或告警）、来自关键系统组件的日志、以及来自执行安全功能的系统（例如，防火墙、IDS/IPS、文件完整性监控 (FIM) 系统等）的日志，以识别潜在的问题。 注意，每个组织对于“安全事件”的界定各不相

PCI DSS 要求	测试程序	指南
子商务重定向服务器等）的日志	**10.6.1.b** 查看流程并与工作人员面谈，确认至少每天审核一次以下内容： • 所有安全事件 • 可存储、处理或传输 CHD 和/或 SAD 或者影响 CHD 和/或 SAD 安全性的所有系统组件的日志 • 所有关键系统组件的日志 • 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	同，而且可能会考虑技术的类型、设备的位置和功能。组织也可能希望维持一个 “正常流量” 的基线，来帮助他们识别异常行为。
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。	**10.6.2.a** 检查安全政策和程序，确认已规定相应程序，以根据组织的政策和风险管理策略，定期手动或采用日志工具审核所有其他系统组件的日志。	所有其他系统组件的日志也应定期进行审核，以识别潜在问题或通过低敏感性系统访问敏感系统的尝试行为。审核频率应由实体的年度风险评估确定。
	10.6.2.b 检查组织的风险评估文档记录并与工作人员面谈，确认已根据组织的政策和风险管理策略实施审核。	
10.6.3 跟进审核过程中发现的例外和异常。	**10.6.3.a** 检查安全政策和程序，确认已规定跟进审核过程中所发现例外和异常的程序。	如果未调查日志审核过程中发现的例外和异常，实体可能不知道其网络内部正在发生的非授权和潜在的恶意活动。
	10.6.3.b 查看流程并与工作人员面谈，确认已跟进例外和异常。	
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）。	**10.7.a** 检查安全政策和程序，确认规定以下内容： • 检查日志保留政策 • 关于保留检查日志至少一年的程序，其中最少 3 个月的日志可立即在线访问。	保留日志至少一年是因为需要一段时间才能发现已经出现或即将出现的威胁，并为调查者提供充足的日志历史记录，以更好地确定潜在漏洞和潜在受影响系统存在的时间。通过设置 3 个月日志立即可用，实体可快速发现数据漏洞并最大程度地降低其影响。将日志存储在离线位置可防止日志立即可用，但也导致需要更长的时间才能恢复日志数据、执行分析以及识别受影响的系统或数据。
	10.7.b 与工作人员面谈并查看检查日志，确认检查日志至少一年可用。	
	10.7.c 与工作人员面谈并查看流程，确认至少可立即恢复前 3 个月的日志以供分析。	
10.8 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。	**10.8** 检查文档记录并与工作人员面谈，确认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均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守安全政策和日常操作程序，始终确保监控所有网络资源和持卡人数据访问。

要求 11：　　定期测试安全系统和流程。

恶意个人和研究人员不断发现漏洞，而新软件不断引出漏洞。应经常测试系统组件、流程和自定义软件，以确保安全控制继续反映不断变化的环境。

PCI DSS 要求	测试程序	指南
11.1 实施流程以测试是否存在无线接入点 (802.11)，并按季度检测和识别所有授权和非授权的无线接入点 ***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。*	**11.1.a** 检查政策和程序，确认已规定相应的流程，以按季度检测并识别授权和非授权的无线接入点。	在网络中实施和/或利用无线技术是恶意用户访问网络和持卡人数据的最常用方法之一。若在公司不知情的情况下安装了无线设备或网络，攻击者便可"悄无声息"地轻松进入网络。非授权无线设备可隐藏于或连接到计算机或其他系统组件、或者直接连接到网络端口或网络设备（例如交换机或路由器）。任何这种非授权设备都会导致非授权接入点进入环境。 了解授权的无线设备有助于管理员快速识别非授权无线设备，而在识别非授权无线接入点后作出响应有助于预先将 CDE 向恶意个人暴露的可能性降到最低。 由于无线接入点可轻松连接到网络、难以检测无线接入点是否存在以及非授权无线设备造成的风险更高，因此即使存在禁止使用无线技术的政策，也必须执行这些流程。 可根据特定环境的大小和复杂度决定适当的工具和流程，用以充分确保环境中未安装有恶意的无线接入点。 例如：对于商场中的一个独立售货亭，其所有通信组件均放在防篡改外壳中，售货亭自行实施详细的物理检查便足以确保未连接或安装恶意的无线接入点。然而，对于有多个节点的环境（例如大型零售店、呼叫中心、服务器机房或数据中心），很难执行详细的物理检查。在这种情况下，可结合多种方法来满足要求，例如将物理系统检查与无线分析器的结果相结合。
	11.1.b 确认所用方法足以检测并识别任何非授权无线接入点，其中至少包括： ▪ 在系统组件中插入 WLAN 卡 ▪ 将系统组件连接到便携或移动设备以创建无线接入点（例如通过 USB 等） ▪ 将无线设备连接到网络端口或网络设备	
	11.1.c 检查最近的无线扫描结果，**确**认： • 已识别出授权和非授权无线接入点，且 • 至少每季度扫描一次所有系统组件和设施。	
	11.1.d 如果采用自动监控（例如无线 IDS/IPS、NAC 等），确认配置会发出警报以通知工作人员。	
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。	**11.1.1** 检查文档记录，确认已保留一份授权的无线接入点清单，并且所有授权无线接入点均有业务理由记录。	
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。	**11.1.2.a** 检查组织的事故响应计划（要求 12.9 ），确认其中已规定在检测到非授权的无线接入点时需作出响应。	
	11.2.1.b 与负责人员面谈并/或检查最近的无线扫描和相关响应，确认在发现非授权的无线接入点时已采取措施。	

PCI DSS 要求	测试程序	指南
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，更改网络拓朴，修改防火墙规则，产品升级）时也运行漏洞扫描。 ***注：****可在季度扫描过程中综合多次扫描报告，表明所有系统均已扫描，且所有相关漏洞均已解决。* *可能需要其他文档记录来确认未修复的漏洞正在解决过程当中。* *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 的遵从。在最初 PCI DSS 审核后的几年里，必须要出现四次季度扫描结果均为通过的情况。*	**11.2** 检查扫描报告和支持文档记录，确认已按如下方式执行内部和外部漏洞扫描：	漏洞扫描是一个针对内外部网络设备和服务器运行的自动工具，旨在暴露可能被恶意个人发现和利用的潜在漏洞。 PCI DSS 要求的漏洞扫描有三种： • 内部季度漏洞扫描由合格人员执行（不要求使用 PCI SSC 认证的授权扫描服务商 (ASV)） • 外部季度漏洞扫描，必须由授权扫描服务商执行。 • 重大变更后需要的内部和外部扫描 一旦发现这些漏洞，实体应予以修复，并重复扫描直至修复所有漏洞。 及时发现并解决漏洞可减少漏洞被利用以及系统组件或持卡人数据被破坏的可能性。
11.2.1 执行每季度一次的内部漏洞扫描，并视需要重复扫描，直至所有“高风险”漏洞（具体规定请参阅要求 6.1）均得以解决。必须由合格人员执行扫描。	**11.2.1.a** 审核扫描报告并确认在最近 12 个月内已执行四次季度内部扫描。	用于识别内部系统漏洞的既有流程规定每季度需执行一次漏洞扫描。应首先解决会对环境造成最大风险的漏洞（例如根据要求 6.1 列为“高”风险的漏洞）。 内部漏洞扫描可由合理独立于被扫描系统组件的合格内部员工（例如防火墙管理员不应负责扫描防火墙）执行，或者实体也可选择由专门从事漏洞扫描的公司执行内部漏洞扫描。
	11.2.1.b 审核扫描报告，并确认扫描过程包含重复扫描直至 PCI DSS 要求 6.1 中定义的所有“高风险”漏洞均已解决。	
	11.2.1.c 与工作人员面谈，确认扫描由合格的内部人员或合格的外部第三方执行，且若适用，也应确保测试者的组织独立性（不要求是 QSA 或 ASV）。	
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。 ***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*	**11.2.2.a** 审核最近四个季度的外部漏洞扫描结果，确认最近 12 个月内已执行四次季度外部漏洞扫描。	由于外部网络面临的破坏风险较大，因此季度外部漏洞扫描必须由 PCI SSC 认证的授权扫描服务商执行。
	11.2.2.b 审核每个季度的扫描和重复扫描结果，确认已符合《ASV 计划指南》对扫描通过的要求（例如不存在 CVSS 评级为 4.0 或以上的漏洞，且无自动故障）。	

PCI DSS 要求	测试程序	指南
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》。*	**11.2.2.c** 审核扫描报告，确认这些扫描均由经 PCI SSC 认证的授权扫描服务商 (ASV) 完成。	
11.2.3 在发生任何重要变更后，视需要执行内部和外部扫描和重复扫描。必须由合格人员执行扫描。	**11.2.3.a** 检查并关联变更控制文档记录与扫描报告，确认已扫描有任何重大变更的系统组件。 **11.2.3.b** 审核扫描报告并确认扫描过程包括重复扫描，直至： ▪ 外部扫描不存在 CVSS 评级为 4.0 或以上的漏洞， ▪ 内部扫描 PCI DSS 要求 6.1 中定义的所有“高风险”漏洞均得以解决。 **11.2.3.c** 验证扫描由合格的内部人员或合格的外部第三方执行，且若适用，也应确保测试者的组织独立性（不要求是 QSA 或 ASV）。	要确定什么是重大变更，很大程度上取决于给定环境的配置。如果某项升级或修改可能会授权访问持卡人数据，或影响持卡人数据环境的安全性，它就可以被视为一项重大变更。 在发生任何重大变更后对环境进行扫描可确保这些变更已经适当完成，这样环境安全则不会因变更而受到威胁。所有受变更影响的系统组件均需扫描。
11.3 实施一种包含以下内容的穿透测试法： • 以行业认可的穿透测试法为基础（例如 NIST SP800-115） • 包括覆盖整个 CDE 环境和关键系统 • 来自网络内部和外部的测试 • 包括用于验证任何网段和范围缩小控制的测试 • 定义应用层穿透测试，至少包括要求 6.5 中列出的漏洞 • 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 • 包括审核并考虑过去 12 个月内遇到的威胁和漏洞 • 指定保留穿透测试结果和修复活动结果。 ***注：****要求 11.3 中的此更新在 2015 年 6 月 30 日前属于最优方法，此后将成为一项要求。在 PCI DSS 3.0 版发布前，必须遵守 PCI DSS 2.0 版中的穿透测试要求。*	**11.3** 检查穿透测试方法并与负责人员面谈，确认已实施一种方法并且包含以下方面： • 以行业认可的穿透测试法为基础（例如 NIST SP800-115） • 包括覆盖整个 CDE 环境和关键系统 • 来自网络内部和外部的测试 • 包括用于验证任何网段和范围缩小控制的测试 • 定义应用层穿透测试，至少包括要求 6.5 中列出的漏洞 • 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 • 包括审核并考虑过去 12 个月内遇到的威胁和漏洞 • 指定保留穿透测试结果和修复活动结果。	穿透测试的目的在于模拟现实世界中的攻击情形，了解攻击者能够穿透环境的程度。这让实体能够更好地了解其潜在的暴露风险，从而制定攻击防御策略。 穿透测试不同于漏洞扫描，因为穿透测试是一种活动进程，可能会使用已识别的漏洞。执行漏洞扫描可能是穿透测试者为制定测试策略要执行的首要步骤之一，但不是唯一步骤。即使漏洞扫描未检测到已知漏洞，穿透测试者往往也会对系统有足够了解，从而识别可能存在的安全缺口。 穿透测试通常是一个以手动为主的过程。测试者虽可使用一些自动工具，但主要利用其系统知识来洞察环境。测试者通常会将利用漏洞的几种类型与突破防御层的目标联系起来。例如，如果测试者发现访问某应用服务器的一种方法，他们会将这个受到威胁的服务器作为一个点，以该服务器有权访问的资源为基础发起一次新的攻击。通过这种方式，测试者能够模拟攻击者采取的攻击方法，找出环境中潜在的薄弱区域。 *不同组织的穿透测试技术各不相同，测试的类型、深度和复杂程度也取决于具体的环境和组织的风险评估。*

PCI DSS 要求	测试程序	指南
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。	**11.3.1.a** 检查最近一次外部穿透测试的工作范围和结果，确认穿透测试： • 按照规定的方法执行 • 至少每年执行一次 • 环境发生任何重大变更后也执行	定期以及环境发生重大变更后执行穿透测试是一种主动的安全措施，有助于最大限度地减少恶意个人访问 CDE 的可能。 要确定什么是重大的升级或修改，很大程度上取决于给定环境的配置。如果某项升级或修改可能会授权访问持卡人数据，或影响持卡人数据环境的安全性，它就可以被视为一项重大的升级或修改。在网络升级和修改后执行穿透测试，可以确保所采取的控制措施在升级或修改后仍然有效。
	11.3.1.b 确认测试由合格的内部人员或合格的外部第三方执行，且若适用，也应确保测试者的组织独立性（不要求是 QSA 或 ASV）。	
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。	**11.3.2.a** 检查最近一次内部穿透测试的工作范围和结果，确认穿透测试至少每年执行一次，并且在环境发生任何重大变更后也执行。 • 按照规定的方法执行 • 至少每年执行一次 • 环境发生任何重大更化后也执行	
	11.3.2.b 确认测试由合格的内部人员或合格的外部第三方执行，且若适用，也应确保测试者的组织独立性（不要求是 QSA 或 ASV）。	
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。	**11.3.3** 检查穿透测试结果，确认已发现的可利用漏洞已被修复，且通过重复执行的测试确认漏洞已经修复。	
11.3.4 如果利用网络分段将 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/方法有任何变更后也执行测试，以确认该分段方法行之有效，并已将所有范围外系统与范围内系统隔离。	**11.3.4.a** 检查分段控制并审核穿透测试方法，核实已规定用于测试所有分段方法的穿透测试程序，以确认其行之有效，并已将所有范围外系统与范围内系统隔离。	穿透测试是一种重要的工具，可确认用于隔离 CDE 与其他网络的任何现有分段方法是否有效。无论来自实体网络外部，还是来自网络内部、CDE 外部，穿透测试均应以分段控制为重点，以确认其不能穿过分段控制进而访问 CDE。例如，执行网络测试和/或开放端口扫描，以确认范围内网络未与范围外网络连接。
	11.3.4.b 检查最近一次穿透测试的结果，确认用于验证分段控制的穿透测试： • 至少每年执行一次，且在分段控制/方法有任何变更后也执行 • 覆盖使用中的所有分段控制/方法 • 确认分段方法行之有效并隔离所有范围外系统与范围内系统。	

PCI DSS 要求	测试程序	指南
11.4 利用入侵检测和/或入侵防御技术来检测和/或防御网络入侵。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。 确保所有入侵检测和防御引擎、基线和签名均为最新。	**11.4.a** 检查系统配置和网络图，确认目前已采用相关技术（例如入侵检测系统和/或入侵防御系统）监控以下位置的所有流量 • 持卡人数据环境周围 • 持卡人数据环境中的关键点	入侵检测和/或入侵防御技术（例如 IDS/IPS）会将进入网络的流量与数千种威胁（黑客工具、特洛伊木马和其他恶意软件）的已知“签名”和/或行为做对比，并在出现这种企图时发出警报并/或加以阻止。如果没有检测未授权活动的积极主动的方法，对计算机资源的攻击（或滥用）便可能在无人注意的情况下实时发生。应监控这些技术发出的安全警报，以便阻止入侵企图。
	11.4.b 检查系统配置并与负责人员面谈，确认入侵检测和/或入侵防御技术会在发现可疑威胁时向工作人员发出警报。	
	11.4.c 检查 IDS/IPS 配置和供应商文档记录，确认已按照供应商的说明对入侵检测和/或入侵防御技术进行配置、维护和升级，以确保提供最佳保护。	
11.5 部署变更检测机制（例如文件完整性监控工具），在发现重要的系统文件、配置文件或内容文件出现非授权修改时警示工作人员；同时配置该软件至少每周执行一次重要文件比对。 ***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。*	**11.5.a** 查看系统设置和受监控文件，并审核监控活动结果，确认已在持卡人数据环境中使用变更检测机制。 应予以监控的文件有： ▪ 系统可执行文件 ▪ 应用程序可执行文件 ▪ 配置和参数文件 ▪ 集中存储文件、历史或归档文件、日志和检查文件 ▪ 由实体（通过风险评估或其他方法）确定的其他重要文件	变更检测解决方案（例如文件完整性监控 (FIM) 工具）可检查对重要文件的修改，并在发现此类修改时发出通知。如果未适当实施并监控变更检测解决方案的输出结果，恶意个人便可能修改配置文件内容、操作系统程序或应用程序可执行文件。如果未检测到非授权变更，则可能让现有安全控制无效并/或导致持卡人数据被盗，并且不会对正常处理产生任何明显影响。
	11.5.b 确认已配置该机制，可在重要文件出现非授权修改时警示工作人员，并至少每周执行一次重要文件比对。	
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。	**11.5.1** 与工作人员面谈，确认已对所有警报进行调查并解决。	
11.6 确保已记录、正在使用且所有相关方了解用于安全监控与测试的安全政策和操作程序。	**11.6** 检查文档记录并与工作人员面谈，确认用于安全监控与测试的安全政策和操作程序均： • 已记录， • 正在使用，且 • 为所有相关方所了解	工作人员需了解并遵守安全政策和操作程序，确保始终进行安全监控与测试。

维护信息安全政策

要求 12：维护针对所有工作人员的信息安全政策。

强有力的安全政策不仅为整个实体奠定了安全基调，而且让工作人员了解公司对他们的要求。所有工作人员均应了解数据的敏感性及其保护这些数据的责任。在要求 12 中，“工作人员”指“常驻”实体经营场所或可以其他方式访问持卡人数据环境的全职和兼职员工、临时工、承包商和顾问。

PCI DSS 要求	测试程序	指南
12.1 制定、公布、维护和宣传安全政策	**12.1** 检查信息安全政策并确认已公布并向所有相关人员（包括供应商和业务合作伙伴）宣传该政策。	公司的信息安全政策可为旨在保护其最宝贵资产的安全措施的实施制定操作步骤。所有工作人员均应了解数据的敏感性及其保护这些数据的责任。
12.1.1 至少每年审核一次安全政策，并在环境发生变更时予以更新。	**12.1.1** 确认至少每年审核一次信息安全政策，并视需要予以更新，以反映业务目标或风险环境的变更情况。	安全威胁和保护方法会迅速演变。如果不更新安全政策以反映相关变化，便不能针对这些威胁制定新的保护措施。
12.2 实施符合以下条件的风险评估流程： • 至少每年执行一次评估，并在环境发生重大变更时（例如收购、合并、迁址等）也执行评估； • 确定重要资产、威胁和漏洞；以及 • 形成正式的风险评估。 （风险评估的方法包括但不限于 OCTAVE、ISO 27005 和 NIST SP 800-30。）	**12. 2.a** 确认每年一次的风险评估过程有文档记录，确定资产、威胁和漏洞，并形成正式的风险评估。 **12. 2.b** 审核风险评估文档记录，确认至少每年执行一次风险评估过程，并在环境有重大变更时也执行。	组织可通过风险评估识别可能对其业务产生不利影响的威胁和相关漏洞。随后，可以有效地分配资源，实施控制措施，从而降低威胁成为现实的可能性及/或减少潜在影响。 至少每年执行一次风险评估并在有重大变更时也执行评估，这样组织便能始终了解最新的组织变更以及不断演变的威胁、趋势和技术。
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。 ***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、电子邮件的使用和互联网的使用* 确保这些使用政策要求：	**12.3** 检查关键技术的使用政策并与负责人员面谈，确认已实施并遵守以下政策：	工作人员使用政策可以禁止使用某些设备和其他技术（如果这是公司政策），或者为工作人员提供正确使用和实施方面的指导。如果使用政策不到位，工作人员可能会使用违反公司政策的技术，从而让恶意个人获得关键系统和持卡人数据的访问权。

PCI DSS 要求	测试程序	指南
12.3.1 被授权方的明确许可	**12.3.1** 确认使用政策包含被授权方明确允许使用这些技术的流程。	如果实施这些技术无需经过适当许可，工作人员可能会根据自己认为的业务需要简单地实施一个解决方案，但也可能为恶意个人攻击关键系统和数据打开方便之门。
12.3.2 技术使用验证	**12.3.2** 确认使用政策包含针对所有技术使用的验证流程，即所有技术在使用时均需通过用户 ID 和密码或其他验证项目（例如令牌）进行验证。	如果应用技术时未经适当验证（用户 ID 和密码、令牌、VPN 等），恶意个人便可能轻松利用这项无保护的技术访问关键系统和持卡人数据。
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	**12.3.3** 确认使用政策已定义一份列出所有设备和获准使用设备的工作人员的列表。	恶意个人可能会破坏实体安全，在网络上安置自己的设备作为“后门”。工作人员也可能绕过程序，安装设备。一份准确的贴有正确标签的设备清单可用于快速识别未经批准的安装。
12.3.4 一种确定负责人、联系信息和用途（例如设备的贴标、编码和/或盘存）的准确方便的方法	**12.3.4** 确认使用政策规定了一种确定负责人、联系信息和用途（例如设备的贴标、编码和/或盘存）的准确方便的方法。	恶意个人可能会破坏实体安全，在网络上安置自己的设备作为“后门”。工作人员也可能绕过程序，安装设备。一份准确的贴有正确标签的设备清单可用于快速识别未经批准的安装。考虑制定一套正式的设备命名规范，并采用现有的库存控制系统记录所有设备。逻辑标签可与能将设备与负责人、联系信息和用途相关联的代码类信息一起使用。
12.3.5 可接受的技术使用方式	**12.3.5** 确认使用政策规定了可接受的技术使用方式。	通过规定可接受的业务用途和公司批准设备及技术的放置位置，公司可更好地管理和控制配置与操作控制之间的缺口，确保不为恶意个人访问关键系统和持卡人数据打开“后门”。
12.3.6 技术可接受的网络位置	**12.3.6** 确认使用政策规定了技术可接受的网络位置。	
12.3.7 公司批准的产品列表	**12.3.7** 确认使用政策包含公司批准的产品列表。	
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	**12.3.8.a** 确认使用政策规定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。	远程访问技术经常成为访问重要资源和持卡人数据的“后门”。在不使用时中断远程访问技术（例如您的 POS 供应商、其他供应商或业务合作伙伴用以支持您系统的技术），可以最大限度地减少网络访问和风险。
	12.3.8.b 检查远程访问技术的配置，确认远程访问会话将在不活跃状态持续一定时间后自动中断。	
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	**12.3.9** 确认使用政策规定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。	
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	**12.3.10.a** 确认使用政策规定在通过远程访问技术访问持卡人数据时禁止将该数据复制、移动或存储到本地硬盘上。	为确保所有工作人员均了解不得将持卡人数据存储或复制到本地个人计算机或其他媒介上的责

PCI DSS 要求	测试程序	指南
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。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。	**12.3.10.b** 对于获得适当授权的工作人员，确认使用政策规定须按照 PCI DSS 要求保护持卡人数据。	任，您的政策应当明确禁止此类活动，获得明确许可的工作人员除外。将持卡人数据存储或复制到本地硬盘或其他媒介上时必须遵守所有适用的 PCI DSS 要求。
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。	**12.4.a** 确认信息安全政策明确规定所有工作人员的信息安全责任。	如未明确规定安全角色和职责分配，与安全小组之间的互动就可能不一致，从而导致不安全地应用技术或使用过时或不安全的技术。
	12.4.b 抽样选取部分负责人员进行面谈，确认其了解这些安全政策。	
12.5 将下列信息安全管理职责分配给个人或团队：	**12.5** 检查信息安全政策与程序，确认： • 信息安全职责已正式分配给首席安全官或其他具有丰富安全知识的管理人员。 • 下列信息安全职责已明确、正式分配：	每个负责信息安全管理的个人或团队均应通过特定政策了解其职责和相关任务。如果不采用这种责任分配制度，流程中存在的缺口便可能打开重要资源或持卡人数据的访问通道。
12.5.1 制定、记录和分发安全政策与程序。	**12.5.1** 确认已正式分配制定、记录和分发安全政策与程序的职责。	
12.5.2 监控和分析安全警报与信息，并分发给相应人员。	**12.5.2** 确认已正式分配安全警报的监控和分析职责，以及向适当的信息安全与业务部门管理人员分发信息的职责。	
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。	**12.5.3** 确认已正式分配建立、记录并分发安全事故响应和逐级上报程序的职责。	
12.5.4 管理用户帐户，包括添加、删除和修改	**12.5.4** 确认已正式分配用户帐户管理（添加、删除和修改）和验证管理的职责。	
12.5.5 监控并控制所有数据访问。	**12.5.5** 确认已正式分配监控并控制所有数据访问的职责。	
12.6 实施正式的安全意识计划，使所有工作人员意识到持卡人数据安全的重要性。	**12.6.a** 审核安全意识计划，确认该计划使所有工作人员意识到持卡人数据安全的重要性。	如果不向工作人员传达安全责任，则错误或有意图的操作可能会导致已实施的安全保障和流程无效。
	12.6.b 检查安全意识计划程序和文档记录并执行以下操作：	
12.6.1 人员一经录用即进行培训，此后每年至少培训一次。 ***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。*	**12.6.1.a** 确认安全意识计划提供多种传达意识和教授工作人员的方法（例如，海报、信函、备忘录、基于网络的培训、会议和宣传）。	如果安全意识计划不提供定期复习课程，工作人员便可能会遗忘或绕过关键安全流程和程序，从而导致重要资源和持卡人数据暴露。
	12.6.1.b 确认人员一经录用即参加安全意识培训且此后每年至少参加一次。	

PCI DSS 要求	测试程序	指南
	12.6.1.c 抽样选取部分工作人员进行面谈，确认他们已完成安全意识培训且意识到持卡人数据安全的重要性。	
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。	**12.6.2** 确认安全意识计划规定工作人员以手写或电子形式每年至少确认一次自己已阅读并了解信息安全政策。	要求工作人员以手写或电子形式进行确认有助于确保他们已阅读并了解安全政策/程序，且已经并将继续致力于遵守这些政策。
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。） ***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。*	**12.7** 咨询人力资源部管理层并确认在录用可访问持卡人数据或持卡人数据环境的工作人员之前已对其实施背景调查（符合当地的法律规定的前提下）。	在录用预计可访问持卡人数据的工作人员之前对其实施彻底的背景调查，可降低有可疑背景或犯罪背景的个人对 PAN 和其他持卡人数据进行非授权使用的风险。
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：	**12.8** 通过查看并审核政策、程序和支持文档记录，确认已通过实施流程来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（例如，备份磁带存储机构、网络托管公司或安全服务提供商等托管服务提供商、接收数据来分析欺诈建模的公司等），具体方式如下：	如果商户或服务提供商与其他服务提供商共享持卡人数据，则应实施某些要求，确保此类服务提供商持续保护该数据。
12.8.1 保留一份服务提供商名单。	**12.8.1** 确认已保留一份服务提供商名单。	跟踪记录所有服务提供商可确定潜在风险在组织外部的延伸方向。
12.8.2 要求服务提供商出具书面协议，确认其负责维护所持有的持卡人数据，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，或在可能影响持卡人数据环境安全性的程度内维护数据安全，并保留此协议。 ***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。*	**12.8.2** 查看书面协议并确定服务提供商确认其负责维护所持有的持卡人数据，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，或在可能影响持卡人数据环境安全性的程度内维护数据安全。	服务提供商所做的确认证明他们会致力于维护从客户处获取的持卡人数据的适当安全。 本要求涉及组织与服务提供商之间的书面协议，与要求 12.9 结合使用，旨在促进双方对其相应的 PCI DSS 责任达成一致理解。例如，协议可能包括维护适用的 PCI DSS 要求，作为所提供服务的一部分。

PCI DSS 要求	测试程序	指南
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）。	**12.8.3** 确认已记录并实施此政策和程序（包括雇用任何服务提供商之前相应的尽职调查）。	本流程可确保在雇用任何服务提供商时均经过组织内部的全面审核，包括在与服务提供商建立正式关系之前执行风险分析。 每个组织具体的尽职调查流程和目标均不同。需要考虑的内容包括提供商的报告惯例、漏洞通知和事故响应程序、为双方分配 PCI DSS 责任的详细方法、提供商验证其 PCI DSS 遵从性的方法以及他们提供的证据等。
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。	**12.8.4** 确认组织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。	了解服务提供商的 PCI DSS 遵从性状态可确保他们遵守，并了解他们是否遵守与您的组织相同的要求。如果服务提供商提供的服务种类繁多，则本要求应适用于提供给客户的服务以及在客户 PCI DSS 评估范围内的服务。 实体所维护的具体信息取决于他们与提供商之间的特定协议、服务的类型等。这样做是为了让所评估的实体理解其提供商已经同意满足哪些 PCI DSS 要求。
12.8.5 维护涉及分别由各个服务提供商和实体管理的 PCI DSS 要求的信息。	**12.8.5** 确认实体维护涉及分别由各个服务提供商和实体管理的 PCI DSS 要求的信息。	
12.9 *针对服务提供商的额外要求*：服务提供商以书面形式向客户确认其负责维护所持有的持卡人数据，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，或在可能影响持卡人数据环境安全性的程度内维护数据安全。 ***注：****本要求在 2015 年 6 月 30 日前属于最优方法，此后将成为一项要求。* ***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。* *仅当评估对象为服务提供商时，本要求才适用。*	**12.9.1** 审核服务提供商的政策和程序并查看书面协议模板，确认服务提供商以书面形式向客户确认他们会维护所有适用的 PCI DSS 要求，包含处理、访问或以其他方式存储、处理或传输客户的持卡人数据或敏感验证数据，或者代表客户管理其持卡人数据环境。	本要求适用于所评估的实体为服务提供商时的情况。本要求与要求 12.8.2 结合使用，旨在促进服务提供商及其客户对各自相应的 PCI DSS 责任达成一致理解。服务提供商所做的确认证明他们会致力于维护从客户处获取的持卡人数据的适当安全。 服务提供商应与客户就提供书面确认的方法达成一致。
12.10 实施事故响应计划。随时准备立即响应系统漏洞。	**12.10** 检查事故响应计划和相关程序，确认实体通过执行以下操作随时准备立即响应系统漏洞：	如果没有全面的安全事故响应计划或相关方未正确传播、阅读和理解计划，对于响应计划的困惑和统一响应的缺乏会导致日后生产停工、不必要的公共媒体曝光以及新的法律责任。

PCI DSS 要求	测试程序	指南
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： ▪ 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	**12.10.1.a** 确认事故响应计划包括： ▪ 出现威胁时的角色、责任以及沟通策略，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（例如，“加州参议院第 1386 号法案”要求，数据库中有加州居民资料的任何公司在发现实际威胁或怀疑出现威胁时都应通知受影响的消费者） ▪ 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	事故响应计划应全面且包含所有关键因素，这样您的公司才能在出现影响持卡人数据的漏洞时作出有效响应。
	12.10.1.b 从之前报告的事故或警报中选取样本，与工作人员面谈并查看文档记录，确认已遵循书面事故响应计划和程序。	
12.10.2 至少每年测试一次计划。	**12.10.2** 确认至少每年测试一次计划。	若不进行恰当的测试，则可能会漏掉关键步骤并导致事故中的曝光度增加。
12.10.3 指定可全天候响应警报的特定人员。	**12.10.3** 查看、审核政策并与负责人员面谈，确认有指定人员可全天候响应事故并通过监控来找出非授权活动的证据、检测非授权无线接入点、关键 IDS 警报和/或涉及关键系统或内容文件非授权变更的报告。	如果没有一支受过培训且随时准备响应的事故响应团队，则网络可能会受到更大的损害，且关键数据和系统可能会因对目标系统的不恰当处理而受到“污染”。这会妨碍事后调查的顺利进行。
12.10.4 为具有安全漏洞响应责任的员工提供恰当的培训。	**12.10.4** 查看、审核政策并与负责人员面谈，确认已定期培训有安全漏洞响应责任的工作人员。	
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。	**12.10.5** 查看并审核流程，确认“事故响应计划”包含了监控并响应来自安全监控系统（包括检测非授权无线接入点）的警报。	这些监控系统旨在关注数据的潜在风险，对于快速采取措施预防漏洞至关重要，且必须包含在事故响应流程中。
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。	**12.10.6** 查看、审核政策并与负责人员面谈，确认已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。	事故发生后在事故响应计划中添加“经验教训”有助于保持计划为最新并应对新的威胁和安全趋势。

附录 A：针对共享托管服务提供商的 PCI DSS 附加要求

要求 A.1：共享托管服务提供商必须保护持卡人数据环境

根据要求 12.8 和 12.9 中的规定，所有有权访问持卡人数据的服务提供商（包括共享托管服务提供商）均必须遵守 PCI DSS。另外，要求 2.6 指出共享托管服务提供商必须保护每个实体的托管环境和数据。因此，共享托管服务提供商还必须遵守本附录中的要求。

要求	测试程序	指南
A.1 根据 A.1.1 至 A.1.4，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： 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。 ***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。如果适用，每个实体均必须遵守 PCI DSS 并验证其遵从性。*	**A.1** 尤其在对共享托管服务提供商进行 PCI DSS 评估时，若要确认共享托管服务提供商确实会保护实体（商户和服务提供商）的托管环境和数据，请从托管商户和服务提供商的代表性样本中选择部分服务器（Microsoft Windows 和 Unix/Linux）并执行以下 A.1.1 到 A.1.4 的操作：	PCI DSS *附录 A* 针对希望为其商户和/或服务提供商客户提供符合 PCI DSS 要求的托管环境的共享托管服务提供商而设计。
A.1.1 确保每个实体仅运行可访问自身持卡人数据环境的流程。	**A.1.1** 如果共享托管服务提供商允许实体（例如，商户或服务提供商）运行自己的应用程序，请确认使用该实体的唯一 ID 来运行这些应用程序流程。例如： • 系统中的任何实体均不得使用共享的网络服务器用户 ID。 • 实体使用的所有 CGI 脚本必须作为该实体的唯一用户 ID 创建和运行。	如果商户或服务提供商获准在共享服务器上运行自己的应用程序，则这些应用程序应使用商户或服务提供商的用户 ID 而非作为特权用户运行。
A.1.2 每个实体的访问权限和特权仅限自身的持卡人数据环境。	**A.1.2.a** 确认任何应用程序流程的用户 ID 均不属于特权用户（root 权限/管理员权限）。	为确保每个商户或服务提供商的访问权限和特权限制为只能访问自己的环境，请考虑以下内容：(1) 商户或服务提供商的网络服务器用户 ID 的权限；(2) 授予读取、写入和执行文件的权限；(3) 授予写入系统二进制文件的权限；(4) 授予商户和服务提供商日志文件的权限；(5) 确保商户或服务提供商无法独占系统资源的控制措施。
	A.1.2.b 确认每个实体（商户、服务提供商）拥有的读取、写入或执行权限仅适用于其所属的文件或目录或者必要的系统文件（通过文件系统权限、访问控制列表、chroot 作业系统、jailshell 等加以限制）。 **注意：**实体的文件不能与群组共享。	
	A.1.2.c 确认实体用户没有共享系统二进制文件的写入权限。	
	A.1.2.d 确认只有拥有日志条目的实体才能查看这些条目。	

要求	测试程序	指南
	A.1.2.e 为确保各实体不会独占服务器资源从而利用漏洞（例如，错误、争用和重启会导致缓冲区溢出等情况），请确认已针对这些系统资源的使用制定相关限制： ▪ 磁盘空间 ▪ 带宽 ▪ 内存 ▪ CPU	
A.1.3 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唯一且符合 PCI DSS 要求 10。	**A.1.3** 确认共享托管服务提供商已按如下方式启用每个商户和服务提供商环境中的日志记录： 启用第三方常见应用程序的日志。 默认情况下，日志处于活动状态。 日志可供其所属实体审核。 日志位置已清楚传达给其所属实体。	应在共享托管环境中使用日志，这样商户和服务提供商便能访问并审核其持卡人数据环境特定的日志。
A.1.4 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。	**A.1.4** 确认共享托管服务提供商具备相关书面政策，可在出现威胁时针对相关服务器提供及时的取证调查。	共享托管服务提供商必须具备相关流程，可在需要对威胁进行取证调查时提供方便快捷的响应，至少应提供适度的细节以便了解个体商户和服务提供商的详细信息。

附录 B： 补偿性控制

当实体因合理的技术限制或书面业务限制无法满足明确指定的要求，但已通过实施其他措施或补偿性控制充分降低与该要求相关的风险时，大部分 PCI DSS 要求可能都需要考虑引入补偿性控制。

补偿性控制必须满足以下标准：

1. 符合最初 PCI DSS 要求的目的和严格程度。
2. 提供与最初 PCI DSS 要求相似的防御级别，使补偿性控制能充分抵消最初 PCI DSS 要求旨在防御的风险。（请参阅 *PCI DSS 导航*，了解每条 PCI DSS 要求的目的。）
3. “超越”其他 PCI DSS 要求。（仅仅只是遵循其他 PCI DSS 要求并不构成补偿性控制。）

   评估补偿性控制的“超越”部分时，请考虑以下各项：

注：*以下从 a) 到 c) 的各项为示例，仅供参考。所有补偿性控制都必须由执行 PCI DSS 审核的评估商审核并验证其充分性。补偿性控制的有效性取决于实施控制的具体环境、相关的安全控制以及控制配置。公司应了解特定的补偿性控制并非在所有环境下均有效。*

a) 如果受审核的项目需要用到现有的 PCI DSS 要求，则不能将该要求视为补偿性控制。例如，非控制台管理访问的密码在发送时必须进行加密，从而降低明文管理密码遭到拦截的风险。实体不得使用其他 PCI DSS 密码要求（入侵者锁定、复杂密码等） 来补偿缺失的加密密码，因为此类密码要求不会降低明文口令遭到拦截的风险。而且，其他密码控制已经是受审核项目（密码）的 PCI DSS 要求。

b) 如果其他领域需要而受审核项目不需要用到现有的 PCI DSS 要求，则可将该要求视为补偿性控制。例如，双因素验证是针对远程访问的 PCI DSS 要求。当不支持加密密码传输时，*来自内部网络的*双因素验证也可视为非控制台管理访问的补偿性控制。符合以下条件时，双因素验证是可接受的补偿性控制：(1) 通过解决明文管理密码遭到拦截的风险，满足最初要求的目的；(2) 在安全的环境中正确设置。

c) 现有的 PCI DSS 要求可结合新的控制措施成为补偿性控制。例如，如果某公司无法根据要求 3.4 使持卡人数据不可读（例如，通过加密），则补偿性控制可包括一个或多个设备、应用程序以及能处理以下各项的控制措施：(1) 内部网络分段；(2) IP 地址或 MAC 地址过滤；以及 (3) 来自内部网络的双因素验证。

4. 与不遵守 PCI DSS 要求导致的其他风险相称。

评估商必须根据上述 1-4 项在每次年度 PCI DSS 评估中全面评估补偿性控制，以验证每项补偿性控制都能充分解决最初 PCI DSS 要求旨在解决的风险。为保持遵从性，必须在评估完成后制定相应的流程和控制措施，以确保补偿性控制始终有效。

附录 C： 补偿性控制工作表

如果要采用补偿性控制来满足 PCI DSS 要求，请使用本工作表界定针对任何要求的补偿性控制。注意：补偿性控制也应记录在 PCI DSS 要求相应章节的《遵从性报告》中。

注：*只有已采取风险分析并具有合理的技术限制或书面业务限制的公司才能考虑使用补偿性控制来实现遵从性。*

要求编号和定义：

	所需信息	解释
1. 限制	列出导致无法遵守最初要求的限制。	
2. 目的	定义最初控制的目的；确定通过补偿性控制实现的目的。	
3. 已确定的风险	确定由于缺少最初控制而导致的任何其他风险。	
4. 补偿性控制的定义	定义补偿性控制并解释其如何实现最初控制的目的并解决增加的风险（若有）。	
5. 补偿性控制的验证	定义如何验证并测试补偿性控制。	
6. 维护	规定流程和控制措施以维护补偿性控制。	

补偿性控制工作表 - 完整示例

利用本工作表为通过补偿性控制备注为"到位"的任何要求定义补偿性控制。

要求编号：*8.1.1 - 在允许任何用户访问系统组件或持卡人数据前，是否为他们分配了唯一的用户 ID？*

	所需信息	解释
1. 限制	列出导致无法遵守最初要求的限制。	*XYZ 公司使用无 LDAP 的独立 Unix 服务器。因此，每个用户都需要"root"登录。XYZ 公司不可能管理"root"登录，也无法记录每个用户的所有"root"活动。*
2. 目的	定义最初控制的目的；确定通过补偿性控制实现的目的。	*要求唯一登录具有双重目的。首先，从安全角度来看，不应该共享登录凭证。其次，使用共享登录无法明确指出特定操作的具体负责人。*
3. 已确定的风险	确定由于缺少最初控制而导致的任何其他风险。	*如果无法确保所有用户均有可跟踪的唯一 ID，则会给访问控制系统带来其他风险。*
4. 补偿性控制的定义	定义补偿性控制并解释其如何实现最初控制的目的并解决增加的风险（若有）。	*XYZ 公司将要求所有用户使用"SU"（替代用户）命令从桌面登录服务器。这允许用户访问"root"帐户并在"root"帐户下执行操作，但其操作会记入 SU 日志目录中。因此，无需与用户共享"root"密码，即可通过 SU 帐户跟踪每个用户的操作 。*
5. 补偿性控制的验证	定义如何验证并测试补偿性控制。	*XYZ 公司向评估商证明已执行 SU 命令且已记录个人使用该命令执行的所有活动，以确定个人执行操作时使用的是 root 权限。*
6. 维护	规定流程和控制措施以维护补偿性控制。	*XYZ 公司会记录相关流程和程序以确保 SU 配置不会变更、更改或删除，进而允许个人用户无需经过单独识别、跟踪和记录便可执行 root 命令。*

附录 D： 网络分段与企业设施/系统组件抽样