Payment Card Industry
数据安全标准

要求及测试程序

4.0 版

2022 年 3 月

文件变更

日期	版本	说明
2008 年 10 月	1.2	将 PCI DSS 1.2 版介绍为“PCI DSS 要求和安全评估程序”，消除了文件之间的冗余，并对 PCI DSS 安全审核程序 1.1 版进行了一般和具体修改。如需完整信息，请参见 PCI 数据安全标准 1.1 版至 1.2 版的变更摘要。
2009 年 7 月	1.2.1	添加 PCI DSS 1.1 版和 1.2 版之间被错误删除的句子。
		将测试程序 6.3.7.a 和 6.3.7.b 中的“then（然后）”更正为“than（比）”。
		移除测试程序 6.5.b 中“in place（到位）”和“not in place（未到位）”列的灰色标记。
		对于补偿性控制工作表 - 已完成的示例，将页面顶部的措辞更正为：“使用本工作表为任何通过补偿性控制指出为“到位”的要求确定补偿性控制。”
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 版至 2.0 版的变更摘要。
2013 年 11 月	3.0	更新于 2.0 版。请参阅 PCI DSS – PCI DSS 2.0 版至 3.0 版的变更摘要。
2015 年 4 月	3.1	更新于 PCI DSS 3.0 版。有关变更详情，请参阅 PCI DSS - PCI DSS 3.0 版至 3.1 版的变更摘要。
2016 年 4 月	3.2	更新于 PCI DSS 3.1 版。有关变更详情，请参阅 PCI DSS - PCI DSS 3.1 版至 3.2 版的变更摘要。
2018 年 5 月	3.2.1	更新于 PCI DSS 3.2 版。有关变更详情，请参阅 PCI DSS – PCI DSS 3.2 版至 3.2.1 版的变更摘要。
2022 年 3 月	4.0	将文件名称改为"支付卡行业数据安全标准：要求及测试程序"。 更新于 PCI DSS v3.2.1。要了解变更详情，请参阅 PCI DSS - PCI DSS 3.2.1 版至 4.0 版的变更摘要。

确认通知：在所有使用目的和情况下，PCI SSC 网站上的英文文本应作为此文件的官方版本。当翻译文本和英文文本之间出现任何歧义和不一致之处时，正确的内容应以该位置的英文文本为准。

目录

1 导言和 PCI 数据安全标准概述

制定支付卡行业数据安全标准（PCI DSS）是为了鼓励和加强支付卡帐户数据的安全性，并促进全球广泛采用一致的数据安全措施。PCI DSS 提供了一个旨在保护帐户数据的技术和操作要求的基线。虽然 PCI DSS 专门为关注支付卡帐户数据的环境而设计，但也可以用来保护支付生态系统中的其他元素免受威胁和安全。

表 1 显示了 12 项主要的 PCI DSS 要求。

表 1。主要 PCI DSS 要求

PCI 数据安全标准 - 高级别概述	
建立和维护安全网络和系统	**1.** 安装和维护网络安全控制。 **2.** 安全配置应用于所有系统组件。
保护帐户数据	**3.** 保护所存储帐户数据。 **4.** 在开放的公共网络上传输过程中使用强效加密法保护持卡人数据。
维护漏洞管理计划	**5.** 保护所有系统和网络免受恶意软件侵害。 **6.** 开发和维护安全系统和软件。
实施强有力的访问控制措施	**7.** 根据“必须知道”原则限制系统组件和持卡人数据的访问权限。 **8.** 识别用户并验证系统组件的访问权限。 **9.** 限制持卡人数据的实体访问权限。
定期监控和测试网络	**10.** 记录并监控系统组件和持卡人数据的所有访问权限。 **11.** 定期测试系统和网络的安全性。
维护信息安全政策	**12.** 使用组织政策和计划支持信息安全。

本文件《支付卡行业数据安全标准要求和测试程序》由 12 项 PCI DSS 主要要求、详细的安全要求、相应的测试程序以及与每个要求相关的其他信息组成。以下章节提供了详细的指导方针和最佳实践，以帮助各实体准备、实施和报告 PCI DSS 评估的结果。PCI DSS 要求和测试程序始于第 40 页。

PCI DSS 包括一套保护帐户数据的最低要求，并可能通过额外的控制和实践来加强，以进一步降低风险，并纳入当地、区域和部门的法律和法规。此外，立法或监管要求可能要求对个人信息或其他数据元素（例如，持卡人姓名）进行特别保护。

限制条件

如果本标准中的任何要求与国家、州或地方法律相冲突，则适用国家、州或地方法律。PCI DSS 资源

PCI 安全标准委员会（PCI SSC）网站（www.pcisecuritystandards.org）提供了以下额外资源，以协助组织进行 PCI DSS 评估和认证；

- 文件库，包括：
  - *PCI DSS* 变更摘要
  - PCI DSS 快速参考指南
  - 信息补充和指南
  - PCI DSS 的优先处理方法
  - 遵从性报告（ROC）报告模板和报告说明
  - 自我评估调查问卷（SAQ）和 SAQ 说明和指南
  - 遵从性测试（AOC）
- 常见问题解答（FAQ）
- 小商户网站的 PCI
- PCI 培训课程和信息网络研讨会

- 合格安全性评估商（QSA）和授权扫描服务商名单（ASV）
- PCI 批准的设备、应用程序和解决方案的清单

PCI SSC 网站上有 60 多份指导文件和信息补充，为 PCI DSS 提供具体的指导和注意事项。示例包括：

- PCI DSS 范围界定和网络分段指南
- PCI SSC 云计算指南
- 多因素验证指南
- 第三方安全保证
- 有效的日常日志监控
- 穿透测试指南
- 实施安全意识计划的最佳做法
- 维护 PCI DSS 遵从性的最佳做法
- 大型机构的 PCI DSS
- 使用 SSL/早期 TLS 和对 ASV 扫描的影响
- 使用 SSL/早期 TLS 进行 POS POI 终端连接
- 令牌化产品安全指南
- 保护基于电话的支付卡数据

注：信息补充是对 PCI DSS 的补充，并确定了满足 PCI DSS 要求的额外注意事项和建议。信息补充不会取代、替代或扩展 PCI DSS 或其任何要求。

如需这些信息和其他资源，请参考文件库：www.pcisecuritystandards.org。

此外，请参阅附录 G 了解 PCI DSS 术语的定义。

2 PCI DSS 适用性信息

PCI DSS 适用于所有存储、处理或传输持卡人数据（CHD）和/或敏感验证数据（SAD）或可能影响持卡人数据环境（CDE）安全性的实体。这包括所有参与支付卡帐户处理的实体—包括商户、处理商、收单机构、发卡机构和其他服务提供商。

是否要求任何实体遵守或认证其是否遵从 PCI DSS 的要求，由管理遵从性计划的组织（例如支付品牌和收单机构）自行决定。要了解任何额外标准，请联系相关组织。

确定帐户数据、持卡人数据和敏感验证数据

持卡人数据和敏感验证数据被视为帐户数据，确定方式如下：

表 2。帐户数据

帐户数据	
持卡人数据包括：	**敏感验证数据包括：**
• 主帐户号（PAN） • 持卡人姓名 • 到期日 • 业务码	• 全磁道数据（磁条数据或芯片上的同等数据） • 卡验证代码 • PIN/PIN 数据块

PCI DSS 要求适用于具有存储、处理或传输帐户数据（持卡人数据和/或敏感验证数据）环境的实体，以及具有可能影响 CDE 安全的环境的实体。一些 PCI DSS 要求也可能适用于拥有不存储、处理或传输帐户数据的环境的实体–例如，将其 CDE 1的支付操作或管理外包的实体。将其支付环境或支付操作外包给第三方的实体仍有责任确保第三方根据适用的 PCI DSS 要求保护账户数据。

主帐户号（PAN）是持卡人数据的决定因素。因此，帐户数据这一术语涵盖了以下内容：完整的 PAN、与 PAN 一起出现的任何其他持卡人数据元素，以及任何敏感验证数据元素。

如果持卡人姓名、业务码和/或到期日与 PAN 一起存储、处理或传输，或以其他方式出现在 CDE 中，则必须根据适用于持卡人数据的 PCI DSS 要求进行保护。

如果实体存储、处理或传输 PAN，则存在适用 PCI DSS 要求的 CDE。有些要求可能不适用，例如，如果该实体不存储 PAN，那么要求 3 中有关保护存储的 PAN 的要求将不适用于该实体。

即使实体不存储、处理或传输 PAN，一些 PCI DSS 要求仍可适用。请考虑以下情况：

- 如果该实体存储 SAD，要求 3 中专门与 SAD 存储有关的要求将适用。
- 如果该实体聘请第三方服务提供商代表其存储、处理或传输 PAN，则要求 12 中与服务提供商管理有关的要求将适用。
- 如果该实体可以影响 CDE 的安全，因为实体的基础设施的安全可以影响持卡人数据的处理方式（例如，通过控制生成支付表格或页面的网络服务器），则一些要求将适用。
- 如果持卡人数据只存在于物理介质（如纸张）上，则要求 9 中与物理介质的安全和处理有关的要求将适用。
- 与事件响应计划有关的要求适用于所有实体，以确保在怀疑或实际违反持卡人数据保密性的情况下有程序可循。

[1] 根据那些管理遵从性计划的组织（例如支付品牌和收单机构）；实体应联系相关组织以了解更多细节。

在 PCI DSS 中使用帐户数据、敏感验证数据、持卡人数据和主帐户号

PCI DSS 包括特别提到帐户数据、持卡人数据和敏感验证数据的要求。需要注意的是，这些类型的数据各不相同，这些术语不可互换使用。要求中对帐户数据、持卡人数据或敏感验证数据的具体引用是有明确目的的，并且要求特别适用于所引用的数据类型。

帐户数据的元素和存储要求

表 3 列出了持卡人和敏感验证数据的元素，每个数据元素的存储是否被允许或禁止，以及每个数据元素在存储时是否必须不可读—例如，使用强效加密法。本表并非详尽无遗，并且仅用于说明所述要求如何适用于不同的数据元素。

表 3。帐户数据元素存储要求

		数据元素	存储限制	要求使存储的数据不可读
帐户数据	持卡人数据	主帐户号（PAN）	根据要求 3.2 的规定，存储量保持在最低水平	是的，根据要求 3.5 的规定
		持卡人姓名	根据要求 3.2 的规定，存储量保持在最低水平[2]	没有
		业务码		
		到期日		
	敏感验证数据	全磁道数据	根据要求 3.3.1[3] 的规定，授权后无法存储。	对，在授权完成之前存储数据必须使用要求 3.3.2 中规定的强效加密法进行保护。
		卡验证代码		
		PIN/PIN 数据块		

如果 PAN 与持卡人数据的其他元素一起存储，根据 PCI DSS 要求 3.5.1，则必须只有使 PAN 不可读。

授权后不得存储敏感验证数据（即使是加密的验证数据）。这甚至适用于不存在 PAN 的环境。

[2] 当数据与 PAN 存在于同一环境中时。

[3]除发卡机构和支持发卡服务的公司所允许的情况外。要求 3.3.3 单独规定了发卡机构和发卡服务的要求。

3 PCI DSS 与 PCI SSC 软件标准之间的关系

PCI SSC 通过支付应用程序数据安全标准（PA-DSS）和软件安全框架（SSF）支持在持卡人数据环境（CDE）中使用安全支付软件，该框架由安全软件标准和安全软件生命周期（安全 SLC）标准组成。经过 PCI SSC 认证并列出的软件可以提供保证，该软件采用安全做法开发，并满足了一系列规定的软件安全要求。

PCI SSC 安全软件计划包括已被认证为符合适用的 PCI SSC 软件标准的支付软件和软件供应商的列表。

- **认证软件**：PCI SSC 网站上列出的支付软件是经过认证的支付应用程序（PA-DSS）或经过认证的支付软件（安全软件标准），已经由合格的评估商进行评估，以确认该软件符合该标准中的安全要求。这些标准中的安全要求着重于保护支付交易和帐户数据的完整性和保密性。
- **认证软件供应商**：安全 SLC 标准确定了软件供应商的安全要求，以在整个软件生命周期中整合安全软件开发实践。经过认证符合安全 SLC 标准的软件供应商在 PCI SSC 网站上被列为安全 SLC 合格的供应商。

注：PA-DSS 和相关计划将于 2022 年 10 月退役。关于 PA-DSS 认证应用程序的到期日，请参考 PCI SSC 认证支付应用程序列表。在到期日之后，应用程序被列为"仅可接受用于预设部署"。关于实体是否可以继续使用已过期列表的 PA-DSS 应用程序，由管理遵从性计划的组织（例如支付品牌和收单机构）自行决定；实体应联系相关组织以了解更多细节。

有关 SSF 或 PA-DSS 的更多信息，请参考各自的计划指南：www.pcisecuritystandards.org。

所有存储、处理或传输帐户数据的软件，或者可能影响帐户数据或 CDE 安全的软件，都在实体的 PCI DSS 评估范围内。虽然使用经过认证的支付软件支持实体 CDE 的安全，但使用这种软件本身并不能使实体符合 PCI DSS。该实体的 PCI DSS 评估应包括验证该软件是否正确配置并安全实施，以支持适用的 PCI DSS 要求。此外，如果已定制被列入 PCI 名单的支付软件，则在 PCI DSS 评估期间将需要进行更为深入的审核，因为该软件可能不再是最初认证的版本的代表。

由于安全威胁不断演变，不再受供应商支持的软件（例如，被供应商认定为"寿命结束"）可能无法提供与支持版本相同的安全水平。我们强烈建议各实体保持其软件的时效性，并更新到现有的最新软件版本。

我们鼓励自行开发软件的实体参考 PCI SSC 的软件安全标准，并将其中的要求作为最佳实践，用于其开发环境中。在符合 PCI DSS 的环境中实施的安全支付软件将有助于最大限度地减少导致帐户数据受到威胁和欺诈的安全漏洞的可能性。请参阅订制和定制软件。

PCI DSS 对支付软件供应商的适用性

如果支付软件供应商也是存储、处理或传输帐户数据的服务提供商，或者可以访问客户的帐户数据—例如，以支付服务提供商的身份或通过远程访问客户环境，则 PCI DSS 可能适用于该供应商。PCI DSS 可能适用的软件供应商包括那些提供支付服务的供应商，以及在云中提供支付终端、软件即服务（SaaS）、云中电子商务和其他云支付服务的云服务提供商。

订制和定制软件

所有存储、处理或传输帐户数据的订制和定制软件，或者可能影响帐户数据或 CDE 安全的软件，都在实体的 PCI DSS 评估范围内。

根据 PCI SSC 的软件安全框架标准（安全软件标准或安全 SLC 标准）之一开发和维护的订制和定制软件将支持实体满足 PCI DSS 要求 6。

有关详情，请参见附录 F。

注：PCI DSS 要求 6 完全适用于未按照 PCI SSC 的软件安全框架标准之一进行开发和维护的订制和定制软件。使用软件供应商开发可能影响帐户数据或其 CDE 安全性的订制和定制软件的实体，有责任确保这些软件供应商根据 PCI DSS 要求 6 开发软件。

4 PCI DSS 要求的范围

PCI DSS 要求适用于：

- 持卡人数据环境（CDE）由以下部分组成：
  - 存储、处理和传输持卡人数据和/或敏感验证数据的系统组件、人员和流程，和
  - 可能不存储、处理或传输 CHD/SAD 的系统组件，但它们可以不受限制地连接到那些存储、处理或传输 CHD/SAD 的系统组件。

和

- 可能影响 CDE 安全的系统组件、人员和流程。[4]

“系统组件”包括网络设备、服务器、计算设备、虚拟组件、云组件和软件。系统组件的包括但不限于：

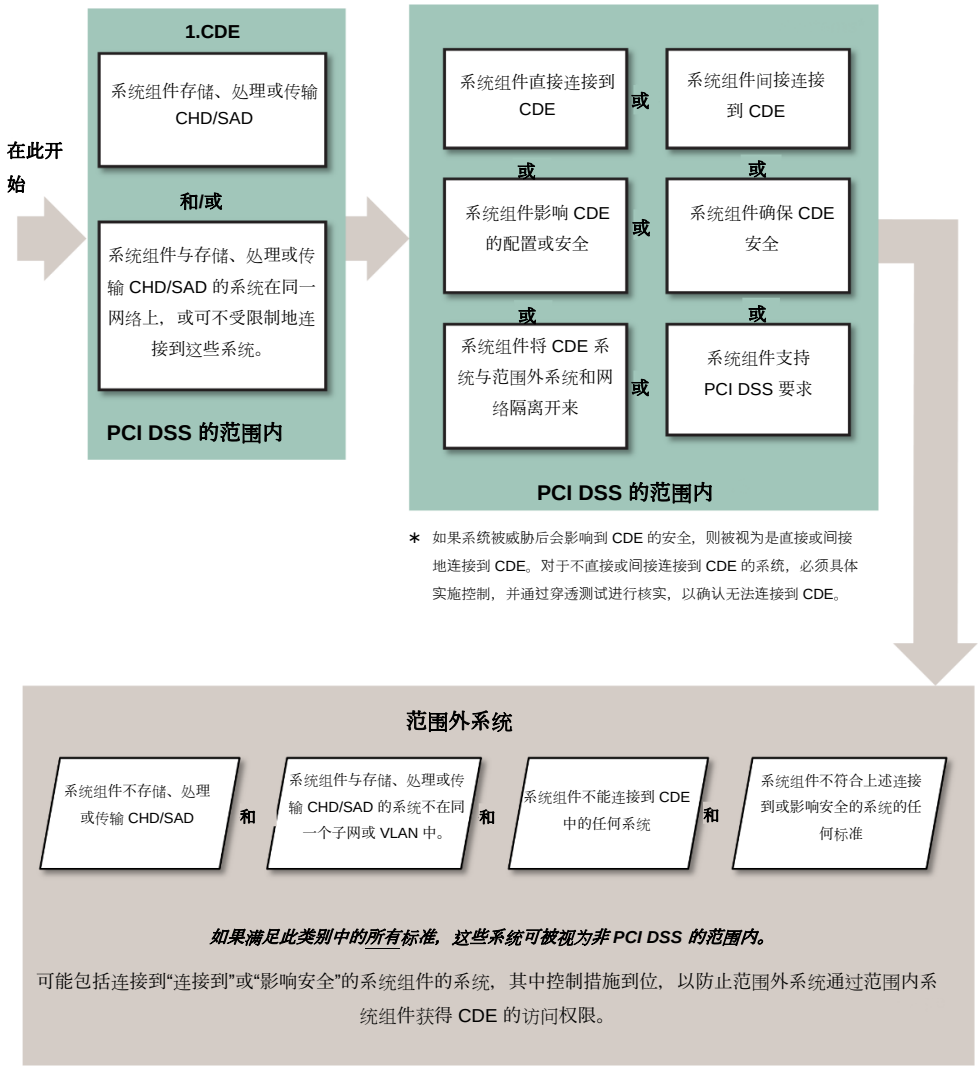
- 存储、处理或传输帐户数据的系统（例如，支付终端、授权系统、清算系统、支付中间件系统、支付后台系统、购物车和店面系统、支付网关/开关系统、欺诈监控系统）。
- 提供安全服务的系统（例如，验证服务器、访问控制服务器、安全信息和事件管理（SIEM）系统、物理安全系统（例如，标记访问或 CCTV）、多因素验证系统、反恶意软件系统）。
- 促进分段的系统（例如，内部网络安全控制）。
- 可能影响帐户数据或 CDE 安全的系统（例如，名称解析，或电子商务（网络）重定向服务器）。
- 虚拟化组件，例如虚拟机、虚拟交换机/路由器、虚拟设备、虚拟应用程序/桌面和虚拟机监视器。
- 云基础设施和组件，包括外部和内部，并包括容器或图像的实例、虚拟私有云、基于云的身份和访问管理、驻留在内部或云中的 CDE、带有容器化应用程序的 服务网格以及容器协调工具。

[4]有关其他指导，请参阅*信息补充：PCI SSC 网站上的*PCI DSS 范围界定和网络分段指南。

- 网络组件，包括但不限于网络安全控制、交换机、路由器、VoIP 网络设备、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）。
- 终端用户设备，例如计算机、笔记本、工作站、管理工作站、平板电脑和移动设备。
- 打印机，以及扫描、打印和传真的多功能设备。
- 任何格式的存储帐户数据（例如，纸质、数据文件、音频文件、图像和视频记录）。
- 应用程序、软件和软件组件、无服务器应用程序，包括所有购买的、订阅的（例如，软件即服务）、订制和定制软件，包括内部和外部（例如，互联网）应用程序。
- 实施软件配置管理的工具、代码库和系统，或用于将对象部署到 CDE 或可能影响 CDE 的系统。

图 1 显示了为 PCI DSS 界定系统组件范围的注意事项。

图 1。了解 PCI DSS 的范围界定



年度 PCI DSS 范围确认

准备进行 PCI DSS 评估的第一步是实体准确地确定审核的范围。被评估实体必须根据 PCI DSS 要求 12.5.2 确认其 PCI DSS 范围的准确性，确定帐户数据的所有位置和流向，并确定所有连接到 CDE 的系统，或者如果被威胁，可能影响 CDE 的系统（例如，验证服务器、远程访问服务器、日志服务器），以确保它们被纳入 PCI DSS 范围内。在范围界定过程中应考虑所有类型的系统和地点，包括备份/恢复站点和故障转移系统。

PCI DSS 要求 12.5.2 中规定了实体确认其 PCI DSS 范围准确性的最少步骤。该实体应保留文件，以显示 PCI DSS 范围的确定方式。保留该文件供评估商审核，并在实体的下一次 PCI DSS 范围确认活动中用作参考。对于每一次 PCI DSS 评估，评估商都要认证该实体是否准确确定并记录了评估的范围。

注：*PCI DSS 要求 12.5.2 规定了该年度 PCI DSS 范围确认，是实体应该执行的活动。该活动不同于实体的评估商在评估期间执行的范围界定确认，也不打算被其取代。*

分段

将 CDE 与实体网络的其余部分分段（或隔离），并不是 PCI DSS 的要求。但是，我们强烈建议采用这种方法，因为它可以减少：

- PCI DSS 评估的范围
- PCI DSS 评估的成本
- 实施和维护 PCI DSS 控制的成本和难度
- 组织相对于支付卡帐户数据的风险（通过将该数据合并到更少、更多的控制地点来减少）

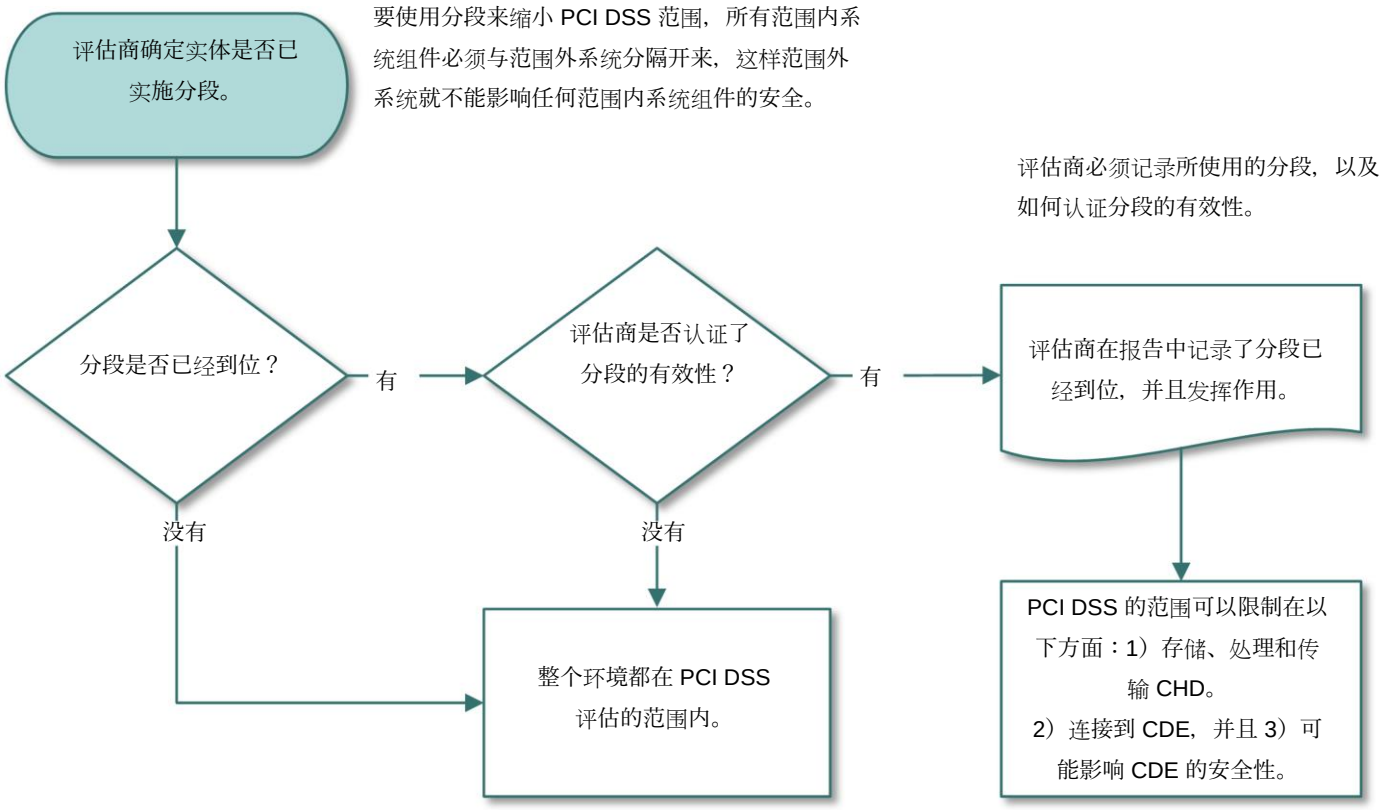
如果分段不充分（有时称为“扁平网络”），整个网络都在 PCI DSS 评估的范围内。可以通过一些物理或逻辑方法来实现分段，例如正确配置的内部网络安全控制、具有强大访问控制列表的路由器，或其他限制网络特定分段的访问权限的技术。要被视为非 PCI DSS 范围，系统组件必须与 CDE 适当分段（隔离），这样，即使该组件被威胁，非范围系统组件也不会影响 CDE 的安全。

缩小 CDE 范围的一个重要前提是清楚了解与帐户数据的存储、处理和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，将帐户数据限制在尽可能少的位置，可能需要对长期存在的业务实践进行重新设计。

通过数据流程图记录帐户数据流有助于实体充分了解帐户数据如何进入组织，它在组织内的位置，以及它如何在组织内各个系统中穿行。数据流程图还显示了存储、处理和传输帐户数据的所有位置。这些信息支持实施分段的实体，也可以支持确认分段用于将 CDE 与非范围网络隔离开来。

如果分段用于减少 PCI DSS 评估的范围，评估商必须核实分段是否足以减少评估的范围，如图 2 所示。在高层次上，适当分段将存储、处理或传输帐户数据的系统与不存储、处理或传输帐户数据的系统隔离开来。然而，一个特定分段实施的充分性是高度可变的，并取决于几个因素，例如一个特定的网络配置、部署的技术和其他可能实施的控制。

图 2。分段和对 PCI DSS 范围的影响



无线技术

如果无线技术用于存储、处理或传输帐户数据（例如，无线销售点设备），或者如果无线局域网（WLAN）是 CDE 的一部分或连接到 CDE，则适用并必须执行 PCI DSS 关于保护无线环境的要求和测试程序。

即使在 CDE 中不使用无线技术，并且实体有禁止在其环境中使用无线技术的政策，也必须根据 PCI DSS 要求 11.2.1 执行非法无线检测。这是因为无线接入点可以轻松地连接到网络上，很难检测到它的存在，以及未经授权的无线设备带来的风险增大。

在实施无线技术之前，实体应该仔细评估对该技术的需求和风险。考虑只将无线技术部署在非敏感数据的传输上。

加密持卡人数据和对 PCI DSS 范围的影响

根据 PCI DSS 要求 3.5，使用强效加密法对持卡人数据进行加密是一种可接受的使数据不可读的方法。然而，仅靠加密通常不足以使持卡人数据不在 PCI DSS 的范围内，也不能消除该环境中对 PCI DSS 的需求。由于持卡人数据的存在，该实体的环境仍在 PCI DSS 的范围内。例如，在商户实体支付卡交易环境中，可以实际接触到支付卡以完成交易，还可能有包含持卡人数据的纸质报告或收据。同样，在商户虚拟支付卡交易环境中，例如邮购/电话订购和电子商务，支付卡的详细信息通过渠道提供，需要根据 PCI DSS 进行评估和保护。

以下各项均在 PCI DSS 的范围内：

- 执行持卡人数据加密和/或解密的系统，以及执行密钥管理功能的系统。
- 未与加密和解密以及密钥管理流程隔离开来的加密持卡人数据。
- 加密持卡人数据存在于同时包含解密密钥的系统或媒体上，
- 与解密密钥存在于同一环境中的加密持卡人数据，
- 加密持卡人数据可以被一个同时拥有解密钥匙的实体所访问。

注：*列入 PCI 的 P2PE 解决方案可以显著减少适用于商户的持卡人数据环境的 PCI DSS 要求的数量。但是，它并不能完全消除 PCI DSS 在商户环境中的适用性。*

加密持卡人数据和对第三方服务提供商的 PCI DSS 范围的影响

如果第三方服务提供商（TPSP）只接收和/或存储由另一实体加密的数据，并且他们无法解密数据，那么如果满足某些条件，TPSP 可能会认为加密数据不在范围之内。这是因为数据的责任通常由有能力解密数据或影响加密数据安全的一个或多个实体承担。确定哪一方对特定的 PCI DSS 控制负责，将取决于几个因素，包括谁可以访问解密密钥，每一方履行的角色，以及各方之间的协议。应该明确规定和记录责任，以确保 TPSP 和提供加密数据的实体都了解哪个实体负责哪些安全控制。

举个例子，一个提供存储服务的 TPSP 接收并存储客户提供的加密持卡人数据用于备份目的。该 TPSP 没有加密或解密密钥的访问权限，也不为其客户进行任何密钥管理。TPSP 在确定其 PCI DSS 范围时可以排除任何此类加密数据。然而，作为其与客户签订的服务协议的一部分，TPSP 确实有责任控制加密数据存储的访问权限。

确保根据适用的 PCI DSS 要求保护加密数据和加密密钥的责任通常由实体之间共享。在上述例子中，客户决定其哪些人员被授权访问存储介质，而存储设施则负责管理物理和/或逻辑访问控制，以确保只有客户授权的人员才能获得存储介质的访问权限。适用于 TPSP 的具体 PCI DSS 要求将取决于所提供的服务和双方之间的协议。在提供存储服务的 TPSP 的示例中，TPSP 提供的物理和逻辑访问控制将需要至少每年审核一次。这种审核可以作为商户的 PCI DSS 评估的一部分来执行，或者，审核可以由 TPSP 执行，控制也可以由 TPSP 认证，并向商户提供适当证据。有关"适当证据"的信息，请参阅 *TPSP 的选择：认证符合客户 PCI DSS 要求的 TPSP 服务是否遵从 PCI DSS*。

再举一个例子，TPSP 只接收加密持卡人数据，用于路由到其他实体，并且没有数据或密钥的访问权限，可能对该加密数据不承担任何 PCI DSS 责任。在这种情况下，TPSP 不提供任何安全服务或访问控制，他们可能被视为与公共或不信任网络相同，因此，通过 TPSP 的网络发送/接收帐户数据的实体有责任确保应用 PCI DSS 控制来保护传输的数据。

使用第三方服务供应商

实体（在本节中称为"客户"）可能会选择使用第三方服务提供商（TPSP）来存储、处理或传输帐户数据，或代表客户管理范围内系统组件。使用 TPSP 可能会对客户的 CDE 安全产生影响。

***注：**使用符合 PCI DSS 的 TPSP 并不能使客户符合 PCI DSS，也不能免除客户对其自身 PCI DSS 遵从性的责任。即使客户使用 TPSP 来满足所有帐户数据功能，该客户仍然有责任按照管理遵从性计划的组织（例如，支付品牌和收单机构）的要求确认其自身的遵从情况。客户应联系相关组织了解任何要求。*

使用 TPSP 和对客户满足 PCI DSS 要求 12.8 的影响

在许多不同的情况下，客户可能使用一个或多个 TPSP 来实现客户 CDE 内或相关的功能。在使用 TPSP 的所有情况下，客户必须根据要求 12.8 管理和监督其所有 TPSP 的 PCI DSS 遵从性状态，包括 TPSP：

- 可以访问客户的 CDE。
- 代表客户管理范围内系统组件，和/或
- 能影响客户 CDE 的安全。

根据要求 12.8 管理 TPSP，包括进行尽职调查，制定适当协议，确定哪些要求适用于客户，哪些要求适用于 TPSP，并至少每年监测 TPSP 的遵从性状态。

要求 12.8 没有规定客户的 TPSP 必须符合 PCI DSS，只是要求客户按照要求中的规定监控其遵从性状态。因此，TPSP 无需符合 PCI DSS 即可使其客户满足要求 12.8。

TPSP 用于满足客户 PCI DSS 要求的服务的影响

当 TPSP 代表客户提供符合 PCI DSS 要求的服务，或者该服务可能影响客户 CDE 的安全性时，那么这些要求就在客户的评估范围内，该服务的遵从性将影响客户的 PCI DSS 遵从性。TPSP 必须证明其符合适用的 PCI DSS 要求，才能为其客户实施这些要求。例如，如果一个实体聘请 TPSP 来管理其网络安全控制，而 TPSP 没有提供证据证明它符合 PCI DSS 要求 1 中的适用要求，那么这些要求对客户的评估是未到位的。再举一个例子，代表客户存储持卡人数据备份的 TPSP 需要满足与访问控制、物理安全等相关的适用要求，以便其客户在评估时考虑这些要求。

了解 TPSP 客户和 TPSP 之间责任的重要性

客户和 TPSP 应该清楚地识别和理解以下内容：

- 包括在 TPSP 的 PCI DSS 评估范围内的服务和系统组件。
- TPSP 的 PCI DSS 评估所涵盖的特定 PCI DSS 要求和子要求。
- 任何由 TPSP 的客户负责、纳入其自身 PCI DSS 评估中的要求，以及
- 任何由 TPSP 和其客户共同负责的 PCI DSS 要求。

例如，云提供商应明确界定其哪些 IP 地址作为其季度漏洞扫描过程的一部分进行扫描，哪些 IP 地址是其客户的责任。

根据要求 12.9.2，TPSP 需要支持其客户关于 TPSP 提供给客户的服务相关的 PCI DSS 遵从性状况的信息请求，以及哪些 PCI DSS 要求是 TPSP 的责任，哪些是客户的责任，以及哪些是客户和 TPSP 之间的责任。有关责任矩阵模板，请参考了解 *PCI DSS 4.0 版的提示和工具*。该模板可用于记录和澄清 TPSP 和客户之间如何分担责任。

TPSP 的选择：认证符合客户 PCI DSS 要求的 TPSP 服务是否遵从 PCI DSS。

TPSP 负责按照管理遵从性计划的组织（例如，支付品牌和收单机构）的要求，展示其 PCI DSS 遵从性。TPSP 应联系相关组织了解任何要求。

当 TPSP 提供的服务旨在满足或促进满足客户的 PCI DSS 要求，或可能影响客户 CDE 的安全性时，这些要求都在客户的 PCI DSS 评估范围内。在这种情况下，TPSP 有两种选择来认证遵从性：

- **年度评估**：TPSP 接受年度 PCI DSS 评估，并向其客户提供证据，表明 TPSP 符合适用的 PCI DSS 要求；或
- **多项按需评估**：如果 TPSP 不进行年度 PCI DSS 评估，它必须在其客户的要求下进行评估，并且/或者参与其客户的每项 PCI DSS 评估，并将每次审核的结果提供给各自的客户。

如果 TPSP 接受了其自身的 PCI DSS 评估，它应该向其客户提供足够的证据，以核实 TPSP 的 PCI DSS 评估的范围涵盖了适用于客户的服务，并且相关的 PCI DSS 要求已被审查并确定到位。如果供应商持有 PCI DSS 遵从性证明（AOC），TPSP 必须应要求向客户提供 AOC。客户还可以要求 TPSP 的 PCI DSS 遵从性报告（ROC）的相关部分。可以编辑 ROC 来保护任何机密信息。

如果 TPSP 没有接受其自身的 PCI DSS 评估，因此没有 AOC，TPSP 应该提供与适用的 PCI DSS 要求有关的明确证据，以便客户（或其评估商）能够确认 TPSP 是否符合这些 PCI DSS 要求。

TPSP 列入支付品牌的 PCI DSS 合规服务供应商名单

对于根据要求 12.8 监控 TPSP 遵从性状态的客户来说，TPSP 列入支付品牌的 PCI DSS 合规服务提供商名单上***可能是 TPSP 遵从性状态的充分证据***-如果从名单上可以清楚地看到，TPSP 的 PCI DSS 评估覆盖了适用于客户的服务。如果从清单上无法清楚地看到，客户应该获得其他书面确认，以解决 TPSP 的 PCI DSS 遵从性状态。

对于寻找 PCI DSS 遵从性证据的客户来说，如果 TPSP 代表客户满足要求，或者所提供的服务会影响客户 CDE 的安全，则 TPSP 列入支付品牌的 PCI DSS 合规服务提供商名单上，***并不能充分证明***该 TPSP 的适用 PCI DSS 要求被纳入评估。如果 TPSP 具有 PCI DSS AOC，则应根据要求将其提供给客户。

5 实施 PCI DSS 到正常业务过程的最佳做法

作为其整体安全战略的一部分，实施业务正常流程（又称 BAU）的实体正在采取措施，确保为保护数据和环境而实施的安全控制措施继续正确实施，并在正常业务过程中正常运作。

一些 PCI DSS 要求旨在作为 BAU 流程，通过监控安全控制来确保其持续有效。该实体的这种监督有助于提供合理保证，即在 PCI DSS 评估之间保持其环境的遵从性。虽然目前标准中确定了一些 BAU 要求，但在可能的情况下，实体应该采用针对其组织和环境的额外 BAU 流程。BAU 流程是核实自动和手动控制是否按预期执行的一种方式。无论 PCI DSS 要求是自动还是手动，BAU 流程必须检测到异常情况，并发出警报和报告，以便负责的个人及时处理这种情况。

如何将 PCI DSS 纳入 BAU 活动的示例包括但不限于：

- 将 PCI DSS 遵从性的总体责任和义务分配给个人或团队。这可以包括由行政管理部门为特定的 PCI DSS 遵从性计划制定的章程，并与行政管理部门沟通。
- 制定性能指标，以衡量安全举措的有效性，并持续监控安全控制，包括那些大量依赖的安全控制，例如网络安全控制、入侵检测系统/入侵防御系统（IDS/IPS）、变更检测机制、反恶意软件解决方案和访问控制，以确保它们有效地按照预期运行。
- 更频繁地审核记录数据，以了解趋势或行为，而这些趋势或行为仅靠监控可能不那么明显。
- 确保检测并及时响应安全控制中的所有故障。响应安全控制失效的流程应包括：
  - 恢复安全控制。
  - 识别失效的原因。
  - 识别并解决安全控制失效期间出现的任何安全问题。
  - 实施缓解措施，例如流程或技术控制，以防止失效原因再次发生。
  - 恢复安全控制监控，也许在一段时间内加强监控，以核实控制是否有效运行。
- 在完成变更之前，审核可能给环境带来安全风险的变更（例如，添加新系统、更换系统或网络配置），并包括以下内容：

  - 执行风险评估，以确定变更对 PCI DSS 范围的潜在影响（例如，允许 CDE 中的一个系统与另一个系统之间的连接的新网络安全控制规则，可能将其他系统或网络纳入 PCI DSS 的范围内）。
  - 确定适用于受变更影响的系统和网络的 PCI DSS 要求（例如，如果新系统在 PCI DSS 的范围内，则需要根据系统配置标准进行配置，包括变更检测机制、反恶意软件、补丁和检查记录。需要将这些新的系统和网络添加到范围内系统组件清单和季度漏洞扫描时间表中）。
  - 更新 PCI DSS 范围，并视情况实施安全控制。
  - 更新文件以反映已实施变更。
- 审核组织结构变更对 PCI DSS 范围和要求的影响（例如，公司合并或收购）。
- 定期审核外部连接和第三方访问。
- 对于使用第三方进行软件开发的实体，定期确认这些软件开发活动继续遵守要求 6 中的软件开发要求。
- 执行定期审核，以确认 PCI DSS 要求继续到位，并且人员遵循既定流程。定期审核应涵盖所有设施和地点，包括零售网点和数据中心，无论是自我管理还是使用 TPSP 例如，定期审核可用于确认配置标准已应用于适用的系统，默认供应商帐户和密码已被删除或禁用，补丁和反恶意软件解决方案保持时效性，检查日志正被审查，等等。如果 PCI DSS 中未另行规定，定期审核的频率应由实体根据其环境的规模和复杂性确定。

这些审核也可用于核实是否备存了 PCI DSS 评估所需的证据。例如，检查日志、漏洞扫描报告以及网络安全控制规则集的审核等证据，对于协助实体准备下一次 PCI DSS 评估是必要的。

- 与所有受影响的各方（包括外部和内部）建立沟通，讨论新发现的威胁和组织结构变更。沟通材料应帮助接收者了解威胁的影响、缓解措施以及进一步信息或升级的联络点。
- 至少每 12 个月审核一次硬件和软件技术，以确认它们继续得到供应商的支持，并能满足实体的安全要求，包括 PCI DSS。如果供应商不再支持技术，或技术不能满足实体的安全需求，则实体应准备一个补救计划，包括在必要时替换技术。

注：*本节中的一些最佳实践也被列为某些实体的 PCI DSS 要求。例如，那些正在进行全面 PCI DSS 评估的实体、按照额外的"仅服务提供者"要求进行认证的服务提供者，以及需要按照附录 A3 进行认证的指定实体：指定的实体补充认证。*

每个实体都应考虑在其环境中实施这些最佳实践，即使该实体不需要对它们（例如，正在进行自我评估的商户）进行认证。

有关更多指导，请参考 PCI SSC 网站文件库中的*维护 PCI DSS 遵从性的最佳做法*。

6 评估商：PCI DSS 评估的抽样

对于执行 PCI DSS 评估的评估商来说，抽样是一种选择，当被测试的群体中有大量项目时，可以促进评估流程。

虽然评估商在审核实体的 PCI DSS 遵从性时，从被测群体中的类似项目中抽样是可以接受的，但实体仅将 PCI DSS 要求应用于其环境的一个样本是不可接受的（例如，每季度的漏洞扫描要求适用于所有系统组件）。同样，评估商仅对 PCI DSS 要求进行抽样审核，以确定是否符合要求，也是不可接受的。

虽然抽样允许评估商对低于 100% 的特定抽样群体进行测试，但评估商应始终努力实现最全面的审核。如果能够快速有效地测试完整群体（无论规模如何），并且对被评估实体的资源影响最小，我们鼓励评估商使用自动程序或其他机制。如果没有自动程序来测试 100% 的群体，抽样也是一种同样可以接受的方法。

在考虑了被评估环境的整体范围、复杂性和一致性，以及实体用于满足要求的流程的性质（无论是自动还是手动）后，评估商可以从被审核的群体中独立选择具有代表性的样本，以评估实体是否遵从 PCI DSS 要求。样本必须是群体中所有变体的代表性选择，并且必须足够大，以保证评估商在整个群体中按预期实施控制。在测试某项要求的定期执行情况时（例如，每周或每季度，或定期），评估商应尝试选择代表评估所涵盖的整个时期的样本，以便评估商可以合理判断该要求在整个评估期间得到满足。年复一年地测试相同的项目样本，可能不会检测到非样本项目的未知变体。评估商必须重新认证每次评估的抽样理由，并考虑以前的样本集。每次评估必须选择不同的样本。

适当选择样本取决于检查样本成员时考虑的内容。例如，确定已知受恶意软件影响的服务器上是否存在反恶意软件，可能会导致确定该群体是环境中的所有服务器，或环境中所有运行特定操作系统的服务器，或所有非大型机的服务器等。然后，选择一个适当的样本将包括所确定群体的所有成员的代表，包括运行确定的操作系统的所有服务器，包括所有版本，以及群体中用于不同功能的服务器（网络服务器、应用服务器、数据库服务器等）。

在考虑特定配置项目的情况下，可以适当地划分群体，并确定单独的样本组。例如，在审核操作系统配置设置时，如果环境中存在不同的操作系统，所有服务器的样本可能并不合适。在这种情况下，每个操作系统类型的样本将适合于识别配置已经为每个操作系统适当地设置。每个样本集应该包括每个操作系统类型的代表性服务器，包括版本，以及代表性功能。

其他抽样的示例包括根据被评估的要求，选择具有类似或不同角色的人员，例如，管理员的样本，以及所有员工的样本。

评估商需要在计划、执行和评估样本时使用专业判断，以支持他们关于该实体是否和如何满足要求的结论。评估商抽样的目的是为了获得足够的证据，为他们的意见提供合理依据。在独立选择样本时，评估商应考虑以下几点：

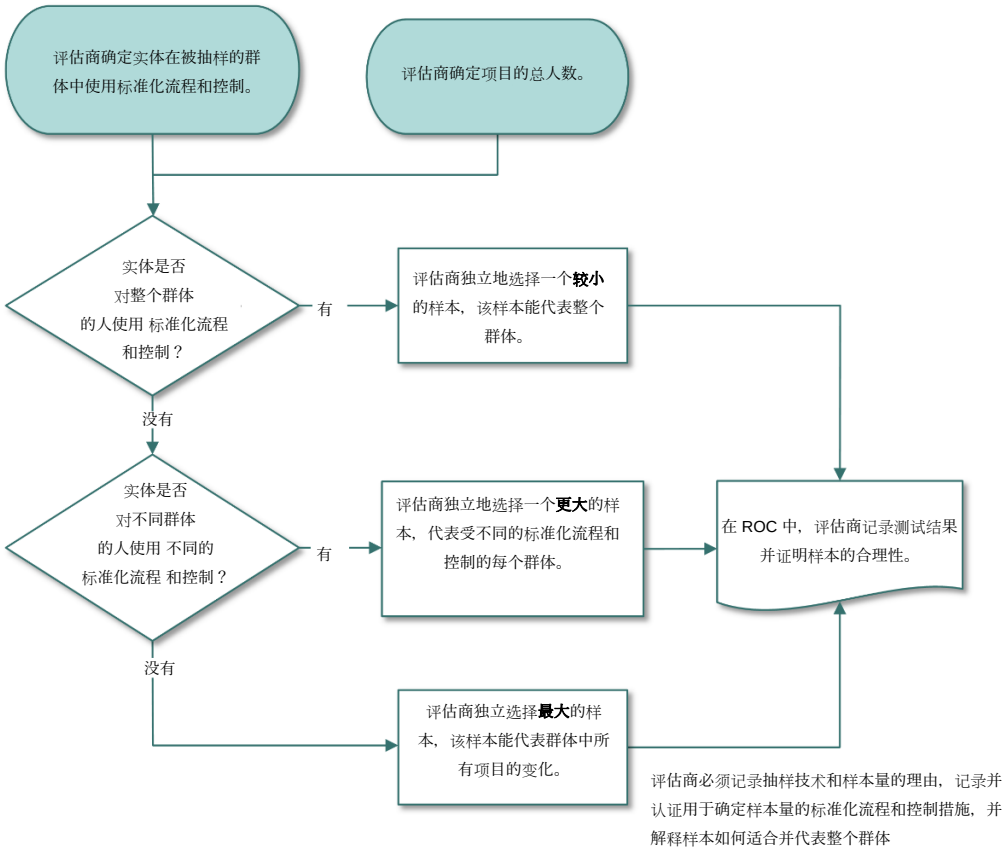
- 评估商必须在不受被评估实体影响的情况下从完整的群体中选择样本。
- 如果该实体拥有确保一致性的标准化流程和控制，并且适用于群体中的每个项目，则样本可能比实体没有标准化流程/控制的情况下更小。样本必须足够大，以向评估商提供合理保证，即群体中的项目遵守适用于群体中每个项目的标准化流程。评估商必须核实标准化控制的实施和有效运作。
- 如果该实体制定了一个以上的标准化流程（例如，针对不同类型的业务设施/系统组件），样本必须包括适用于每种流程的项目。例如，可以根据可能影响评估要求一致性的特征（例如使用不同的流程或工具）将群体划分为子群体。然后从每个子群体中选择样本。
- 如果该实体没有制定标准化的 PCI DSS 流程/控制，并且是通过非标准化流程来管理群体中的每个项目，则样本必须更大，以便评估商确信 PCI DSS 要求适当地适用于群体中的每个项目。
- 系统组件的样本必须包括所使用的每种类型和组合。当实体拥有一个以上的 CDE 时，样本必须包括所有范围内系统组件的群体。例如，当抽样应用程序时，样本必须包括每种应用程序的所有版本和平台。
- 样本量必须始终大于 1，除非在给定群体中只有一个项目，或使用自动控制，评估商已确认该控制在每个被评估的样本群体中按程序运行。
- 如果评估商依靠制定的标准化流程和控制措施作为选择样本的基础，但在测试过程中发现标准化流程和控制措施没有到位或没有有效运行，则评估商应增加样本量，以试图获得满足 PCI DSS 要求的保证。

对于每个使用抽样的实例，评估商必须：

- 记录抽样技术和样本量的理由。
- 认证并记录用于确定样本量的标准化流程和控制。
- 解释样本合适并代表整个群体的方式。

图 3 显示了确定样本大小的注意事项。

图 3。PCI DSS 抽样注意事项



***注：**在 PCI DSS 4.0 版中，所有测试程序都移除了对抽样的具体引用。之所以移除这些引用，是因为在某些测试程序中只提及抽样，可能意味着这些测试程序必须进行抽样（其实不然），或者只有在特别提及的地方才允许抽样。评估商应在适合被测群体的情况下选择样本，并根据上述情况，在考虑环境的整体范围和复杂性后做出这些决定。*

7 PCI DSS 要求中使用的时间框架说明

某些 PCI DSS 要求已经为需要通过定期和可重复的流程持续执行的活动制定了具体的时间框架。其目的是，在尽可能接近该时间框架的间隔内执行该活动，但不超过该时间框架。实体可以自行决定更频繁地执行某项活动（例如，每月执行一项活动，而 PCI DSS 要求规定每三个月执行一次）。

表 4 概述了 PCI DSS 要求中使用的不同时间段的频率。

表 4。PCI DSS 要求的时间框架

PCI DSS 要求中的时间框架	描述和示例
每日	一年中的每一天（不仅仅是在工作日）。
每周	至少每七天一次。
每月	至少每 30 至 31 天一次，或在每月的第 n 天。
每三个月（“每季度”）一次	至少每 90 至 92 天一次，或在每三个月的第 n 天。
每 6 个月	至少每 180 至 184 天一次，或在每六个月的第 n 天。
每 12 个月（“每年”）一次	至少每 365 天（或闰年为 366 天）一次，或在每年的同一天。
定期	发生的频率由实体自行决定，并由实体的风险分析予以记录和支持。该实体必须证明，该频率对于活动的有效性和满足要求的意图是适当的。
立即	毫不拖延。实时或接近实时。
迅速	在合理范围内尽快进行。

PCI DSS 要求中的时间框架	描述和示例
重大变化	有一些要求，在实体环境发生重大变化时，对其性能进行规定。虽然构成重大变更的因素在很大程度上取决于特定环境的配置，但以下每项活动至少对 CDE 的安全性产生潜在影响，必须在相关 PCI DSS 要求的背景下被视为重大变更： • 添加新的硬件、软件或网络设备到 CDE 中。 • CDE 中硬件和软件的任何更换或重大升级。 • 帐户数据流动或存储的任何变更。 • CDE 的边界和/或 PCI DSS 评估范围的任何变更。 • CDE 底层支持基础设施的任何变更（包括但不限于目录服务、时间服务器、日志和监控的变更）。 • 支持 CDE 或代表该实体满足 PCI DSS 要求的第三方供应商/服务提供商（或提供的服务）的任何变更。

对于其他 PCI DSS 要求，如果标准没有规定定期活动的最低频率，而是允许“定期”满足要求，实体应根据其业务情况规定频率。实体的安全政策和根据 PCI DSS 要求 12.3.1 执行的风险分析必须支持实体规定的频率。该实体还必须能够证明其规定的频率对于活动的有效性和满足要求的意图是适当的。

在这两种情况下，如果 PCI DSS 规定了所需的频率，以及在 PCI DSS 允许“定期”执行的情况下，那么实体应该持有记录和实施的流程，以确保在合理的时间框架内执行该活动，并至少包括以下几点：

- 当某项活动没有按照其规定的时间表执行时，该实体会被及时通知；
- 该实体确定导致错过预定活动的事件；
- 该实体在错过活动后尽快执行该活动，并按计划恢复或制定新的计划；
- 该实体制作文件，显示上述元素的发生。

当实体制定了上述流程来检测和处理错过的预定活动时，允许采取合理的方法，也就是说，如果规定至少每三个月执行一次活动，那么，如果该活动推到很迟才执行，但遵循了该实体的书面和实施的流程（按上述规定），则并不会自动导致该实体不合规。但是，如果没有此类流程和/或

由于监督、管理不善或缺乏监督而未按计划执行活动，则该实体未满足要求。在这种情况下，只有当实体 1）记录（或重新确认）上述流程以确保预定活动按时进行，2）重新制定时间表，以及 3）提供证据证明实体已按其时间表至少执行一次预定活动时，该要求才算到位。

注：*对于最初的 PCI DSS 评估（指实体从未接受过先前的评估），如果某项要求有规定的活动时间框架，则不要求在上一年度的每个此类时间框架中都执行该活动，但要求评估商核实：*

- *该活动是在最近的时间范围内（例如，最近的三个月或六个月）按照适用的要求执行的，并且*
- *该实体制定了书面政策和程序，以便在规定的时间范围内继续执行该活动。*

对于初次评估后的后续年份，该活动必须在每个规定的时间框架内至少执行一次。例如，要求每三个月执行一次的活动必须在前一年至少执行了四次，间隔时间不超过 90-92 天。

8 实施和认证 PCI DSS 的方法

为了支持在实现安全目标方面的灵活性，有两种方法来实施和认证 PCI DSS。各实体应确定最适合其安全实施的方法，并使用该方法来认证控制。

规定的方法

遵循实施和认证 PCI DSS 的传统方法，使用标准中规定的要求和测试程序。在规定的方法中，实体实施安全控制，以满足规定的要求，评估商按照规定的测试程序来核实是否满足了要求。

规定的方法支持拥有符合 PCI DSS 要求的控制措施的实体，如上所述。这种方法也可能适合那些希望在如何满足安全目标方面获得更多指导的实体，以及那些刚接触信息安全或 PCI DSS 的实体。

补偿性控制

作为规定的方法的一部分，由于合理的书面技术或业务制约因素而无法明确满足 PCI DSS 要求的实体可以实施其他控制或*补偿性控制*，以充分减轻与要求相关的风险。每年，实体必须记录任何补偿性控制措施，并由评估商审核和认证，并包括在提交的遵从性报告中。

注：更多详细信息，请参见附录 B：补偿性控制 和 附录 C：补偿性控制工作表。

定制方法

重点关注每个 PCI DSS 要求的目标（如果适用），允许实体实施控制以满足要求所述的定制方法目标，其方式并不严格遵循规定的要求。由于每个定制的实施都是不同的，因此没有规定的测试程序；评估商需要制定适合特定实施的测试程序，以认证所实施的控制措施是否满足所述目标。

注：更多详细信息，请参阅附录 D：定制方法 和 附录 E：支持定制方法的样本模板。

定制方法支持安全实践创新，允许实体更灵活地展示他们当前的安全控制如何满足 PCI DSS 目标。这种方法适用于那些能很好处理风险的实体，即他们展示了强大的安全风险管理方法，包括但不限于专门的风险管理部门或整个组织的风险管理方法。

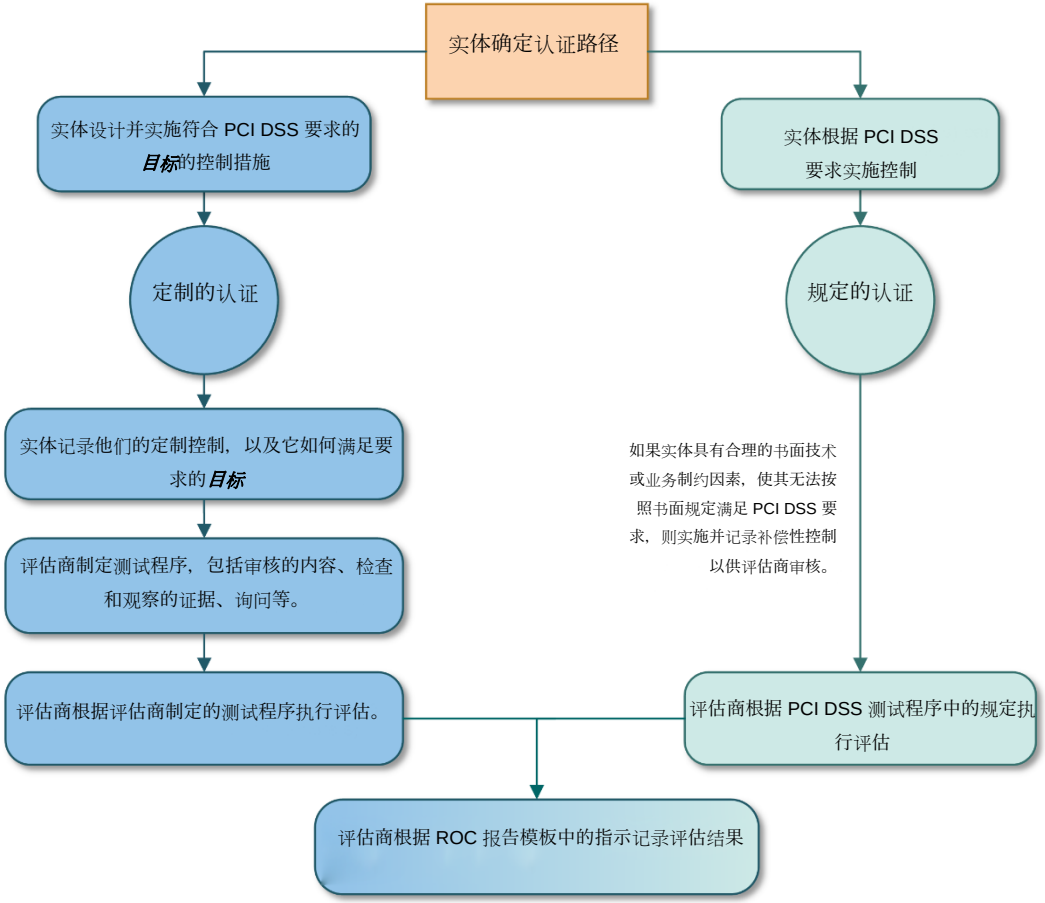
使用定制方法实施和认证的控制措施预计将达到或超过规定方法中的要求所提供的安全性。认证定制实施所需的文件和努力程度也会比规定的方法更多。

可以通过定义或定制的方法来满足大多数 PCI DSS 要求。然而，一些要求没有明确的定制方法目标；定制方法不是这些要求的选择。

各实体可以在其环境中同时使用定义的和定制的方法。这意味着实体可以使用定义的方法来满足一些要求，并使用定制的方法来满足其他要求。这也意味着，实体可以使用定义的方法来满足一个系统组件或一个环境中的特定 PCI DSS 要求，并使用定制的方法来满足不同系统组件或不同环境中的相同 PCI DSS 要求。通过这种方式，PCI DSS 评估可以包括定义和定制的测试程序。

图 4 显示了 PCI DSS 4.0 版的两个认证选项。

图 4。PCI DSS 认证方法



9 保护有关实体安全状况的信息

与成为和维护 PCI DSS 遵从性环境有关的流程会产生许多实体可能认为敏感的人工伪造产物，并可能希望以此来保护这些人工伪造产物，包括以下项目：

- 遵从性报告或自我评估调查问卷（相关遵从性证明不被认为是敏感的，第三方服务提供商（TPSP）应与客户分享其 AOC）。
- 网络图和帐户数据流程图，以及安全配置和规则。
- 系统配置标准。
- 加密和密钥管理方法和协议。

各实体应审核与 PCI DSS 控制或评估有关的所有人工伪造产物，并根据实体对此类信息的安全政策进行保护。

TPSP 需要（PCI DSS 要求 12.9）为其客户提供以下支持：

- 客户监控 TPSP 的 PCI DSS 遵从性状态所需的信息（使客户能够遵守要求 12.8），以及
- 如果 TPSP 的服务旨在满足或促进满足客户的 PCI DSS 要求，或者这些服务可能影响客户 CDE 的安全，则证明 TPSP 符合适用的 PCI DSS 要求。

本节不影响或否定 TPSP 根据要求 12.9 向其客户提供支持和信息的义务。

关于对 TPSP 的期望以及 TPSP 与客户之间关系的更多详细信息，请参见第三方服务供应商的使用。

合格安全性评估商公司保护机密和敏感信息

每个合格安全性评估商（QSA）公司都会与 PCI SSC 签署协议，表明他们将遵守 QSA 的资格要求。该文件的*保护机密和敏感信息*部分包括以下内容：

"QSA 公司必须拥有并遵守保护机密和敏感信息的书面流程。这必须包括符合行业公认做法的充分物理、电子和程序保障措施，以保护机密和敏感信息在存储、处理和/或交流这些信息时不受任何威胁或未经授权的访问。

QSA 公司必须维护其在履行 QSA 公司职责和义务过程中获得的信息的隐私权和保密性，除非（以及在一定程度上）法律授权要求披露这些信息。"

10 PCI DSS 要求的测试方法

每项要求的测试程序中确定的测试方法描述了评估商为确定实体是否满足要求而要执行的预期活动。每个测试方法的目的描述如下：

- 检查：评估商严格评估数据证据。常见示例包括文件（电子或物理），屏幕截图，配置文件，检查日志，和数据文件。
- 观察：评估员观察其环境中的某些事物或动作。观察对象的实例包括执行任务或流程的人员、执行功能或响应输入的系统、环境条件和物理限制。
- 询问：评估商与个别工作人员进行交谈。询问的目的可能包括确认是否执行了某项活动，描述如何执行某项活动，以及相关人员是否具有特定的知识或理解。

测试方法旨在让被评估实体证明他们满足要求的具体方式。它们还让被评估实体和评估商共同了解到将要执行的评估活动。要检查或观察的特定项目和要询问的人员应该适合于被评估的要求和每个实体的特定实施。在记录评估结果时，评估商确定所执行的测试活动以及每项活动的结果。

11 遵从性报告的说明和内容

*PCI DSS 遵从性报告（ROC）模板*提供了遵从性报告（ROC）的说明和内容。

必须使用 PCI DSS 遵从性报告（ROC）模板作为创建 PCI DSS 遵从性报告的模板。

是否要求任何实体遵守或认证其是否遵从 PCI DSS 的要求，由管理遵从性计划的组织（例如支付品牌和收单机构）自行决定。各实体应联系相关组织，以确定任何报告要求和指示。

12 PCI DSS 评估流程

PCI DSS 评估流程包括以下高层次步骤：[5]

1. 确认 PCI DSS 评估的范围。
2. 执行 PCI DSS 环境评估。
3. 根据 PCI DSS 指南和说明，完成适用的评估报告。
4. 完整填写《服务供应商或商户遵从性证明》（如适用）。正式的遵从性证明仅在 PCI SSC 网站上提供。
5. 将适用的 PCI SSC 文件和遵从性证明，以及任何其他要求的文件，例如 ASV 扫描报告，提交给提出请求的组织（那些管理遵从性计划的组织，例如支付品牌和收单机构（针对商户），或其他请求者(针对服务提供商)。
6. 如果需要，执行补救措施，以解决未到位的要求，并提供一份最新报告。

注： *如果控制措施尚未实施或计划在未来某个日期完成，则不认为 PCI DSS 要求已经到位。在实体解决了任何开放或未到位的项目后，评估商将重新评估，以确认补救措施已经完成，并满足所有要求。请参考以下资源（可在 PCI SSC 网站查询），以记录 PCI DSS 评估：*

- *关于完成遵从性报告（ROC）的指示，请参阅 PCI DSS 遵从性报告（ROC）模板。*
- *有关填写自我评估调查问卷（SAQ）的指示，请参阅 PCI DSS SAQ 指示和指南。*
- *有关提交 PCI DSS 遵从性认证报告的指示，请参阅 PCI DSS 遵从性证明。*

[5] PCI DSS 评估流程，以及完成每个步骤的角色和责任，根据评估的类型和遵从性计划而有所不同，这些计划由支付品牌和收单机构管理。

13 其他参考资料

表 5 列出了在 PCI DSS 要求或相关指南中引用的外部组织。这些外部组织及其参考资料仅作为信息提供，并不取代或扩展任何 PCI DSS 要求。

表 5。PCI DSS 要求中引用的外部组织

参考资料	完整名称	来源
ANSI	美国国家标准协会	www.ansi.org
CIS	互联网安全中心	www.cisecurity.org
CSA	云安全联盟	www.csa.org
ENISA	欧盟网络安全局 (前称欧洲网络和信息安全局)	www.enisa.europa.eu
FIDO 联盟	FIDO 联盟	www.fidoalliance.org
ISO	国际标准化组织	www.iso.org
NCSC	英国国家网络安全中心	www.ncsc.gov.uk
NIST	国家标准与技术研究所	www.nist.gov
OWASP	开放式网络应用程序安全项目	www.owasp.org
SAFEcode	卓越代码软件保障论坛	www.safecode.org

14 PCI DSS 版本

截至本文件发布之日，PCI DSS v3.2.1 的有效期至 2024 年 3 月 31 日，此日期后将停用。此日期后，所有 PCI DSS 认证必须参考 PCI DSS 4.0 版或更新版本。

PCI DSS 3.2.1 版或 4.0 版均可用于 2022 年 3 月至 2024 年 3 月 31 日之间执行的评估。

表 6 概述了 PCI DSS 版本及其相关日期。[6]

表 6。PCI DSS 版本

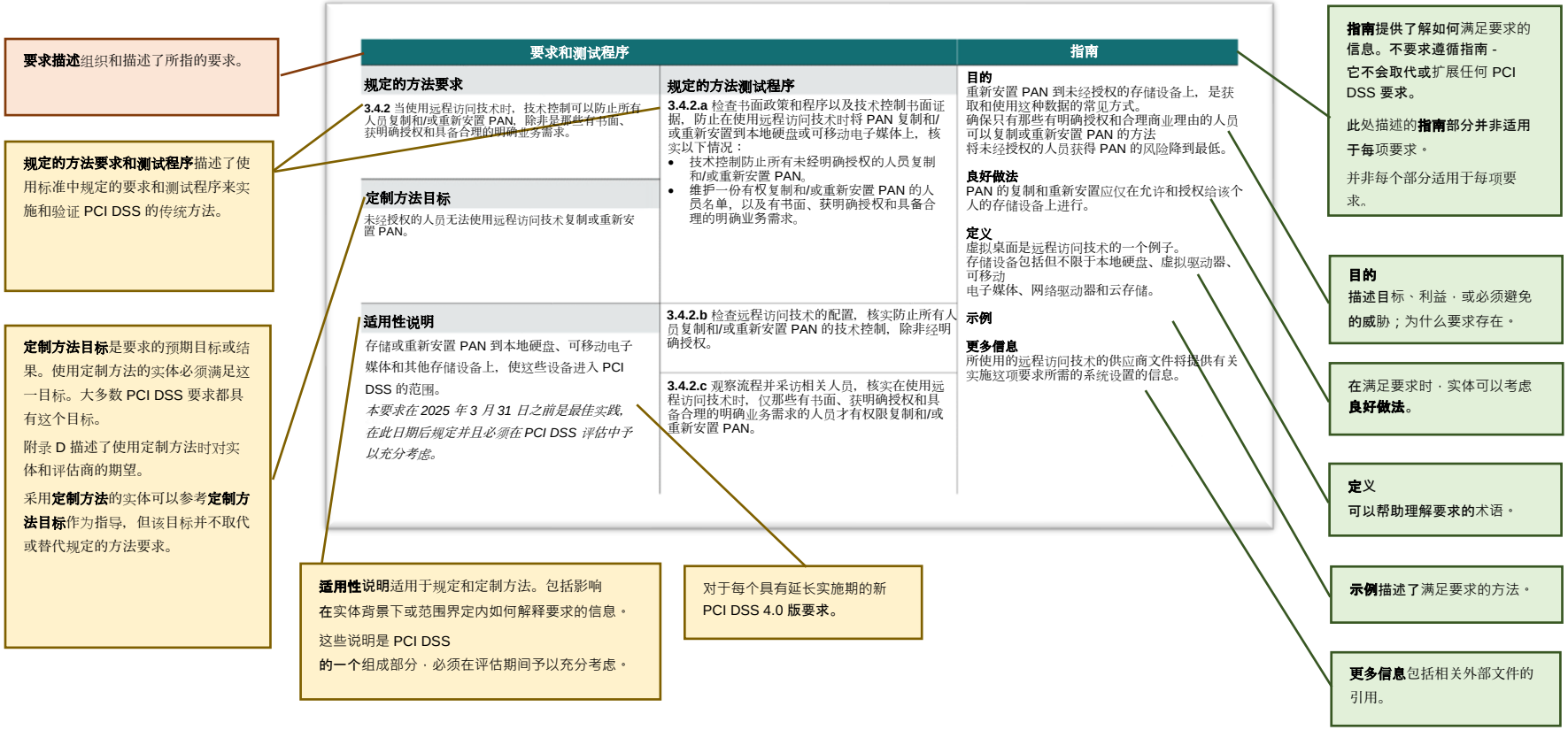
版本	已发布	已退役
PCI DSS 4.0 版 (本文件)	2022 年 3 月	待定
PCI DSS 3.2.1 版	2018 年 5 月	2024 年 3 月 31 日

[6]在 PCI DSS 新版本发布后可能会有所变动。

15 详细的 PCI DSS 要求和测试程序

图 5 描述了 PCI DSS 要求的列标题和内容。

图 5。了解要求的各个部分



仅针对服务供应商的额外要求

有些要求仅在被评估实体是服务提供商的情况下适用。这些要求在要求中被确定为"*仅针对服务供应商的额外要求*"，并适用于所有其他适用的要求。如果被评估的实体既是商户又是服务提供商，则注明为"*仅针对服务提供商的额外要求*"的要求适用于该实体业务中的服务提供商部分。标有"*仅针对服务提供商的额外要求*"的要求也被推荐为最佳实践，供所有实体考虑。

附录，针对不同类型实体的额外 PCI DSS 要求

除了 12 项主要要求之外，PCI DSS 附录 A 还包含针对不同类型实体的额外 PCI DSS 要求。在附录 A 中，章节包括：

- 附录 A1：针对多租户服务提供商的额外 PCI DSS 要求。
- 附录 A2：针对使用 SSL/早期 TLS 进行实体信用卡 POS POI 终端连接的实体的额外 PCI DSS 要求
- 附录 A3：指定的实体补充认证(DESV)

建立和维护安全网络和系统

要求 1：　安装和维护网络安全控制

章节	
1.1	确定和理解安装和维护网络安全控制的流程和机制。
1.2	配置和维护网络安全控制（NSC）。
1.3	限制持卡人数据环境的网络访问权限。
1.4	控制可信网络和不可信网络之间的网络连接。
1.5	减轻能够连接到不可信网络和 CDE 的计算设备对 CDE 产生的风险。

概述

网络安全控制（NSC），例如防火墙和其他网络安全技术，是网络策略执行点，通常根据预先定义的*策略或规则*控制两个或多个逻辑或物理网络分段（或子网）之间的网络流量。

NSC 检查所有进入（入口）和离开（出口）网络分段的网络流量，并根据确定的策略决定是否允许网络流量通过，或是否应该拒绝通过。通常情况下，NSC 被置于具有不同安全需求或信任程度的环境之间，然而在一些环境中，NSC 不分信任界限控制着个别设备的流量。政策执行通常发生在 OSI 模型的第 3 层，但存在于更高层的数据也经常被用来确定政策决策。

传统上，该功能由物理防火墙提供；然而，现在该功能可能由虚拟设备、云访问控制、虚拟化/容器系统和其他软件定义网络技术提供。

NSCs 用于控制实体自身网络内的流量—例如，在高敏感区域和低敏感区域之间，也用于保护实体的资源免于不可信网络的影响。持卡人数据环境（CDE）是一个实体网络中较敏感区域的例子。通常情况下，进出不可信网络的看似微不足道的路径可以提供进入敏感系统的无保护途径。NSCs 提供了任何计算机网络的关键保护机制。

不可信网络的常见例子包括互联网、专用连接，例如企业对企业的通信渠道、无线网络、运营商网络（例如手机）、第三方网络，以及实体控制能力之外的其他来源。此外，不可信网络还包括被认为是 PCI DSS 范围外的企业网络，因为它们没有接受评估，因此必须被视为不可信，因为安全控制的存在尚未得到验证。虽然实体可能从基础设施的角度认为内部网络是可信的，但如果网络不在 PCI DSS 的范围内，则该网络对于 PCI DSS 必须被视为不可信网络。

请参阅附录 G 了解 PCI DSS 术语的定义。

要求和测试程序		指南
1.1 确定和理解安装和维护网络安全控制的流程和机制。		
规定的方法要求 **1.1.1** 要求 1 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。	**规定的方法测试程序** **1.1.1** 检查文件并询问相关人员，以核实是否根据本要求中规定的所有元素管理了要求 1 中确定的安全政策和操作程序。	**目的** 要求 1.1.1 涉及有效管理和维护整个要求 1 规定的各种政策和程序。虽然定义要求 1 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。
定制方法目标 受影响人员确定满足要求 1 的活动的期望、控制和监督，并由其理解并遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。
1.1.2 记录、分配和理解执行要求 1 中活动的角色和责任。	**1.1.2.a** 检查文件，以核实是否记录和分配了执行要求 1 中活动的角色和责任的描述。	
	1.1.2.b 询问负责执行要求 1 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	
定制方法目标		
分配执行要求 1 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。		

要求和测试程序		指南
1.2 配置和维护网络安全控制（NSC。		
规定的方法要求 **1.2.1** NSC 规则集的配置标准： • 已确定。 • 已实施。 • 已维护。 **定制方法目标** 确定并持续运用配置和运行 NSC 的方式。	**规定的方法测试程序** **1.2.1.a** 检查 NSC 规则集的配置标准，以核实该标准是否符合本要求中规定的所有元素。 **1.2.1.b** 检查 NSC 规则集的配置设置，以核实是否根据配置标准实施了规则集。	**目的** 实施这些配置标准导致 NSC 的配置和管理，以正确执行其安全功能（通常称为规则集）。 **良好做法** 这些标准通常确定了可接受协议的要求，允许使用的端口，以及可接受的具体配置要求。配置标准也可能概述了实体认为在其网络内不可接受或不允许的元素。 **定义** NSC 是网络架构的关键组成部分。最常见的是，NSC 被用于 CDE 的边界，以控制输入和输出 CDE 的网络流量。 配置标准概述了实体对配置其 NSC 的最低要求。 **示例** 这些配置标准所涵盖的 NSC 的例子包括但不限于防火墙、配置有访问控制列表的路由器和云虚拟网络。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**良好做法**
1.2.2 根据要求 6.5.1 中确定的变更控制流程审批和管理网络连接和 NSC 配置的所有变更。	**1.2.2.a** 检查书面程序，核实网络连接和 NSC 配置的变更是否根据要求 6.5.1 的规定纳入了正式的变更控制流程。	变更应该由具有适当权力和知识的个人批准，以了解变更的影响。核实应该提供合理保证，即变更没有对网络安全产生不利影响，并且变更按预期执行。 为了避免不得不解决由变更引入的安全问题，所有变更都应在实施前获得批准，并在变更实施后进行核实。一旦获得批准和核实，网络文件应予更新（纳入这些变更），以防止网络文件和实际配置之间存在不一致。
	1.2.2.b 检查网络配置设置，以确定对网络连接所做的变更。询问负责人员并检查变更控制记录，核实是否根据要求 6.5.1 的规定批准和管理了确定的网络连接变更。	
定制方法目标	**1.2.2.c** 检查网络配置设置，以确定对 NSC 配置所做的变更。询问负责人员并检查变更控制记录，核实是否根据要求 6.5.1 的规定批准和管理了确定的 NSC 配置变更。	
网络连接和 NSC 的变更不能导致错误的配置、非安全服务的实施或未经授权的网络连接。		
适用性说明		
网络连接的变更包括增加、移除或修改连接。 NSC 配置的变更包括那些与组件本身有关的变更，以及那些影响其如何执行安全功能的变更。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
1.2.3 保持一份准确的网络图，显示 CDE 和其他网络之间的所有连接，包括任何无线网络。	**1.2.3.a** 检查网络图和网络配置，以核实是否存在符合本要求中规定的所有元素的准确网络图。	保持一个准确、最新的网络图可以防止网络连接和设备被忽视，并在不知情的情况下留在不安全的位置和易于遭到威胁。 适当维护的网络图通过识别连接到 CDE 的系统，帮助组织核实其 PCI DSS 范围。
	1.2.3.b 检查文件和询问负责人员，以核实网络图是否准确，并在环境发生变化时进行更新。	**良好做法** 与 CDE 的所有连接应予以确定，包括为 CDE 系统组件提供安全、管理或维护服务的系统。各实体应考虑在其网络图中包括以下元素： • 所有地点，包括零售地点、数据中心、公司地点、云提供商等。 • 所有网络分段的明确标识。 • 提供分段的所有安全控制，包括每个控制的唯一标识符（例如，控制的名称、品牌、型号和版本）。 • 所有范围内系统组件，包括 NSC、网络应用程序防火墙、反恶意软件解决方案、变更管理解决方案、IDS/IPS、日志聚合系统、支付终端、支付应用程序、HSM 等。 • 通过阴影框或其他机制对图中任何超出范围的区域进行明确标识。 • 最后更新日期，以及作出和批准更新的人的姓名。 *（下一页继续）*
定制方法目标		
保持并提供显示 CDE、所有可信网络和所有不可信网络之间的边界的图示。		
适用性说明		
当前网络图或其他确定网络连接和设备的技术或拓扑解决方案可用于满足这项要求。		

要求和测试程序		指南
		• 解释图表的图例或密钥。 授权人员应该更新网络图，以确保该等图继续提供网络的准确描述。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
1.2.4 保持一份满足以下要求的准确数据流程图： • 显示所有帐户数据在系统和网络间的流动情况。 • 在环境发生变化时视需要进行更新。	**1.2.4.a** 检查数据流程图并询问相关人员，以核实该图是否根据本要求规定的所有元素显示了所有帐户数据流。	一个随时可用的最新数据流程图通过显示帐户数据如何在网络上以及在单个系统和设备之间流动，帮助组织了解和跟踪其环境范围。 保持最新的数据流程图可以防止帐户数据被忽视，并在不知情的情况下留在不安全的位置。
	1.2.4.b 检查文件和询问负责人员，以核实数据流程图是否准确，并在环境发生变化时进行更新。	**良好做法** 数据流程图应包括所有接收帐户数据进入和送出网络的连接点，包括与开放的公共网络的连接、应用程序处理流、存储、系统和网络之间的传输以及文件备份。 数据流程图是网络图的补充，应该与网络图相协调并对其进行补充。作为一种最佳实践，实体可以考虑在其数据流程图中包括以下内容： • 所有帐户数据的处理流程，包括授权、采集、结算、拒付和退款。 • 所有不同的受理渠道，包括实体信用卡、虚拟信用卡和电子商务。 • 所有类型的数据接收或传输，包括任何涉及硬拷贝/纸质媒体。 • 帐户数据从进入环境到最终处置的流程。 • 传输和处理帐户数据的位置，储存帐户数据的位置，以及储存是短期的还是长期的。 *（下一页继续）*
定制方法目标		
保持并提供显示系统组件之间和跨网络分段的所有帐户数据传输的图示。		
适用性说明		
数据流程图或其他确定帐户数据在系统和网络间的流动的技术或拓扑解决方案可用于满足这项要求。		

要求和测试程序		指南
		• 收到的所有帐户数据的来源（例如，客户、第三方等），以及与之共享帐户数据的任何实体。 • 最后更新日期，以及作出和批准更新的人的姓名。
规定的方法要求 **1.2.5** 确定并批准所有允许的服务、协议和端口，并且具有明确的业务需求。	**规定的方法测试程序** **1.2.5.a** 检查文件以核实是否存在所有允许的服务、协议和端口的清单，包括每项服务的业务理由和批准。 **1.2.5.b** 检查 NSC 的配置设置，核实是否只有经批准的服务、协议和端口在使用。	**目的** 由于未使用或非安全服务（例如 telnet 和 FTP）、协议和端口，威胁频频发生，因为这些因素会导致开放进入 CDE 的不必要访问点。此外，对于已启用但未使用的服务、协议和端口，它们往往被忽视，留在不安全的位置，并且未执行补充程式。通过识别业务所需的服务、协议和端口，实体可以确保所有其他服务、协议和端口均已禁用或移除。 **良好做法** 应该了解与允许的每个服务、协议和端口相关的安全风险。应由独立于管理配置的人员授予批准。审批人员应具备适合做出审批决定的知识和责任。
定制方法目标 未经授权的网络流量（服务、协议或以特定端口为目的地的数据包）不能进入或离开网络。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 威胁利用非安全网络配置。 **良好做法** 如果非安全服务、协议或端口对业务来说是必要的，那么组织应该清楚地理解和接受这些服务、协议和端口所带来的风险，该服务、协议或端口的使用应该是合理的，并且实体应该确定和实施减轻使用这些服务、协议和端口风险的安全功能。 **更多信息** 关于被视为非安全服务、协议或端口的指导，请参考行业标准和指导（例如，来自 NIST、ENISA、OWASP）。
1.2.6 确定并实施所有正在使用的、被视为是非安全服务、协议和端口的安全功能，以至于风险得到缓解。	**1.2.6.a** 检查识别所有正在使用的非安全服务、协议和端口的文件，核实是否确定了每个服务、协议和端口的安全功能，以至于风险得到缓解。	
	1.2.6.b 检查 NSC 的配置设置，核实每个已确定的非安全服务、协议和端口是否都实施了已确定的安全功能。	
定制方法目标		
了解、评估与使用不安全服务、协议和端口有关的具体风险，并适当地加以缓解。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
1.2.7 至少每六个月对 NSC 的配置进行一次审核，以确认其相关性和有效性。	**1.2.7.a** 检查文件，核实是否制定了相应程序，至少每六个月对 NSC 的配置进行一次审核。	这种审核使组织有机会清理任何不需要的、过时的或不正确的规则和配置，因为未经授权的人可能会利用这些规则和配置。此外，它确保所有规则和配置只允许授权的服务、协议和端口，以符合书面业务理由。
	1.2.7.b 检查有关审核 NSC 配置的文件并询问负责人员，核实审核是否至少每六个月执行了一次。	**良好做法**
	1.2.7.c 检查 NSC 配置，核实是否移除或更新了被确定为不再受业务理由支持的配置。	这项审核可以使用手动、自动或基于系统的方法实施，目的是确认管理流量规则的设置、允许进出网络的内容与批准的配置相符。 审核应确认所有允许的访问权限都有合理的业务理由。任何关于规则或配置的差异或不确定性都应上报予以解决。 虽然该要求规定这项审核至少每六个月执行一次，但对其网络配置进行大量更改的组织来说，他们可能会考虑更频繁地执行审核，以确保配置继续满足业务需求。
定制方法目标		
定期核实允许或限制访问可信网络的 NSC 配置，以确保只允许具有当前业务理由的授权连接。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
1.2.8 NSC 的配置文件： • 受到保护免于未经授权的访问。 • 与现行网络配置保持一致。	**1.2.8.** 检查 NSC 的配置文件，以核实它们是否符合本要求中规定的所有元素。	为了防止未经授权的配置被应用到网络中，具有网络控制配置的存储文件需要保持最新，并确保其不受未经授权的更改。 确保配置信息的时效性和安全性确保每当运行配置时都能应用正确的 NSC 设置。
定制方法目标		**示例**
不能使用不可信的配置对象（包括文件）确定或修改 NSC。		如果路由器的安全配置存储在非易失性存储器中，当重启该路由器时，这些控制应确保其安全配置得到恢复。
适用性说明		
任何用于配置或同步 NSC 的文件或设置都被视为是“配置文件”。 这包括文件、自动和基于系统的控制、脚本、设置、作为代码的基础设施，或其他备份、存档或远程存储的参数。		

要求和测试程序		指南
1.3 限制持卡人数据环境的网络访问权限。		
规定的方法要求	**规定的方法测试程序**	**目的** 本要求旨在防止恶意者通过未经授权的 IP 地址访问实体的网络，或以未经授权的方式使用服务、协议或端口。 **良好做法** 应该评估所有输入 CDE 的流量，无论流量来自哪里，以确保它遵循既定的授权规则。应该对连接进行检查，以确保流量只限于授权通信—例如，通过限制源/目的地址和端口，以及阻止内容。 **示例** 实施一项规则，拒绝所有非特别需要的输入和输出流量—例如，通过使用明确的“拒绝所有”或允许声明后的隐含拒绝，有助于防止无意中的漏洞，允许非预期和潜在的有害流量。
1.3.1 限制输入 CDE 的流量，具体如下： • 只限制必要的流量。 • 明确拒绝所有其他流量。	**1.3.1.a** 检查 NSC 的配置标准，核实它们所确定的限制输入 CDE 的流量是否符合本要求中规定的所有元素。	
定制方法目标	**1.3.1.b** 检查 NSC 的配置，核实是否根据本要求中规定的所有元素限制了输入 CDE 的流量。	
未经授权的流量不能进入 CDE。		

要求和测试程序		指南
规定的方法要求 **1.3.2** 限制输出 CDE 的流量，具体如下： • 只限制必要的流量。 • 明确拒绝所有其他流量。 **定制方法目标** 未经授权的流量不得离开 CDE。	**规定的方法测试程序** **1.3.2.a** 检查 NSC 的配置标准，核实它们所确定的限制输出 CDE 的流量是否符合本要求中规定的所有元素。 **1.3.2.b** 检查 NSC 的配置，核实是否根据本要求中规定的所有元素限制了输出 CDE 的流量。	**目的** 本要求旨在防止实体网络内的恶意者和受威胁系统组件与不可信的外部主机进行通信。 **良好做法** 应该评估所有输出 CDE 的流量，无论其目的地是哪里，以确保它遵循既定的授权规则。应该对连接进行检查，以便流量只限于授权通信—例如，通过限制源/目的地址和端口，以及阻止内容。 **示例** 实施一项规则，拒绝所有非特别需要的输入和输出流量—例如，通过使用明确的“拒绝所有”或允许声明后的隐含拒绝，有助于防止无意中的漏洞，允许非预期和潜在的有害流量。
规定的方法要求 **1.3.3** NSC 安装在所有无线网络和 CDE 之间，无论无线网络是否为 CDE，为此： • 默认拒绝所有从无线网络进入 CDE 的无线流量。 • 仅允许具有授权商业目的的无线流量进入 CDE。 **定制方法目标** 未经授权的流量不得穿越 CDE 中任何无线网络和有线环境之间的网络边界。	**规定的方法测试程序** **1.3.3.** 检查配置设置和网络图，以核实 NSC 是否在所有无线网络和 CDE 之间实施，并符合本要求规定的所有元素。	**目的** 网络中已知的（或未知的）无线技术的实施和利用是恶意者访问网络和帐户数据的常见途径。如果在实体不知情的情况下安装了无线设备或网络，那么恶意者可以轻松地“隐身”进入网络。如果 NSC 不限制从无线网络进入 CDE，未经授权访问无线网络的恶意者可以轻松地连接到 CDE 并威胁帐户信息。

<table>
<tr><th colspan="2">要求和测试程序</th><th>指南</th></tr>
<tr><td colspan="3">1.4 控制可信网络和不可信网络之间的网络连接。</td></tr>
<tr><td>规定的方法要求</td><td>规定的方法测试程序</td><td rowspan="3">目的
在进入和离开可信网络的每个连接处实施 NSC，允许实体监控和控制访问权限，并最大限度地降低恶意者通过不受保护的连接获得内部网络访问权限的机会。
示例
实体可以实施 DMZ，它是网络的一部分，负责管理不可信网络（关于不可信网络的例子，请参考要求 1 概述）和组织需要向公众提供的服务（例如 Web 服务器）之间的连接。请注意，如果实体的 DMZ 处理或传输 帐户数据（例如，电子商务网站），它也被视为 CDE。</td></tr>
<tr><td>1.4.1 NSC 在可信网络和不可信网络之间实施。</td><td>1.4.1.a 检查配置标准和网络图，以核实 NSC 是否在可信和不可信的网络之间实施。</td></tr>
<tr><td>定制方法目标
未经授权的流量不能穿越可信网络和不可信网络之间的网络边界。</td><td>1.4.1.b 检查网络配置，以核实 NSC 是否根据书面配置标准和网络图在可信和不可信的网络之间实施。</td></tr>
</table>

要求和测试程序		指南
规定的方法要求 **1.4.2** 限制从不可信网络输入可信网络的流量，具体如下： • 与获授权提供公开访问的服务、协议和端口的系统组件进行通信。 • 有状态响应可信网络中系统组件启动的通信。 • 拒绝所有其他通信。 **定制方法目标** 只有经过授权或响应可信网络中的系统组件的流量才能从不可信网络进入可信网络。 **适用性说明** 本要求旨在解决可信和不可信网络之间的通信会话，并非解决协议的具体细节。 如果状态由 NSC 维护，该要求并不限制 UDP 或其他无连接网络协议的使用。	**规定的方法测试程序** **1.4.2.** 检查供应商的文件和 NSC 的配置，核实是否根据本要求规定的所有元素限制了从不可信网络输入到可信网络的流量。	**目的** 确保明确授权系统组件的公共访问权限，减少系统组件不必要地暴露在不可信网络中的风险。 **良好做法** 提供公开访问服务的系统组件，例如电子邮件、网络和 DNS 服务器，最易受到来自不可信网络的威胁。 理想情况下，这些系统被置于一个专门的可信网络中，该网络面向公众（例如，DMZ），但通过 NSC 与更敏感的内部系统分离开来，这有助于在这些外部访问系统被威胁时保护网络的其余部分。此功能的目的是防止恶意行为者从互联网访问组织的内部网络，或以未经授权的方式使用服务、协议或端口。 如果作为 NSC 的内置功能提供该功能，该实体应确保其配置不会导致该功能被禁用或绕过。 **定义** 维护每个连接到网络的“状态”意味着 NSC“知道”对先前连接的明显响应是有效的授权响应（因为 NSC 保留了每个连接的状态），还是试图欺骗 NSC 以允许连接的恶意流量。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
1.4.3 实施反欺骗措施，以检测和阻止伪造的源 IP 地址进入可信网络。	**1.4.3** 检查供应商的文件和 NSC 的配置，核实是否实施了反欺骗措施，以检测和阻止伪造的源 IP 地址进入可信网络。	过滤进入可信网络的数据包有助于，除其他外，确保数据包不会被 “欺骗”，使其看起来像是来自组织自己的内部网络。例如，反欺骗措施防止来自互联网的内部地址进入 DMZ。 **良好做法** 产品通常将反欺骗设置为默认，可能无法对其进行配置。各实体应查阅供应商的文件以了解更多信息。 **示例** 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该数据包的来源。 恶意者通常会试图欺骗（或模仿）发送的 IP 地址，以愚弄目标系统，使其相信该数据包来自可信来源。
定制方法目标		
具有伪造 IP 源地址的数据包不得进入可信网络。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
1.4.4 不能从不可信网络直接访问存储持卡人数据的系统组件。	**1.4.4.a** 检查数据流程图和网络图，核实是否有文件规定不能从不可信网络直接访问存储持卡人数据的系统组件。	如果可以从可信网络直接访问持卡人数据，例如，因为它存储在 DMZ 内的系统或云数据库服务中，外部攻击者便可轻松地访问持卡人数据，因为可以穿透的防御层更少。使用 NSC 来确保只能从可信网络直接访问存储持卡人数据的系统组件（例如数据库或文件），可以防止未经授权的网络流量进入系统组件。
	1.4.4.b 检查 NSC 的配置，核实是否实施了控制措施，确保不能从不可信网络直接访问存储持卡人数据的系统组件。	
定制方法目标		
不能从不可信网络访问存储的持卡人数据。		
适用性说明		
本要求不旨在适用于在易失性存储器中存储帐户数据，但确实在存储器被视为持久性存储器的情况下适用（例如，RAM 磁盘）。帐户数据只能在支持相关业务流程所需的时间内存储在易失性存储器中（例如，直到相关支付卡交易完成为止）。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 限制内部、私人和本地 IP 地址的披露，有助于防止黑客了解这些 IP 地址，并利用这些信息来访问网络。 **良好做法** 用于满足这项要求的方法可能有所不同，视所使用的特定网络技术而定。例如，用于满足该要求的控制对于 IPv4 网络和 IPv6 网络可能有所不同。 **示例** 掩盖 IP 地址的方法可能包括，但不限于： • IPv4 网络地址转换（NAT）。 • 将系统组件置于代理服务器/NSC 后面。 • 删除或过滤使用注册地址的内部网络的路由广告。 • 内部使用 RFC 1918（IPv4）或在向互联网发起外发会话时使用 IPv6 隐私扩展（RFC 4941）。
1.4.5 内部 IP 地址和路由信息仅披露给授权方。	**1.4.5.a** 检查 NSC 的配置，以核实内部 IP 地址和路由信息是否仅披露给授权方。	
	1.4.5.b 询问相关人员并检查文件，核实是否实施了控制措施，使内部 IP 地址和路由信息仅披露给授权方。	
定制方法目标		
保护内部网络信息免于未经授权的披露。		

要求和测试程序		指南
1.5 减轻能够连接到不可信网络和 CDE 的计算设备对 CDE 产生的风险。		
规定的方法要求	**规定的方法测试程序**	**目的**
1.5.1 安全控制施加于任何连接到不可信网络（包括互联网）和 CDE 的计算设备，包括公司和员工拥有的设备，具体如下： • 确定具体配置设置，以防止威胁被引入实体的网络中。 • 安全控制主动运行。 • 计算设备的用户不能改变安全控制，除非有明确记录并由管理层在有限时间内逐案授权。	**1.5.1.a** 检查政策和配置标准并询问相关人员，以核实是否根据本要求中规定的所有元素实施了连接到不可信网络和 CDE 的计算设备的安全控制。 **1.5.1.b** 检查连接到不可信网络和 CDE 的计算设备上的配置设置，以核实是否根据本要求中规定的所有元素实施了设置。	允许从非企业环境连接到互联网的计算设备（例如，台式计算机、笔记本电脑、平板电脑、智能手机和员工使用的其他移动计算设备）更容易受到基于互联网的威胁。 使用安全控制措施，例如基于主机的控制措施（例如，个人防火墙软件或终端保护解决方案）、基于网络的安全控制措施（例如，防火墙、基于网络的启发式检查和恶意软件模拟）或硬件，有助于保护设备免受基于互联网的攻击，因为当设备重新连接到网络时，攻击者可以利用设备获得组织的系统和数据的访问权限。 *（下一页继续）*
定制方法目标		
连接到不可信环境并同时连接到 CDE 的设备不能将威胁引入到实体的 CDE。		

要求和测试程序		指南
适用性说明 仅当有合理技术需要时，经管理层逐案授权，才可以暂时禁用这些安全控制。如果出于特定目的需要禁用这些安全控制，必须经正式授权。在这些安全控制未被激活期间，可能还需要实施其他安全措施。 这项要求适用于员工拥有和公司拥有的计算设备。不能由公司政策管理的系统会引入弱点，并提供恶意者可能加以利用的机会。		**良好做法** 具体配置设置由实体决定，应符合其网络安全政策和程序。 如果有合理需要暂时禁用连接到不可信网络和 CDE 的公司或员工拥有的设备上的安全控制—例如，支持特定的维护活动或调查技术问题—适当的管理代表应理解采取这种行动的原因，并予以批准。对于这些安全控制的任何禁用或更改，包括在管理员自己的设备上的禁用或更改，都由授权人员执行。 一般认为，管理员拥有的特权可能允许他们禁用自己计算机上的安全控制，但当禁用这些控制时，应该要有警报机制，并采取后续行动以确保程序得到遵循。 **示例** 做法包括禁止为员工拥有的或企业拥有的移动设备分割 VPN 隧道，并要求这些设备启动时进入 VPN。

要求 2：　　安全配置应用于所有系统组件

章节
2.1 确定和理解安全配置应用于所有系统组件的流程和机制。
2.2 安全配置和管理系统组件。
2.3 安全配置和管理无线环境。

概述

恶意者，无论是来自外部还是内部，经常使用默认密码和其他供应商的默认设置来威胁系统。这些密码和设置为我们所知，可轻松通过公共信息予以确定。

将安全配置应用于系统组件，可以减少攻击者威胁系统的可用手段。更改默认密码，删除不必要的软件、功能和帐户，以及禁用或删除不必要的服务都有助于减少潜在的攻击面。

请参阅附录 G 了解 PCI DSS 术语的定义。

要求和测试程序		指南
2.1 确定和理解安全配置应用于所有系统组件的流程和机制。		
规定的方法要求 **2.1.1** 要求 2 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。 **定制方法目标** 受影响人员确定满足要求 2 的活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。	**规定的方法测试程序** **2.1.1** 检查文件并询问相关人员，以核实是否根据本要求中规定的所有元素管理了要求 2 中确定的安全政策和操作程序。	**目的** 要求 2.1.1 涉及有效管理和维护整个要求 2 规定的各种政策和程序。虽然定义要求 2 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内 **定义** 安全政策定义了实体的安全目标和原则。 操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。

要求和测试程序		指南
规定的方法要求 **2.1.2** 记录、分配和理解执行要求 2 中活动的角色和责任。 **定制方法目标** 分配执行要求 2 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。	**规定的方法测试程序** **2.1.2.a** 检查文件，以核实是否记录和分配了执行要求 2 中活动的角色和责任的描述。 **2.1.2.b** 询问负责执行要求 2 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	**目的** 如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。

要求和测试程序		指南
2.2 安全配置和管理系统组件。		
规定的方法要求	**规定的方法测试程序**	**目的** 许多操作系统、数据库、网络设备、软件、应用程序、容器镜像以及实体使用的或实体环境内的其他设备都存在已知弱点。也有配置这些系统组件以修复安全漏洞的已知方法。修复安全漏洞可以减少攻击者可用的机会。 通过制定标准，实体确保将一致和安全地配置他们的系统组件，并解决可能更难完全加固的设备的保护问题。 **良好做法** 掌握最新的行业指南将有助于实体保持安全配置。 应用于系统的具体控制措施会有所不同，应该适合于系统的类型和功能。 许多安全组织已建立系统加固指南和建议，建议如何纠正常见的已知弱点。 **更多信息** 关于配置标准的指导来源包括但不限于：互联网安全中心（CIS）、国际标准化组织（ISO）、美国国家标准与技术研究所（NIST）、云安全联盟以及产品供应商。
2.2.1 制定、实施和维护配置标准，以： • 涵盖所有系统组件。 • 解决所有已知的安全漏洞。 • 与行业公认的系统加固标准或供应商加固建议保持一致。 • 按照要求 6.3.1 的规定，在发现新漏洞问题时进行更新。 • 当配置新系统并在系统组件连接到生产环境之前或之后立即核实是否到位时予以应用。	**2.2.1.a** 检查系统配置标准，以核实它们确定的流程是否包括本要求中规定的所有元素。	
	2.2.1.b 检查政策和程序并询问相关人员，核实系统配置标准是否根据要求 6.3.1 的规定，在发现新漏洞问题时进行更新。	
定制方法目标	**2.2.1.c** 检查配置设置并询问相关人员，核实系统配置标准是否在配置新系统时予以应用，并在系统组件连接到生产环境之前或之后立即核实其是否到位。	
以安全和一致的方式配置所有系统组件，并符合行业公认的加固标准或供应商建议。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
2.2.2 管理供应商的默认帐户，具体如下： • 如果将使用供应商的默认帐户，则根据要求 8.3.6 更改默认密码。 • 如果不使用供应商的默认帐户，则将删除或禁用该帐户。	**2.2.2.a** 检查系统配置标准，核实它们是否根据本要求规定的所有元素管理了供应商默认帐户。 **2.2.2.b** 检查供应商文件，观察使用供应商默认帐户登录的系统管理员，核实是否根据本要求中规定的所有元素实施了帐户。 **2.2.2.c** 检查配置文件并询问相关人员，核实所有不使用的供应商默认帐户是否已被删除或禁用。	恶意者经常使用供应商的默认帐户名和密码来威胁操作系统、应用程序以及它们所处的系统。因为通常公布这些默认设置，并且为人所知，更改这些设置将使系统不易受到攻击。 **良好做法** 应识别所有供应商的默认帐户，并了解其目的和用途。务必建立用于应用程序和系统帐户的控制措施，包括那些用于部署和维护云服务的应用程序和系统帐户，以便它们不使用默认密码，并且不能由未经授权的个人使用。 在不打算使用默认帐户的情况下，将默认密码改为符合 PCI DSS 要求 8.3.6 的唯一密码，取消任何默认帐户访问权限，然后禁用该帐户，这将防止恶意者重新启用该帐户并使用默认密码获得访问权限。 建议使用隔离的暂存网络来安装和配置新系统，也建议用它来确认默认凭证是否尚未引入到生产环境中。 **示例** 需要考虑的默认值包括用户 ID、密码和其他供应商在其产品中常用的验证凭证。
定制方法目标		
不能使用默认密码访问系统组件。		
适用性说明		
这适用于所有供应商的默认帐户和密码，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、支付应用程序以及简单网络管理协议（SNMP）所使用的默认帐户和密码。 这一要求也在系统组件没有安装在实体环境中的情况下适用，例如，作为 CDE 的一部分，通过云端订阅服务访问的软件和应用程序。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
2.2.3 管理需要不同安全级别的主要功能，具体如下： • 一个系统组件上只存在一个主要功能， **或** • 存在于同一系统组件上具有不同安全级别的主要功能相互隔离， **或** • 保护存在于同一系统组件上具有不同安全级别的主要功能，以达到具有最高安全需求的功能所需的级别。	**2.2.3.a** 检查系统配置标准，以核实它们是否包括管理本要求中规定的需要不同安全级别的主要功能。 **2.2.3.b** 检查系统配置，以核实是否根据本要求规定的方式之一管理了需要不同安全级别的主要功能。 **2.2.3.c** 如果使用虚拟化技术，检查系统配置，以核实是否根据以下方式之一管理了需要不同安全级别的系统功能： • 具有不同安全需求的功能不并存于同一个系统组件上。 • 存在于同一系统组件上具有不同安全需求的功能相互隔离。 • 保护存在于同一系统组件上具有不同安全需求的功能，以达到具有最高安全需求的功能所需的级别。	包含其主要功能的一组服务、协议和守护程序的系统将有适当的安全配置文件，以允许该功能有效运行。例如，需要直接连接到互联网的系统会有一个特定的配置文件，如 DNS 服务器、网络服务器或电子商务服务器。相反，其他系统组件可能运行一个主要功能，包括一组不同的服务、协议和守护程序，执行一个实体不希望暴露于互联网的功能。这一要求旨在确保不同的功能不会影响其他服务的安全状况，从而导致它们以更高或更低的安全级别运行。 **良好做法** 理想情况下，每个功能应该置于不同的系统组件上。为此，可以在每个系统组件上只实施一个主要功能。另一个选择是在同一系统组件上隔离具有不同安全级别的主要功能，例如，将网络服务器（需要直接连接到互联网）与应用程序和数据库服务器隔离开来。 *（下一页继续）*
定制方法目标		
具有较低安全需求的主要功能不能影响同一系统组件上具有较高安全需求的主要功能的安全。		

要求和测试程序		指南
		如果一个系统组件包含需要不同安全级别的主要功能，第三种选项是实施额外控制，以确保具有较高安全需求的主要功能的最终安全级别不会因为较低安全的主要功能的存在而降低。此外，应该隔离和/或保护安全级别较低的功能，以确保它们不能访问或影响另一个系统功能的资源，并且不会将安全弱点引入同一服务器上的其他功能。 可以通过物理或逻辑控制将不同安全级别的功能隔离开来。例如，一个数据库系统不应该同时托管网络服务，除非使用虚拟化技术等控制措施，将这些功能隔离并包含在独立的子系统中。另一个例子是使用虚拟实例或按系统功能提供专用内存访问。 如果使用虚拟化技术，应该确定和管理每个虚拟组件的安全级别。虚拟化环境的考虑因素实例包括： • 每个应用程序、容器或虚拟服务器实例的功能。 • 如何存储和保护虚拟机（VM）或容器。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 不必要的服务和功能可以提供更多机会，让恶意者获得系统的访问权限。通过删除或禁用所有不必要的服务、协议、守护程序和功能，组织可以专注于保护所需的功能，并减少未知或不必要的功能被利用的风险。 **良好做法** 默认情况下可以启用许多协议，它们通常被恶意者用来威胁网络。禁用或删除所有不使用的服务、功能和协议，可以将潜在攻击面降到最低—例如，通过删除或禁用不使用的 FTP 或 Web 服务器。 **示例** 不必要的功能可能包括，但不限于脚本、驱动程序、功能、子系统、文件系统、接口（USB 和蓝牙）和不必要的网络服务器。
2.2.4 只启用必要的服务、协议、守护程序和功能，删除或禁用所有不必要的功能。	**2.2.4.a** 检查系统配置标准，核实是否识别和记录了必要的系统服务、协议和守护程序。	
	2.2.4.b 检查系统配置，核实以下情况： • 是否删除或禁用了所有不必要的功能。 • 是否只启用配置标准中记录的必要功能。	
定制方法目标		
不能利用系统组件中存在的不必要功能来威胁系统组件。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
2.2.5 如果存在任何非安全服务、协议或守护程序： • 记录商业理由。 • 记录并实施额外安全功能，以减少使用非安全服务、协议或守护程序的风险。	**2.2.5.a** 如果存在任何非安全服务、协议或守护程序，检查系统配置标准并与询问相关人员，核实它们是否根据本要求中规定的所有元素进行管理和实施。	确保使用适当的安全功能充分保护所有非安全服务、协议和守护程序，使恶意者更难利用网络中的常见威胁点。 **良好做法** 在部署新系统组件之前启用安全功能，将防止非安全配置引入到环境中。一些供应商解决方案可能会提供额外安全功能，以协助确保非安全流程的安全。 **更多信息** 关于被视为非安全服务、协议或守护程序的指导，请参考行业标准和指导（例如，发布自 NIST、ENISA 和 OWASP）。
定制方法目标	**2.2.5.b** 如果存在任何非安全服务、协议或守护程序，检查配置设置，以核实是否实施了额外安全功能，以减少使用非安全服务、守护程序和协议的风险。	
不能利用非安全服务、协议或守护程序来威胁系统组件。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
2.2.6 配置系统安全参数以防止误用。	**2.2.6.a** 检查系统配置标准，核实它们是否包括防止误用的配置系统安全参数。	正确配置系统组件中提供的安全参数，利用系统组件的能力来攻克恶意攻击。 **良好做法**
	2.2.6.b 询问系统管理员和/或安全经理，核实他们是否对系统组件的常见安全参数设置有所了解。	系统配置标准和相关流程应专门处理对所使用的每一类系统具有已知安全影响的安全设置和参数。 为了安全配置系统，负责配置和/或管理系统的人员应该了解适用于系统的具体安全参数和设置。考虑因素还应该包括用于访问云门户的参数的安全设置。
定制方法目标	**2.2.6.c** 检查系统配置，核实是否适当设置了常见安全参数并符合系统配置标准。	**更多信息** 参考供应商文件和要求 2.2.1 中提到的行业参考资料，了解每种类型系统的适用安全参数。
不正确的安全参数配置不会对系统组件产生威胁。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
2.2.7 使用强效加密法对所有非控制台的管理访问进行加密。	**2.2.7.a** 检查系统配置标准，核实它们是否包括使用强效加密法来加密所有非控制台管理访问权限。	如果非控制台（包括远程）管理不使用加密通信，窃听者可能会发现管理授权因素（例如 ID 和密码）。恶意者可以利用这些信息来访问网络，成为管理员，并窃取数据。
	2.2.7.b 观察登录到系统组件的管理员并检查系统配置，核实是否根据本要求管理了非控制台管理访问。	**良好做法** 无论使用哪种安全协议，都应配置为只使用安全版本和配置，以防止使用非安全连接—例如，只使用可信证书，只支持强效加密法，不支持回退到较弱的非安全协议或方法。
	2.2.7.c 检查系统组件和验证服务的设置，以核实非安全远程登录服务是否可用于非控制台管理访问。	**示例** 明文协议（例如 HTTP、telnet 等）不对流量或登录细节进行加密，使窃听者轻松截获这些信息。提供系统的替代访问权限的技术可以促进非控制台访问，包括但不限于带外（OOB）、熄灯管理（LOM）、智能平台管理接口（IPMI）和具有远程功能的键盘、视频、鼠标（KVM）开关。必须使用强效加密法来确保这些和其他非控制台访问技术和方法的安全。
	2.2.7.d 检查供应商的文件并询问访谈人员，以核实是否根据行业最佳实践和/或供应商的建议实施了所使用技术的强效加密法。	**更多信息** 请参考行业标准和最佳实践，例如 *NIST SP 800-52 和 SP 800-57*。
定制方法目标		
不能从任何网络传输中读取或截获明文管理授权因素。		
适用性说明		
这包括通过基于浏览器的接口和应用程序编程接口（API）的管理访问权限。		

要求和测试程序		指南
2.3 安全配置和管理无线环境。		
规定的方法要求	**规定的方法测试程序**	**目的**
2.3.1 对于连接到 CDE 或传输帐户数据的无线环境，在安装时改变所有无线供应商的默认值或确认其安全性，包括但不限于： • 默认无线密钥。 • 无线接入点上的密码。 • SNMP 默认值。 • 任何其他与安全有关的无线供应商默认值。	**2.3.1.a** 检查政策和程序并询问负责人员，核实是否制定了相应程序，根据本要求的所有元素，在安装时改变所有无线供应商的默认值或确认其安全性。	如果无线网络的实施没有足够的安全配置（包括改变默认设置），无线嗅探器可以窃听流量，轻松捕获数据和密码，并轻易进入和攻击网络。 **良好做法** 应构造无线密码，使其能够抵御离线蛮力攻击。
	2.3.1.b 检查供应商的文件并观察登录到无线设备的系统管理员，以核实： • 不使用 SNMP 的默认值。 • 不使用无线接入点上的默认密码/口令。	
定制方法目标 不能使用供应商默认密码或默认配置访问无线网络。	**2.3.1.c** 检查供应商文件和无线配置设置，以核实是否改变了其他与安全有关的无线供应商默认值（如果适用）。	
适用性说明 这包括但不限于默认无线密钥、无线接入点的密码、SNMP 默认值以及任何其他与安全相关的无线供应商默认值。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 每当知道密钥的人离开组织或转到一个不再需要知道密钥的角色时，更换无线密钥，这有助于将密钥的信息仅限于那些有业务需要的人。 另外，在怀疑或知道某个密钥被威胁的情况下更换无线密钥，可以使无线网络更不易遭到威胁。 **良好做法** 这一目标可以通过多种方式实现，包括定期更换密钥、通过确定的 “joiners-movers-leavers”（JML）流程更换密钥、实施额外技术控制，以及不使用固定的预共享密钥。 此外，任何已知或怀疑被威胁的密钥应根据要求 12.10.1 中实体的事件响应计划进行管理。
2.3.2 对于连接到 CDE 或传输帐户数据的无线环境，更换无线密钥，具体如下： • 每当了解密钥的人员离开公司或离开需要了解密钥的角色时。 • 每当怀疑或知道密钥被威胁时。	**2.3.2** 询问负责人员并检查密钥管理文件，核实是否根据本要求中规定的所有元素更换了无线密钥。	
定制方法目标		
了解无线密钥不能使未经授权的人员访问无线网络。		

保护帐户数据

要求 3：　　保护所存储帐户数据

章节	
3.1	确定和理解保护所存储帐户数据的流程和机制。
3.2	帐户数据的存储保持在最低限度。
3.3	敏感验证数据（SAD）在授权后不予以存储。
3.4	限制完整 PAN 显示屏的访问权限和复制持卡人数据的能力。
3.5	确保主帐户号码（PAN）安全，无论它们存放在哪里。
3.6	确保用于保护存储帐户数据的密钥安全。
3.7	当加密法用于保护存储帐户数据时，确定并实施涵盖密钥生命周期所有方面的密钥管理流程和程序。

概述

加密、截词、掩盖和散列等保护方法是帐户数据保护的关键组成部分。如果一个入侵者规避了其他安全控制并获得了加密帐户数据的访问权限，那么没有适当的加密密钥，这些数据是不可读的，对该入侵者来说是不可用的。其他保护存储数据的有效方法也应被视为潜在的风险缓解机会。例如，最大限度地减少风险的方法包括：除非有必要，否则不存储帐户数据；如果不需要完整的 PAN，则截断持卡人数据；以及不使用最终用户的信息传递技术（例如电子邮件和即时信息传递）发送未受保护的 PAN。

如果帐户数据存在于非持久性存储器中（例如，RAM，易失性存储器），则无需对帐户数据进行加密。然而，必须制定适当的控制措施，以确保内存保持非持久性状态。达到业务目的（例如，相关交易）后，数据应从易失性存储器中删除。在数据存储成为持久性的情况下，所有适用的 PCI DSS 要求将适用，包括加密存储数据。

要求 3 适用于保护存储的帐户数据，除非在个别要求中特别指出。

关于“强效加密法”和其他 PCI DSS 术语的定义，请参阅附录 G。

要求和测试程序		指南
3.1 确定和理解保护所存储帐户数据的流程和机制。		
规定的方法要求	**规定的方法测试程序**	**目的** 要求 3.1.1 涉及有效管理和维护整个要求 3 规定的各种政策和程序。虽然定义要求 3 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。
3.1.1 要求 3 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。	**3.1.1** 检查文件并询问相关人员，以核实是否根据本要求中规定的所有元素管理了要求 3 中确定的安全政策和操作程序。	
定制方法目标		
受影响人员确定满足要求 3 的活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。		

<table>
<tr><th colspan="2">要求和测试程序</th><th>指南</th></tr>
<tr><td>规定的方法要求</td><td>规定的方法测试程序</td><td rowspan="4">目的
如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。
良好做法
可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。
作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。
示例
记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。</td></tr>
<tr><td>3.1.2 记录、分配和理解执行要求 3 中活动的角色和责任。</td><td>3.1.2.a 检查文件，以核实是否记录和分配了执行要求 3 中活动的角色和责任的描述。</td></tr>
<tr><td>定制方法目标</td><td rowspan="2">3.1.2.b 询问负责执行要求 3 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。</td></tr>
<tr><td>分配执行要求 3 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。</td></tr>
</table>

要求和测试程序		指南
3.2 帐户数据的存储保持在最低限度。		
规定的方法要求	**规定的方法测试程序**	**目的**
3.2.1 通过实施至少包括以下内容的数据保留和处置政策、程序和流程，帐户数据存储将保持在最低水平： • 覆盖所有储存帐户数据的位置。 • 覆盖授权完成前存储的任何敏感认证数据（SAD）。*本项内容在其生效日期前是最佳实践；详情请参考下面的适用性说明。* • 限制数据存储量和保留时间，以至于其在法律或监管和/或业务要求所需的范围内。 • 存储帐户数据的具体保留要求，确定了保留期限，并包括书面业务理由。 • 根据保留政策，在不再需要时，安全删除或使帐户数据无法恢复的程序。 • 至少每三个月审核一次超过规定保留期的存储帐户数据是否已被安全删除或无法恢复。	**3.2.1.a** 检查数据保留和处置的政策、程序和流程并询问相关人员，核实是否制定了相应流程，以包括本要求中规定的所有元素。 **3.2.1.b** 检查存储帐户数据所在系统组件上的文件和系统记录，核实数据存储量和保留时间是否不超过数据保留政策中规定的要求。 **3.2.1.c** 观察用于使帐户数据无法恢复的机制，核实数据是否无法恢复。	正式的数据保留政策确定了需要保留的数据，保留的时长，以及这些数据的存放位置，以便在不再需要时，可以立即安全地销毁或删除。授权后可能被保存的唯一帐户数据是主帐户或 PAN（变得不可读）、到期日、持卡人姓名和业务码。 在完成授权过程之前，SAD 数据的存储也被列入数据保留和处置政策中，以将这种敏感数据的存储保持在最低限度，并且仅在规定的时间内予以保留。 **良好做法** 在确定存储帐户数据的位置时，必须考虑所有能接触到数据的流程和人员，因为数据可能已被转移并存储在与最初确定不同的位置。经常被忽视的存储位置包括备份和存档系统、可移动数据存储设备、纸质媒体和录音。 为了确定适当的保留要求，实体首先需要了解自己的业务需求，以及适用于其行业或被保留数据类型的任何法律或监管义务。实施一个自动程序，确保在规定的保留期限内自动和安全地删除数据，有助于确保帐户数据的保留不会超出业务、法律或监管目的所必需的范围。 *（下一页继续）*
定制方法目标		
帐户数据只在必要时保留，并且保留最少时间，当不再需要时，安全地删除或使帐户数据无法恢复。		

要求和测试程序		指南
适用性说明 当帐户数据由 TPSP 存储时（例如，在云环境中），实体负责与他们的服务提供商合作，了解 TPSP 如何满足实体的这一要求。考虑因素包括确保安全删除数据元素的所有地理实例。 上述内容（在完成授权之前覆盖的存储 SAD）在 2025 年 3 月 31 日之前是最佳实践，在此日期后将作为要求 3.2.1 的一部分并且必须在 PCI DSS 评估中予以充分考虑。		当数据超过保留期时，消除数据的方法包括安全删除，以完全删除数据或使其无法恢复和无法重建。识别并安全地消除已经超过其指定保留期的存储数据，防止不必要地保留不再需要的数据。这个过程可以通过自动、手动或结合两者完成。 大多数操作系统中的删除功能并不是“安全删除”，因为它允许恢复已被删除的数据，因此，必须使用专门的安全删除功能或应用程序来使数据无法恢复。 *请记住，如果你不需要它，就不要储存它!* **示例** 可以运行自动程序化程序来定位和删除数据，也可以对数据存储区进行人工审核。无论使用哪种方法，监控该过程是一个好主意，以确保其成功完成，并记录结果和认证其是否完整。实施安全删除方法可以确保在不再需要时无法检索到数据。 **更多信息** *见 NIST SP 800-88 Rev.1，媒体消毒指南。*

要求和测试程序		指南
3.3 敏感验证数据（SAD）在授权后不予以存储。		
规定的方法要求 **3.3.1** 授权后不保留 SAD，即使已加密。所有收到的敏感验证数据在授权过程完成后将无法恢复。 **定制方法目标** 这项要求不适用于定制方法。 **适用性说明** 本要求不适用于支持发卡服务的发卡服务的公司（需要 SAD 来满足合理发卡业务的需要），并且有业务理由来存储敏感验证数据。 有关针对发卡机构的额外要求，请参考要求 3.3.3。 敏感验证数据包括要求 3.3.1.1 至 3.3.1.3 中引用的数据。	**规定的方法测试程序** **3.3.1.a** 如果收到了 SAD，检查书面政策、程序和系统配置，核实数据在授权后是否不予保留。 **3.3.1.b** 如果收到了 SAD，检查书面程序并观察安全数据删除流程，核实数据在完成授权过程后是否无法恢复。	**目的** SAD 对于恶意者来说是非常有价值的，因为它可以让他们生成伪造的支付卡并制造欺诈性交易。因此，禁止在完成授权过程后储存 SAD。 **定义** 当商户收到一个交易响应（例如，批准或拒绝）时，授权过程即完成。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
3.3.1.1 在完成授权过程后，不保留任何磁道的全部内容。	**3.3.1.1** 检查数据源，核实完成授权过程后是否不保留任何磁道的全部内容。	如果存储任何磁道的全部内容（如果存在的话，来自支付卡背面的磁条，芯片上包含的同等数据，或其他地方），获得该数据的恶意者可以使用它来复制支付卡并完成欺诈性交易。 **定义** 全磁道数据也称为全磁道、磁道、磁道 1、磁道 2 和磁条数据。每个磁道都包含一些数据元素，本要求只规定了那些在授权后可能被保留的数据元素。 **示例** 为确保在授权过程结束后不保留任何磁道的全部内容，需要审核的数据来源包括但不限于： • 输入的交易数据。 • 所有日志（例如，交易、历史、调试、错误）。 • 历史文件 • 跟踪文件 • 数据库模式。 • 数据库的内容，以及内部和云数据存储。 • 任何现有的内存/崩溃转储文件。
定制方法目标		
这项要求不适用于定制方法。		
适用性说明		
在正常业务过程中，可能需要保留磁道上的以下数据元素： • 持卡人姓名。 • 主帐户号码（PAN）。 • 到期日。 • 业务码。 为了将风险降到最低，只在业务需要时安全地存储这些数据元素。		

要求和测试程序		指南
规定的方法要求 **3.3.1.2** 在完成授权过程后，不保留支付卡验证代码。 **定制方法目标** 这项要求不适用于定制方法。 **适用性说明** 支付卡验证代码是印在支付卡正面或背面的三位或四位数字，用于验证虚拟信用卡交易。	**规定的方法测试程序** **3.3.1.2** 检查数据源，核实完成授权过程后是否不保留支付卡验证代码。	**目的** 如果卡验证代码数据被盗，恶意者可以执行欺诈性的互联网和邮件订单/电话订单（MO/TO）交易。不存储这些数据可以减少其被威胁的可能性。 **示例** 如果在完成授权之前将支付卡验证代码存储在纸质媒体上，那么在完成授权之后，应采用擦除或覆盖验证代码的方法来防止其被读取。使代码不可读的方法包括：用剪刀将代码剪掉，并在代码上贴上适当的不透明的、不可去除的标记。 为确保在授权过程结束后不保留支付卡验证代码，需要审核的数据来源包括但不限于： • 输入的交易数据。 • 所有日志（例如，交易、历史、调试、错误）。 • 历史文件 • 跟踪文件 • 数据库模式。 • 数据库的内容，以及内部和云数据存储。 • 任何现有的内存/崩溃转储文件。

要求和测试程序		指南
规定的方法要求 **3.3.1.3** 在完成授权过程后，不保留个人识别码（PIN）和 PIN 数据块。 **定制方法目标** 这项要求不适用于定制方法。 **适用性说明** 在交易过程的自然过程中，将对 PIN 数据块进行加密，但即使实体再次对 PIN 数据块进行加密，仍然不允许在授权过程完成后予以存储。	**规定的方法测试程序** **3.3.1.3** 检查数据源，核实完成授权过程后是否不保留 PIN 和 PIN 数据块。	**目的** PIN 和 PIN 数据块应该只为持卡人或发卡实体所知。如果这些数据被盗，恶意者可以执行基于 PIN 码的欺诈性交易（例如，店内购物和自动取款机取款）。不存储这些数据可以减少其被威胁的可能性。 **示例** 为确保在完成授权过程后不保留 PIN 和 PIN 数据块，需要审核的数据来源包括，但不限于： • 输入的交易数据。 • 所有日志（例如，交易、历史、调试、错误）。 • 历史文件 • 跟踪文件 • 数据库模式。 • 数据库的内容，以及内部和云数据存储。 • 任何现有的内存/崩溃转储文件。

要求和测试程序		指南
规定的方法要求 **3.3.2** 在完成授权之前，使用强效加密法来加密以电子方式存储的 SAD。 **定制方法目标** 这项要求不适用于定制方法。 **适用性说明** 管理合规计划（例如，支付品牌和收单机构）的组织将决定是否允许在授权前存储 SAD。要了解任何额外标准，请联系相关组织。 这项要求适用于所有 SAD 的存储，即使环境中不存在 PAN。 如果在完成授权之前存储 SAD，则参考要求 3.2.1 的额外要求。 本要求不适用于发卡机构和支持发卡服务的公司，因为这些公司具备合理的发卡业务理由来存储 SAD。） 有关针对发卡机构的要求，请参考要求 3.3.3。 本要求并不取代要求 PIN 数据块的管理方式，也不意味着经过适当加密的 PIN 数据块需要再次加密。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **3.3.2** 检查数据存储、系统配置和/或供应商文件，以核实在完成授权之前是否使用了强效加密法来加密以电子方式存储的 SAD。	**目的** 恶意者可以利用 SAD 来增加成功生成伪造的支付卡和创造欺诈性交易的概率。 **良好做法** 实体应该考虑使用与加密 PAN 不同的密钥来加密 SAD。请注意，这并不意味着需要单独加密存在于 SAD 中的 PAN（作为磁道数据的一部分）。 **定义** 一旦收到授权请求响应（即批准或拒绝）授权过程即告完成。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
3.3.3 ***针对支持发卡服务和存储敏感验证数据的发卡机构和公司的额外要求***：任何敏感验证数据的存储： • 只限于合理发卡业务需要的数据，并且受到保护。 • 使用强效加密法进行加密。*本项内容在其生效日期前是最佳实践；详情请参考下面的适用性说明。*	**3.3.3.a** ***针对支持发卡服务和存储敏感验证数据的发卡机构和公司的额外测试程序：*** 检查书面政策并询问相关人员，核实是否有书面业务理由来存储敏感验证数据。 **3.3.3.b** ***针对支持发卡服务和存储敏感验证数据的发卡机构和公司的额外测试程序：*** 检查数据存储和系统配置，核实是否安全存储了敏感验证数据。	恶意者可以利用 SAD 来增加成功生成伪造的支付卡和创造欺诈性交易的概率。 **良好做法** 实体应该考虑使用与加密 PAN 不同的密钥来加密 SAD。请注意，这并不意味着需要单独加密存在于 SAD 中的 PAN（作为磁道数据的一部分）。 **定义** 合理的发卡业务需求是指需要该数据来促进发卡业务流程。 **更多信息** *参考 ISO/DIS 9564-5《金融服务—个人识别码（PIN）管理和安全—第 5 部分。使用高级加密标准生成、更改和验证 PIN 和支付卡安全数据的方法。*
定制方法目标 仅在支持发卡职能所需的情况下保留敏感验证数据，并受到保护免于未经授权的访问。		
适用性说明 本要求仅适用于发卡机构和支持发卡服务并存储敏感验证数据的公司。 发行支付卡的实体或执行或支持发卡服务的实体通常会创建和控制敏感验证数据，作为发卡职能的一部分。执行、促进或支持发卡服务的公司允许存储敏感验证数据，但前提是他们具备存储这些数据的合理业务需求。 *（下一页继续）*		

要求和测试程序		指南
PCI DSS 要求适用于所有存储、处理或传输帐户数据的实体，包括发卡机构。发卡机构和发卡处理机构的唯一例外是，如果有合理理由，则可以保留敏感验证数据。必须安全地存储任何此类数据，并符合所有 PCI DSS 和特定支付品牌要求。 *上述内容（使用强效加密法来加密存储的 SAD）在 2025 年 3 月 31 日之前是最佳实践，在此日期后将作为要求 3.3.3 的一部分并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
3.4 限制显示完整 PAN 的访问权限和复制 PAN 的能力。		
规定的方法要求	**规定的方法测试程序**	**目的**
3.4.1 PAN 在显示时被掩盖（BIN 和最后四位数字是显示的**最大数字**），这样只有具有合理业务需求的人员可以看到比 BIN 和 PAN 的最后四位数字**更多**的内容。	**3.4.1.a** 检查书面政策和程序，以掩盖 PAN 的显示，核实： • 记录需要访问比 BIN 和 PAN 的最后四位数字更多的内容（包括完整的 PAN）的角色列表，以及每个角色拥有这种访问权限的合理业务需求。 • PAN 在显示时被掩盖，只有具有合理业务需求的人员才能看到比 BIN 和 PAN 的最后四位数字**更多**的内容。 • 所有未经明确授权查看完整 PAN 的角色必须只能看到被掩盖的 PAN。	在计算机屏幕、支付卡收据、纸质报告等物品上显示完整 PAN，可能会导致未经授权的人员获得并欺诈性使用这些数据。确保仅对具有合理业务需求的人显示完整的 PAN，可以将未经授权的人员获取 PAN 数据的风险降到最低。 **良好做法** 根据确定的角色应用访问控制是限制只有那些具有明确的业务需求的个人才能查看完整的 PAN 的一种方法。 掩盖方法应始终只显示执行特定业务功能所需的数字数量。例如，如果只需要最后四位数字来执行一项业务功能，PAN 应该被掩盖，只显示最后四位数字。再举一个例子，如果一个功能需要查看银行识别码(BIN)以确定路线，那么只需为该功能取消掩盖 BIN 数字。 **定义** 截词不是截词的同义词，这些术语不能互换使用。掩盖是指在显示或打印过程中隐藏某些数字，即使整个 PAN 都被储存在系统中。这与截词不同，在截词中，将移除被截断的数字，无法在系统内检索。被掩盖的 PAN 可以被“解除掩盖”，但如果不从另一个来源重新创建 PAN，就不会“解除截断”。 *（下一页继续）*
定制方法目标		
PAN 显示被限制在满足明确业务需求所需的最小数字。		
适用性说明	**3.4.1.b** 检查系统配置，核实完整的 PAN 是否只显示给有书面业务需求的角色，而对于所有其他请求 PAN 都被掩盖。	
本要求并不取代显示持卡人数据的现有的更严格要求—例如，销售点（POS）收据的法律或支付品牌要求。 本要求自在 PAN 在屏幕、纸质收据、打印输出等显示时提供保护，并且不应与存储、处理或传输时保护 PAN 的要求 3.5.1 相混淆。		

要求和测试程序		指南
	3.4.1.c 检查显示的 PAN（例如，在屏幕上，在纸质收据上），核实 PAN 在显示时是否被掩盖，并且只有具备合理业务需求的人员才能够看到比 BIN 和/或 PAN 的最后四位数字更多的信息。	**更多信息** 关于掩盖和截断的更多信息，请参阅 PCI SSC 关于这些主题的常见问题。

要求和测试程序		指南
规定的方法要求 **3.4.2** 当使用远程访问技术时，技术控制可以防止所有人员复制和/或重新安置 PAN，除非是那些有书面、获明确授权和具备合理的明确业务需求。 **定制方法目标** 未经授权的人员无法使用远程访问技术复制或重新安置 PAN。 **适用性说明** 存储或重新安置 PAN 到本地硬盘、可移动电子媒体和其他存储设备上，使这些设备进入 PCI DSS 的范围。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **3.4.2.a** 检查书面政策和程序以及技术控制书面证据，防止在使用远程访问技术时将 PAN 复制和/或重新安置到本地硬盘或可移动电子媒体上，核实以下情况： • 技术控制防止所有未经明确授权的人员复制和/或重新安置 PAN。 • 维护一份有权复制和/或重新安置 PAN 的人员名单，以及有书面、获明确授权和具备合理的明确业务需求。 **3.4.2.b** 检查远程访问技术的配置，核实防止所有人员复制和/或重新安置 PAN 的技术控制，除非经明确授权。 **3.4.2.c** 观察流程并询问相关人员，核实在使用远程访问技术时，仅那些有书面、获明确授权和具备合理的明确业务需求的人员才有权限复制和/或重新安置 PAN。	**目的** 重新安置 PAN 到未经授权的存储设备上，是获取和使用这种数据的常见方式。 确保只有经明确授权和具备合理商业理由的人员才能复制或重新安置 PAN 的相应方法，将未经授权的人员获得 PAN 的风险降到最低。 **良好做法** PAN 的复制和重新安置应仅在允许和授权给该个人的存储设备上进行。 **定义** 虚拟桌面是远程访问技术的一个例子。 存储设备包括但不限于本地硬盘、虚拟驱动器、可移动电子媒体、网络驱动器和云存储。 **更多信息** 所使用的远程访问技术的供应商文件将提供有关实施这项要求所需的系统设置的信息。

要求和测试程序		指南
3.5 确保主帐户号码（PAN）安全，无论它们存放在哪里。		
规定的方法要求	**规定的方法测试程序**	**目的**
3.5.1 通过使用以下任何一种方法，使 PAN 在任何存储位置都不可读： • 基于整个 PAN 的强效加密法的单向散列。 • 截词（不能使用散列法来替换 PAN 的截断部分）。 – 如果相同 PAN 的散列和截断版本，或者相同 PAN 的不同截断格式，存在于一个环境中，则要有额外控制，使不同的版本无法相互关联以重建原始 PAN。 • 索引令牌。 • 强效加密法以及相关密钥管理流程和程序。	**3.5.1.a** 检查有关用于使 PAN 不可读的系统的文件，包括供应商、系统/程序的类型和加密算法（如果适用），核实是否使用了本要求中规定的任何方法使 PAN 不可读。	如果未经授权的个人利用实体的主要访问控制的漏洞或错误配置而获得存储数据的访问权限，那么删除明文存储 PAN 是一种旨在保护数据的深度防御控制。 二级独立控制系统（例如，管理加密法和解密密钥的访问和使用）可防止因一级访问控制系统的失效而导致违反存储 PAN 的保密条款。如果散列用于删除存储的明文 PAN，通过关联一个给定 PAN 的散列和截断版本，那么恶意者就可以轻松地得出原始的 PAN 值。防止这种数据关联的控制措施将有助于确保原始 PAN 不可读。
定制方法目标	**3.5.1.b** 检查数据存储库和检查日志，包括支付应用程序的日志，核实是否使用了本要求中规定的任何方法使 PAN 不可读。	**更多信息**
不能从存储媒介中读取明文 PAN。	**3.5.1.c** 如果环境中存在同一 PAN 的散列和截断版本，检查所实施的控制，核实散列和截断版本是否无法相互关联以重建原始 PAN。	有关截词格式和一般截词的信息，请参见 PCI SSC 关于该主题的常见问题。 有关索引令牌的信息来源包括： • PCI SSC 的令牌化产品安全指南（*https://www.pcisecuritystandards.org/documents/Tokenization_Product_Security_Guidelines.pdf*） • *ANSI X9.119-2-2017：零售金融服务 - 保护敏感支付卡数据的要求 - 第 2 部分：实施授权后令牌化系统*
适用性说明		
如果恶意者能够访问某个 PAN 的截断和散列版本，那么重建原始 PAN 数据是一个相对微不足道的工作。 *（下一页继续）*		

要求和测试程序		指南
此要求适用于存储在主存储体（数据库，或平面文件，例如文本文件电子表格）以及非主存储体（备份、检查日志、异常日志、或故障排除日志）的 PAN，它们都必须受到保护。 此要求并不排除在加密和解密 PAN 时使用包含明文 PAN 的临时文件。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果未经授权的个人利用实体的主要访问控制的漏洞或错误配置而获得存储数据的访问权限，那么删除明文存储 PAN 是一种旨在保护数据的深度防御控制。 二级独立控制系统（例如，管理加密法和解密密钥的访问和使用）可防止因一级访问控制系统的失效而导致违反存储 PAN 的保密条款。 **良好做法** 结合随机生成的秘密密钥以提供抗蛮力攻击和秘密验证完整性的散列函数。 **更多信息** 适当的加密散列算法包括但不限于：HMAC、CMAC 和 GMAC，其有效加密强度至少为 128 位 *(NIST SP 800-131Ar2）*。 关于 HMAC、CMAC 和 GMAC 的更多信息，请参考以下内容：*NIST SP 800-107r1*、*NIST SP 800-38B 和 NIST SP 800-38D*）。 *请参见 NIST SP 800-107（修订版 1）：对使用授权散列算法的应用程序的建议§5.3。*
3.5.1.1 用于使 PAN 不可读的散列（根据要求 3.5.1 的第一条）是整个 PAN 的加密散列，以及符合要求 3 .6 和 3.7 的相关密钥管理流程和程序。	**3.5.1.1.a** 检查有关用于使 PAN 不可读的散列方法的文件，包括供应商、系统/程序类型和加密算法（如适用），核实该散列方法是否导致整个 PAN 的加密散列，以及相关密钥管理流程和程序。	
适用性说明 此要求适用于存储在主存储体（数据库，或平面文件，例如文本文件电子表格）以及非主存储体（备份、检查日志、异常日志、或故障排除日志）的 PAN，它们都必须受到保护。 此要求并不排除在加密和解密 PAN 时使用包含明文 PAN 的临时文件。 *本要求在 2025 年 3 月 31 日之前被视为最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**3.5.1.1.b** 检查有关与加密散列相关的密钥管理程序和流程的文件，核实是否根据要求 3.6 和 3.7 管理了密钥。	
	3.5.1.1.c 检查数据存储库，核实 PAN 是否不可读。	
	3.5.1.1.d 检查检查日志，包括支付应用程序的日志，核实 PAN 是否不可读。	

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
3.5.1.2 如果磁盘级或分区级加密（而不是文件级、列级或字段级的数据库加密）被用来使 PAN 不可读，实施方法如下： • 在可移动电子媒介上 **或** • 如果用于非可移动电子媒介，也将通过另一种符合要求 3.5.1 的机制使 PAN 不可读。	**3.5.1.2.a** 检查加密流程，以核实如果磁盘级或分区级加密被用来使 PAN 不可读，它是否只按以下方式实施： • 在可移动电子媒介上， **或** • 如果用于非可移动电子媒介，检查使用的加密过程，核实是否也通过另一种符合要求 3.5.1 的方法使 PAN 不可读。	磁盘级和分区级加密通常使用相同的密钥对整个磁盘或分区进行加密，所有数据在系统运行时或授权用户要求时自动解密。由于这个原因，磁盘级加密不适合用来保护计算机、笔记本电脑、服务器、存储阵列或任何其他在用户验证时提供透明解密的系统上的存储 PAN。
定制方法目标	**3.5.1.2.b** 检查配置和/或供应商文件，观察加密流程，核实是否根据供应商文件配置了系统，其结果是磁盘或分区不可读。	**更多信息**
这项要求不适用于定制方法。		如果有的话，以下供应商的加固和行业最佳实践指南可以帮助保护这些设备上的 PAN。
适用性说明		
作为数据中心架构一部分的媒（例如，热插拔驱动器、批量磁带备份）被视为要求 3.5.1 所适用的非可移动电子媒介。 磁盘或分区加密实施还必须满足所有其他 PCI DSS 加密和密钥管理要求。 本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。		

要求和测试程序		指南
适用性说明		
作为数据中心架构一部分的媒（例如，热插拔驱动器、批量磁带备份）被视为要求 3.5.1 所适用的非可移动电子媒介。 磁盘或分区加密实施还必须满足所有其他 PCI DSS 加密和密钥管理要求。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
3.5.1.3 如果使用磁盘级或分区级加密（而不是文件、列或字段级的数据库加密）来使 PAN 不可读，管理方法如下： • 单独管理逻辑访问，独立于本地操作系统验证和访问控制机制。 • 解密密钥不与用户帐户关联。 • 安全存储允许访问未加密数据的验证因素（密码、口令或加密密钥）。	**3.5.1.3.a** 如果磁盘级或分区级加密用于使 PAN 不可读，检查系统配置并观察验证流程，核实是否根据本要求中规定的所有元素实施了逻辑访问。 **3.5.1.3.b** 检查包含验证因素（密码、口令或密钥）的文件，并与询问相关人员，以核实是否安全存储了允许访问未加密数据的验证因素，并独立于本地操作系统的验证和访问控制方法。	磁盘级加密通常使用相同的密钥对整个磁盘或分区进行加密，所有数据在系统运行时或授权用户要求时自动解密。许多磁盘加密解决方案拦截操作系统的读/写操作，并执行适当的加密转换，而除了在系统启动时或在会话开始时提供密码或口令外，无需用户进行任何特殊操作。因此，无法防御已设法获得有效用户帐户访问权限的恶意者。 **良好做法** 全盘加密有助于在磁盘物理丢失的情况下保护数据，因此其使用最好只限于可移动电子媒介存储设备。
定制方法目标		
配置磁盘加密实施，规定独立的验证和逻辑访问控制进行解密。		
适用性说明		
磁盘或分区加密实施还必须满足所有其他 PCI DSS 加密和密钥管理要求。		

要求和测试程序		指南
3.6 确保用于保护存储帐户数据的密钥安全。		
规定的方法要求 **3.6.1** 确定并实施相应程序，保护用于保护存储帐户数据的加密密钥免于泄露和误用，其中包括： • 密钥访问权限仅限于最少数量的所需保管人。 • 密钥加密密钥的强度至少与它们所保护的数据加密密钥相同。 • 密钥加密密钥与数据加密密钥分开储存。 • 将密钥安全地储存在尽可能少的位置和形式中。 **定制方法目标** 确定并实施保护用于保护存储帐户数据免于泄露和滥用的加密密钥的流程。 **适用性说明** 本要求适用于用于加密存储帐户数据的密钥和用于保护数据加密密钥的密钥加密密钥。 保护用于保护存储帐户数据免于泄露和滥用的密钥的要求适用于数据加密密钥和密钥加密密钥。因为一个密钥加密密钥可能会授予许多数据加密密钥访问权限，所以密钥加密密钥需要强有力的保护措施。	**规定的方法测试程序** **3.6.1** 检查书面密钥管理政策和程序，核实是否制定了相应流程，用于保护存储帐户数据免于泄露和滥用的加密密钥，并包括本要求中规定的所有元素。	**目的** 必须严加保护密钥，因为那些获得访问权限的人将能够解密数据。 **良好做法** 建议拥有一个基于工业标准的集中式密钥管理系统来管理密钥。 **更多信息** 该实体的密钥管理程序将受益于通过与行业要求保持一致，关于加密密钥管理生命周期的信息来源包括： • *ISO 11568-1 银行业 — 密钥管理（零售）— 第 1 部分*：原则（特别是第 10 章以及所参考的第 2 和 4 部分）。 • *NIST SP 800-57 第 1 部分修订版 5 — 密钥管理建议，第 1 部分：一般事项。*

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
3.6.1.1 ***仅针对服务供应商的额外要求：*** 维护加密架构的书面描述，其中包括： • 用于保护存储帐户数据的所有算法、协议和密钥的细节，包括密钥强度和到期日。 • 防止在生产和测试环境中使用相同的密钥。*本项内容在其生效日期前是最佳实践；详情请参考下面的适用性说明。* • 描述每个密钥的使用情况。 • 任何硬件安全模块（HSM）、密钥管理系统（KMS）和其他用于密钥管理的安全加密设备（SCD）的清单，包括设备的类型和位置，如要求 12.3.4 中所述。	**3.6.1.1** ***仅针对服务提供商评估的额外测试程序：*** 询问负责人员并检查文件，核实是否存在一份描述加密架构的文件，其中包括本要求中规定的所有元素。	保持当前的加密架构文件，使实体能够了解用于保护存储帐户数据的算法、协议和密钥，以及生成、使用和保护密钥的设备。这使实体能够跟上其架构所面临的不断变化的威胁，并在不同的算法和密钥强度所提供的保证水平发生变化时计划更新。保持这样的文件也使实体能够发现丢失或遗失的密钥或密钥管理设备，并识别对其密码结构的未经授权添加。 在生产和测试环境中使用相同的密钥，如果测试环境与生产环境的安全级别不同，就会带来暴露密钥的风险。 **良好做法** 拥有一个自动报告机制可以帮助维护加密属性。
定制方法目标 保持并提供加密架构的准确细节。		
适用性说明 本要求仅在被评估实体是服务提供商的情况下适用。 在云 HSM 实施中，云提供商和云客户将根据本要求分担加密架构的责任。 *上述内容（包括在加密架构，防止在生产和测试中使用相同的密钥）在 2025 年 3 月 31 日之前是最佳实践，在此日期后将作为要求 3.6.1.1 的一部分并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
3.6.1.2 用于加密/解密存储帐户数据的秘密密钥和私人密钥在任何时候都以下列一种（或多种）形式存储： • 用至少与数据加密密钥同等强度的密钥加密密钥加密，并与数据加密密钥分开存储。 • 在一个安全加密设备（SCD）内，例如硬件安全模块（HSM）或 PTS 批准的交互点设备。 • 按照行业认可的方法，至少作为两个全长的密钥组件或密钥份额。	**3.6.1.2.a** 检查书面程序，核实其是否规定了用于加密/解密存储帐户数据的加密密钥必须仅以本要求规定的一种（或多种）形式存在。	安全存储密钥可以防止未经授权或不必要的访问，从而导致存储帐户数据暴露。分开存储密钥意味着它们的存储方式是，如果一个密钥的位置被威胁，第二个密钥也不会被威胁。
定制方法目标	**3.6.1.2.b** 检查系统配置和密钥存储位置，核实用于加密/解密存储帐户数据的加密密钥是否以本要求规定的一种（或多种）形式存在。	**良好做法**
秘密密钥和私人密钥以一种安全的形式存储，以防止未经授权的检索或访问。	**3.6.1.2.c** 凡是使用密钥加密密钥的地方，必须检查系统配置和密钥存储位置，核实： • 密钥加密密钥的强度至少与它们所保护的数据加密密钥相同。 • 密钥加密密钥与数据加密密钥分开储存。	当数据加密密钥存储在 HSM 中时，应保护 HSM 的交互通道，以防止截获加密或解密操作。
适用性说明		
不要求公钥以这些形式中的一种存储。 作为采用 SCD 的密钥管理系统（KMS）的一部分而存储密钥，这是可以接受的。 被分割成两部分的密钥不符合该要求。作为密钥部件或密钥份额储存的秘密密钥或私人密钥必须通过以下方式之一产生： • 使用经批准的随机数生成器并在一个 SCD 内， **或** • 根据 ISO19592 或同等工业标准生成秘密密钥份额。		

<table>
<tr><th colspan="2">要求和测试程序</th><th>指南</th></tr>
<tr><td>规定的方法要求</td><td>规定的方法测试程序</td><td rowspan="5">目的
限制访问明文密钥组件的人数，可以减少存储帐户数据被未授权方检索或变得可见的风险。
良好做法
密钥组件的访问权限应仅授予给具有明确密钥保管人职责（创建、更改、轮换、分发或以其他方式维护加密密钥）的人员。
理想情况下，这将是一小部分人。
目的
将任何密钥存储在 最少的位置，有助于组织跟踪和监控所有密钥位置，并将密钥暴露在未授权方的可能性降到最低。</td></tr>
<tr><td>3.6.1.3 明文密钥组件的访问权限仅限于最少数量的所需保管人。</td><td rowspan="2">3.6.1.3 检查用户访问列表，核实明文密钥组件的访问权限是否仅限于最少数量的所需保管人。</td></tr>
<tr><td>定制方法目标</td></tr>
<tr><td>明文密钥组件的访问权限仅限于所需人员。</td></tr>
<tr><td>规定的方法要求</td><td>规定的方法测试程序</td></tr>
<tr><td>3.6.1.4 将密钥存储在尽可能少的位置。</td><td rowspan="2">3.6.1.4 检查密钥存储位置并观察流程，核实密钥是否被存储在尽可能少的位置。</td></tr>
<tr><td>定制方法目标</td></tr>
<tr><td>只在必要时保留密钥。</td></tr>
</table>

要求和测试程序		指南
3.7 当加密法用于保护存储帐户数据时，确定并实施涵盖密钥生命周期所有方面的密钥管理流程和程序。		
规定的方法要求 **3.7.1** 实施密钥管理政策和程序，包括生成用于保护存储帐户数据的强效密钥。 **定制方法目标** 生成强效加密密钥。	**规定的方法测试程序** **3.7.1.a** 检查用于保护存储帐户数据的密钥的书面密钥管理政策和程序，核实它们是否规定了强效密钥的生成。 **3.7.1.b** 观察生成密钥的方法，核实是否生成了强效密钥。	**目的** 使用强效密钥可以显著提高加密帐户数据的安全水平。 **更多信息** 请参阅“附录 G 中密钥生成”所引用的资料。
规定的方法要求 **3.7.2** 实施密钥管理政策和程序，包括安全分发用于保护存储帐户数据的密钥。 **定制方法目标** 确保密钥在分发过程中安全。	**规定的方法测试程序** **3.7.2.a** 检查用于保护存储帐户数据的密钥的书面密钥管理政策和程序，核实它们是否规定了密钥的安全分配。 **3.7.2.b** 观察分配密钥的方法，核实是否安全分配了密钥。	**目的** 秘密或私人密钥的安全分配或传递是指密钥只分配给要求 3.6.1.2 中确定的授权保管人，并且绝不以非安全方式分配。

要求和测试程序		指南
规定的方法要求 **3.7.3** 实施密钥管理政策和程序，包括安全存储用于保护存储帐户数据的密钥。 **定制方法目标** 确保密钥在存储时安全。	**规定的方法测试程序** **3.7.3.a** 检查用于保护存储帐户数据的密钥的书面密钥管理政策和程序，核实它们是否规定了密钥的安全存储。 **3.7.3.b** 观察储存密钥的方法，核实是否安全储存了密钥。	**目的** 在没有适当保护的情况下存储密钥，可能为攻击者提供访问权限，导致帐户数据的解密和暴露。 **良好做法** 数据加密密钥可以通过密钥加密密钥的方式进行保护。 密钥可以存储在硬件安全模块（HSM）中。 可以解密数据的秘密密钥或私人密钥绝不应出现在源代码中。
规定的方法要求 **3.7.4** 执行密钥管理政策和程序，规定更换已经达到密钥周期的密钥，这些政策和程序由相关的应用程序供应商或密钥所有者确定，并基于行业最佳实践和准则，包括以下内容： • 每类所使用密钥的规定密钥周期。 • 规定密钥周期结束时更换密钥的流程。 **定制方法目标** 使用密钥但不超过其规定的密钥周期。	**规定的方法测试程序** **3.7.4.a** 检查用于保护存储帐户数据的密钥的书面密钥管理政策和程序，核实它们是否规定了更换已达到其密钥周期终点的密钥，并包括本要求中规定的所有元素。 **3.7.4.b** 询问相关人员，检查文件并观察密钥存储位置，核实是否在规定的密钥周期结束时更换了密钥。	**目的** 当加密密钥的密钥周期结束时，必须更换它们，以减少某人获得加密密钥并使用它们来解密数据的风险。 **定义** 密钥周期是密钥可用于指定目的的时间段。通常以密钥的活动期和/或密钥生成的密文数量来确定密钥周期。确定密钥周期的考虑因素包括但不限于基础算法的强度、密钥的大小或长度、密钥威胁的风险以及被加密数据的敏感性。 **更多信息** *NIST SP 800-57 第 1 部分，修订版 5，第 5.3 节 密钥周期* - 提供指导，确定合法实体授权使用特定密钥，或特定系统的密钥将保持有效的时间跨度。关于不同密钥类型的建议密钥周期，请参见 *SP 800-57* 第 1 部分的表 1。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
3.7.5 实施密钥管理政策程序，包括视如下需要报废、替换或销毁用于保护存储帐户数据的密钥： • 密钥已达到其规定的密钥周期终点。 • 密钥的完整性已被削弱，包括当了解明文密钥组件的人员离开公司，或离开知道该密钥组件的角色。 • 怀疑或知道密钥被威胁。 • 已报废或被替换的密钥不用于加密操作。	**3.7.5.a** 检查用于保护存储帐户数据的密钥的书面密钥管理政策和程序，核实它们是否根据本要求规定的所有元素对密钥的报废、替换或销毁做出规定。	应归档、撤销和/或销毁不再需要的密钥、完整性被削弱的密钥、以及已知或怀疑被威胁的密钥，以确保不再使用密钥。 如果需要保留这些密钥（例如，支持归档的加密数据），则应该严加保护。
定制方法目标	**3.7.5.b** 询问相关人员，核实是否根据本要求中规定的所有元素实施了该流程。	**良好做法**
当怀疑或知道密钥的完整性被削弱时，将从有效使用中移除密钥。		归档的加密密钥应仅用于解密/验证目的。 加密解决方案应提供并促进一种程序，以替换应予替换的或已知或怀疑被威胁的密钥。此外，任何已知或怀疑被威胁的密钥应根据要求 12.10.1 中实体的事件响应计划进行管理。
适用性说明		**更多信息**
如果需要保留已报废或被替换的密钥，则必须安全地归档这些密钥（例如，通过使用密钥加密密钥）。		*NIST SP 800-57 第 1 部分，修订版 5，第 8.3.1 节*中概述了存档报废密钥的行业最佳做法，包括由可信任第三方维护存档，并将存档的密钥信息与操作数据分开存储。

要求和测试程序		指南
规定的方法要求 **3.7.6** 当手动明文密钥管理操作由人员执行时，密钥管理政策和程序的实施包括使用分割知识和双重控制来管理这些操作。 **定制方法目标** 任何人无法知道明文秘密密钥或私人密钥。涉及明文密钥的操作不能由一人执行。 **适用性说明** 此控制在手动密钥管理操作时或密钥管理不受加密产品控制的情况下适用。 简单地被分割成两部分的密钥不符合该要求。作为密钥部件或密钥份额储存的秘密密钥或私人密钥必须通过以下方式之一产生： • 使用经批准的随机数发生器，并在一个安全加密设备（SCD）内，例如硬件安全模块（HSM）或 PTS 批准的交互点设备。 **或** • 根据 ISO19592 或同等工业标准生成秘密密钥份额。	**规定的方法测试程序** **3.7.6.a** 检查用于保护存储帐户数据的密钥的书面密钥管理政策和程序，核实它们是否规定了分割知识和双重控制的使用。 **3.7.6.b** 询问相关人员和/或观察过程，核实是否以分割知识和双重控制的方式管理了手动明文密钥。	**目的** 密钥的分割知识和双重控制是用来消除个人能够获得整个密钥的可能性，从而能够未经授权地访问数据。 **定义** 分割知识是一种方法，即两人或两人以上分别拥有密钥组件，每人只知道他们自己的密钥组件，个别密钥组件不传达其他组件或原始密钥的信息。 双重控制要求两个或两人以上验证密钥的使用或执行密钥管理功能。任何一人都不能访问或使用另一个人的验证因素（例如，密码、PIN 或密钥）。 **良好做法** 在使用密钥组件或密钥份额的情况下，程序应确保任何一个保管人都不能访问足够的密钥组件或份额以重建密钥。例如，在一个 m-of-n 方案中（例如 Shamir），在任何三个组件中只有两个需要重建密钥，无论现在还是过去，保管人不能了解超过一个组件。如果保管人以前被分配到组件 A，然后被重新分配，则保管人不应该再被分配到组件 B 或组件 C，因为这将使保管人知道两个组件并有能力重新创建密钥。 *（下一页继续）*

要求和测试程序		指南
		示例 可能手动执行的密钥管理操作包括但不限于密钥的生成、传输、加载、存储和销毁。 **更多信息** 管理密钥组件的行业标准包括： • *NIST SP 800-57* 第 2 部分，修订版 1—密钥管理建议。第 2 部分–密钥管理组织的最佳做法 [4.6 密钥材料分配] • *ISO 11568-2 银行业 — 密钥管理（零售）— 第 2 部分*：对称密文、其密钥管理和生命周期 [4.7.2.3 密钥组件和 4.9.3 密钥组件] • *欧洲支付委员会 EPC342-08 有关加密算法使用和密钥管理的指南* [特别是 4.1.4 密钥安装]。
规定的方法要求 **3.7.7** 实施密钥管理政策和程序，包括防止未经授权的密钥替换。	**规定的方法测试程序** **3.7.7.a** 检查用于保护存储帐户数据的密钥的书面密钥管理政策和程序，核实它们是否规定了防止未经授权的密钥替换。	**目的** 如果攻击者能够用攻击者知道的密钥替代实体的密钥，攻击者将能够解密所有用该密钥加密的数据。 **良好做法** 加密解决方案不应允许或接受来自未经授权的来源或意外过程的密钥替换。 控制措施应包括确保能够接触到密钥组件或份额的个人不能接触到构成导出密钥的必要门槛的其他组件或份额。
定制方法目标 密钥不能由未经授权的人员替换。	**3.7.7.b** 询问相关人员和/或观察过程，核实是否防止了未经授权的密钥替换。	

要求和测试程序		指南
规定的方法要求 **3.7.8** 实施密钥管理政策和程序，包括密钥保管人正式承认（书面或电子）他们理解并接受他们的密钥保管人职责。	**规定的方法测试程序** **3.7.8.a** 检查用于保护存储帐户数据的密钥的书面密钥管理政策和程序，核实它们是否规定了根据本要求规定的所有元素对密钥保管人进行确认。 **3.7.8.b** 检查文件或其他证据，表明关键保管人已根据本要求规定的所有元素提供确认。	**目的** 该过程将有助于确保作为密钥保管人的个人致力于密钥保管人的角色，理解并接受其责任。年度重申可以帮助提醒关键保管人他们的职责。 **更多信息** 关于关键保管人及其角色和责任的行业指导包括： • *NIST SP 800-130 密钥管理系统的设计框架* [5. 密钥保管人的角色和责任（特别是）] • *ISO 11568-1 银行业 — 密钥管理（零售）— 第 1 部分*：原则 [5 密钥管理的原则（特别是 b）]
定制方法目标 密钥保管人了解他们在加密操作方面的职责，并在需要时能够获得援助和指导。		
规定的方法要求 **3.7.9** ***仅针对服务供应商的额外要求：*** 如果服务提供商与其客户共享用于传输或存储帐户数据的加密密钥，则应记录并向服务提供商的客户分发关于安全传输、存储和更新此类密钥的指导。	**规定的方法测试程序** **3.7.9** ***仅针对服务提供商评估的额外测试程序：*** 如果服务提供商与其客户共享用于传输或存储帐户数据的加密密钥，则应检查服务提供商向其客户提供的文件，核实其是否包括了关于如何按照上述 3.7.1 至 3.7.8 要求中规定的所有元素安全地传输、存储和更新客户密钥的指导。	**目的** 向客户提供关于如何安全地传输、存储和更新密钥的指导，有助于防止错误地管理密钥或泄露给未经授权的实体。 **更多信息** 上述 3.7.1-3.7.8 要求的指导中引用了许多关于密钥管理的行业标准。
定制方法目标 当客户收到共享密钥时，向其提供适当的密钥管理指导。		
适用性说明 本要求仅在被评估实体是服务提供商的情况下适用。		

要求 4：　在开放的公共网络上传输过程中使用强效加密法保护持卡人数据

章节
4.1 确定和记录在开放公共网络传输过程中使用强效加密法保护持卡人数据的流程和机制。
4.2 PAN 在传输过程中使用强效加密法进行保护。

概述
使用强效加密法在保护数据的保密性、完整性和不可抵赖性方面提供了更大保证。 为了防止威胁，PAN 必须在网络传输过程中进行加密，因为恶意者可轻松地访问这些网络，包括不可信网络和公共网络。配置错误的无线网络和传统加密和验证协议中的漏洞继续成为恶意者的目标，他们旨在利用这些漏洞来获得持卡人数据环境的特权访问（CDE）。任何通过实体的内部网络传输的持卡人数据都会自然而然地将该网络纳入 PCI DSS 的范围，因为该网络存储、处理或传输持卡人数据。必须根据适用的 PCI DSS 要求对任何此类网络进行评估和考核。 要求 4 适用于传输 PAN，除非在个别要求中明确指出。 通过在传输前加密数据，或对传输数据的会话进行加密，或同时进行加密，可以保护 PAN 的传输。虽然不要求在数据级和会话级都应用强效加密法，但建议这样做。 关于“强效加密法”和其他 PCI DSS 术语的定义，请参阅附录 G。

要求和测试程序		指南
4.1 确定和记录在开放公共网络传输过程中使用强效加密法保护持卡人数据的流程和机制。		
规定的方法要求 **4.1.1** 要求 4 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。 **定制方法目标** 受影响人员确定满足要求 4 内活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。	**规定的方法测试程序** **4.1.1** 检查文件并询问相关人员，核实是否根据本要求中规定的所有元素管理了要求 4 中确定的安全政策和操作程序。	**目的** 要求 4.1.1 涉及有效管理和维护整个要求 4 规定的各种政策和程序。虽然定义要求 4 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。政策和程序，包括更新，都积极传达给所有受影响的人员，并得到操作程序的支持，该程序描述了执行活动的方法。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。
4.1.2 记录、分配和理解执行要求 4 中活动的角色和责任。	**4.1.2.a** 检查文件，以核实是否记录和分配了执行要求 4 中活动的角色和责任的描述。	
	4.1.2.b 询问负责执行要求 4 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	
定制方法目标		
分配执行要求 4 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。		

要求和测试程序		指南
4.2 PAN 在传输过程中使用强效加密法进行保护。		
规定的方法要求	**规定的方法测试程序**	**目的**
4.2.1 在开放的公共网络进行传输时，实施强效加密法和安全协议以保护 PAN，具体如下： • 只接受可信密钥和证书。 • 在开放的公共网络上传输过程中用于保护 PAN 的证书被确认为有效，没有过期或被撤销。*本项内容在其生效日期前是最佳实践；详情请参考下面的适用性说明。* • 所使用协议只支持安全版本或配置，不支持回退到非安全的版本、算法、密钥大小或实施，也不支持使用非安全的版本、算法、密钥大小或实施。 • 加密强度适合于所使用的加密方法。	**4.2.1.a** 检查书面政策和程序并询问相关人员，核实是否确定了相应流程，包括本要求中规定的所有元素。 **4.2.1.b** 检查系统配置，核实是否根据本要求中规定的所有元素实施了强效加密法和安全协议。 **4.2.1.c** 检查持卡人数据的传输情况，核实所有 PAN 在通过开放的公共网络传输时，是否用强效加密法进行了加密。 **4.2.1.d** 检查系统配置，核实无法验证为可信的密钥和/或证书是否被拒绝。	敏感信息必须在公共网络的传输过程中进行加密，因为对于恶意者轻松地在传输过程中拦截和/或转移数据，这是一件常见的事情。 **良好做法** 要求 1 中确定的网络图和数据流程图是一个实用资源，用于确定帐户数据在开放的公共网络上传输或接收的所有连接点。 虽然并非强制性，但对于实体来说，在其内部网络上对 PAN 进行加密，以及实体在建立任何新的网络实施时对通信进行加密，被视为是一种良好做法。 通过在传输前加密数据，或对传输数据的会话进行加密，或同时进行加密，可以保护 PAN 的传输。虽然不要求在数据级和会话级都应用强效加密法，但强烈建议这样做。如果在数据级进行加密，则可以根据要求 3.6 和 3.7 管理用于保护数据的密钥。如果数据在会话级加密，应指定密钥保管人负责管理传输密钥和证书。 *（下一页继续）*
定制方法目标		
不能从开放的公共网络上的任何传输中读取或截获明文 PAN。		

要求和测试程序		指南
适用性说明 可能会出现这样的情况：实体通过不安全的通信渠道收到未经请求的持卡人数据，而这个渠道并不旨在传输敏感数据。在这种情况下，该实体可以选择将该渠道纳入其 CDE 范围，并根据 PCI DSS 对其进行保护，或采取措施防止该渠道被用于持卡人数据。 如果证书是由组织内的内部 CA 所颁发，确认证书的作者并验证证书（例如，通过散列或签名）并且没有过期，那么自签证书也是可以接受的。请注意，“签发人”和“签发对象”字段中的可识别名（DN）相同的自签证书是不能接受的。 *上述内容（确认在开放的公共网络上传输过程中用于保护 PAN 的证书是有效的，没有过期或被撤销）在 2025 年 3 月 31 日之前是最佳实践，在此日期后将作为要求 4.2.1 的一部分并且必须在 PCI DSS 评估中予以充分考虑。*		一些协议实施（例如 SSL、SSH v1.0 和早期的 TLS）具有已知漏洞，攻击者可以利用这些漏洞来获取明文数据的访问权限。至关重要的是，实体应持续了解他们所使用的密文套件的行业定义的弃用日期，并准备在旧版本或协议不再被视为安全时迁移到新的版本或协议。 核实证书是否可信有助于确保安全连接的完整性。要被认为是可信证书，它应由可信来源签发，例如可信的证书颁发机构（CA），并且没有过期。最新的证书吊销列表（CRL）或在线证书状态协议（OCSP）可用于验证证书。 验证证书的技术可以包括证书和公钥锁定，也即是说，在开发过程中或首次使用时，可信证书或公钥将被锁定。实体还可以与开发人员确认或审查源代码，以确保客户和服务器在证书不良时拒绝连接。 对于基于浏览器的 TLS 证书，通常可以通过点击出现在地址栏旁边的锁定图标来验证证书的可信程度。 *（下一页继续）*

要求和测试程序		指南
		示例 开放的公共网络包括，但不限于： • 互联网和 • 无线技术，包括 Wi-Fi、蓝牙、蜂窝技术和卫星通信。 **更多信息** 关于所使用加密方法的适当加密强度，可参考供应商建议和行业最佳实践。 关于强效加密法和安全协议的更多信息，请参阅行业标准和最佳实践，例如 *NIST SP 800-52* 和 *SP 800-57*。 关于可信密钥和证书的更多信息，请参阅 *NIST 网络安全实践指南特别出版物 1800-16，确保网络交易安全：传输层安全（TLS）服务器证书管理。*

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
4.2.1.1 维护实体的用于在传输过程中保护 PAN 的可信密钥和证书的清单。	**4.2.1.1.a** 检查书面政策和程序，核实是否制定了相应流程，使该实体保留其可信密钥和证书的清单。	可信密钥清单有助于实体跟踪算法、协议、密钥强度、密钥保管人和密钥到期日。因此，该实体能够快速响应发现于加密软件、证书和加密算法的漏洞。
	4.2.1.1.b 检查可信密钥和证书的清单，核实其是否保持时效性。	**良好做法** 对于证书，清单应包括签发的 CA 和认证到期日。
定制方法目标		
识别传输过程中用于保护 PAN 的所有密钥和证书并确认为可信。		
适用性说明		
本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。		

要求和测试程序		指南
规定的方法要求 **4.2.1.2** 传输 PAN 或连接到 CDE 的无线网络使用行业最佳实践，实施强效加密法进行验证和传输。 **定制方法目标** 不能从无线网络传输中读取或截获明文 PAN。	**规定的方法测试程序** **4.2.1.2** 检查系统配置，核实传输 PAN 或连接到 CDE 的无线网络是否使用行业最佳实践，实施强效加密法进行验证和传输。	**目的** 由于无线网络不需要物理介质进行连接，因此必须建立控制措施，限制可以连接的人员以及使用的传输协议。恶意用户使用免费和广泛使用的工具来窃听无线通信。使用强效加密法可以帮助限制敏感信息在无线网络中的泄露。 无线网络给组织带来了独特风险；因此，必须根据行业要求对其进行识别和保护。需要强效加密法对 PAN 进行验证和传输，防止恶意用户获得无线网络的访问权限或利用无线网络访问其他内部网络或数据。 **良好做法** 无线网络不应允许回退或降级到非安全协议或不符合强效加密法意图的较低加密强度。 **更多信息** 有关加密的协议选择、配置和设置的更多细节，请查阅供应商的特定文件。

要求和测试程序		指南
规定的方法要求 **4.2.2** 通过终端用户信息传递技术发送 PAN 时，使用强效加密法对其进行保护。 **定制方法目标** 不能从使用最终用户信息传递技术的传输中读取或截获明文 PAN。 **适用性说明** 本要求在客户或其他第三方要求通过最终用户信息传递技术向他们发送 PAN 的情况下亦适用。 可能会出现这样的情况：实体通过不安全的通信渠道收到未经请求的持卡人数据，而这个渠道并不旨在传输敏感数据。在这种情况下，该实体可以选择将该渠道纳入其 CDE 范围，并根据 PCI DSS 对其进行保护，或者删除持卡人数据，并采取措施防止该渠道被用于持卡人数据。	**规定的方法测试程序** **4.2.2.a** 检查书面政策和程序，核实是否制定了相应流程，以便在通过终端用户信息传递技术发送 PAN 时，使用强效加密法对其进行保护。 **4.2.2.b** 检查系统配置和供应商文件，核实通过终端用户信息传递技术发送 PAN 时，是否使用了强效加密法对其进行保护。	**目的** 终端用户信息传递技术通常可轻易地在内部和公共网络的传输过程中被窃听包截获。 **良好做法** 仅当有明确业务需求的情况下，才应考虑使用终端用户信息传递技术来发送 PAN。 **示例** 电子邮件、即时通讯、SMS 和聊天是本要求所指的终端用户信息传递技术类型的例子。

维护漏洞管理计划

要求 5：　　保护所有系统和网络免受恶意软件侵害

章节
5.1 确定并理解保护所有系统和网络免受恶意软件侵害的流程和机制。
5.2 防止或检测并处理恶意软件。
5.3 维护和监控有效的反恶意软件机制和程序。
5.4 反钓鱼机制保护用户免受网络钓鱼攻击。

概述
恶意软件是指在所有者不知情或未经所有者同意的情况下潜入或破坏计算机系统，意图破坏所有者数据、应用程序或操作系统的保密性、完整性或可用性的软件或固件。 示例包括病毒、蠕虫、木马、间谍软件、勒索软件、键盘记录器和根工具包 内核型病毒、恶意代码、脚本和链接。 恶意软件可以在许多企业认可的活动中进入网络，包括员工电子邮件（例如通过网络钓鱼）和使用互联网、移动计算机和存储设备，从而导致系统漏洞的利用。 使用解决所有类型恶意软件的反恶意软件解决方案有助于保护系统免受当前和不断发展的恶意软件威胁。 请参阅*附录 G* 了解 PCI DSS 术语的定义。

要求和测试程序		指南
5.1 确定并理解保护所有系统和网络免受恶意软件侵害的流程和机制。		
规定的方法要求 **5.1.1** 要求 5 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。 **定制方法目标** 受影响人员确定满足要求 5 内活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。	**规定的方法测试程序** **5.1.1** 检查文件并询问相关人员，以核实是否根据本要求中规定的所有元素管理了要求 5 中确定的安全政策和操作程序。	**目的** 要求 5.1.1 涉及有效管理和维护整个要求 5 规定的各种政策和程序。虽然定义要求 5 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果没有正式分配角色和责任，可能无法适当保护网络和系统免受恶意软件攻击。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。
5.1.2 记录、分配和理解执行要求 5 中活动的角色和责任。	**5.1.2.a** 检查文件，以核实是否记录和分配了执行要求 5 中活动的角色和责任的描述。	
	5.1.2.b 询问负责执行要求 5 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	
定制方法目标		
分配执行要求 5 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。		

要求和测试程序		指南
5.2 防止或检测并处理恶意软件。		
规定的方法要求 **5.2.1** 反恶意软件解决方案部署在所有系统组件上，除了那些根据要求 5.2.3 定期评估得出的系统组件不受恶意软件威胁的系统组件。 **定制方法目标** 实施自动化机制，防止系统成为恶意软件的攻击向量。	**规定的方法测试程序** **5.2.1.a** 检查系统组件，核实反恶意软件解决方案是否部署在所有系统组件上，除了那些根据要求 5.2.3 的定期评估确定为不受恶意软件威胁的组件。 **5.2.1.b** 对于没有反恶意软件解决方案的任何系统组件，检查定期评估以核实该组件已被评估，并且评估的结论是该组件不受恶意软件威胁。	**目的** 不断发生针对以前被认为安全的系统中新发现的漏洞的攻击。如果没有定期更新的反恶意软件解决方案，新形式的恶意软件就会被用来攻击系统，使网络瘫痪，或损害数据。 **良好做法** 对实体来说，了解“零日”攻击（那些利用以前未知漏洞的攻击）并考虑专注于行为特征的解决方案是有益的，并将对意外行为发出警报和响应。 **定义** 已知受恶意软件影响的系统组件在现实世界中存在活动的恶意软件漏洞（不仅仅是理论上的漏洞）。
规定的方法要求 **5.2.2** 所部署的反恶意软件解决方案： • 检测所有已知类型的恶意软件。 • 移除、阻止或包含所有已知类型的恶意软件。 **定制方法目标** 恶意软件不能执行或感染其他系统组件。	**规定的方法测试程序** **5.2.2** 检查反恶意软件解决方案的供应商文件和配置，核实该解决方案： • 检测所有已知类型的恶意软件。 • 移除、阻止或包含所有已知类型的恶意软件。	**目的** 防范所有类型和形式的恶意软件以防止未经授权的访问至关重要。 **良好做法** 反恶意软件解决方案可能包括基于网络的控制、基于主机的控制和端点安全解决方案的组合。除了基于签名的工具外，现代反恶意软件解决方案使用的功能包括沙箱、权限升级控制和机器学习。 解决方案技术包括防止恶意软件进入网络，删除或遏制进入网络的恶意软件。 **示例** 恶意软件的类型包括但不限于：病毒、木马、蠕虫、间谍软件、勒索软件、键盘记录器、根工具包内核型病毒、恶意代码、脚本和链接。

要求和测试程序		指南
规定的方法要求 **5.2.3** 定期评估不受恶意软件威胁的任何系统组件，包括以下内容： • 所有不受恶意软件威胁的系统组件的书面清单。 • 识别和评估这些系统组件面临的不断变化的恶意软件威胁。 • 确认这些系统组件是否继续不需要反恶意软件保护。 **定制方法目标** 该实体持续了解不断变化的恶意软件威胁，以确保任何未受保护免受恶意软件威胁的系统不存在感染风险。 **适用性说明** 本要求涵盖的系统组件是那些没有按照要求 5.2.1 部署反恶意软件解决方案的系统组件。	**规定的方法测试程序** **5.2.3.a** 检查书面政策和程序，核实是否制定了相应程序，以定期评估任何不受恶意软件威胁的系统组件，其中包括本要求中规定的所有元素。 **5.2.3.b** 询问相关人员，核实评估是否包括本要求中规定的所有元素。 **5.2.3.c** 检查被确认为不受恶意软件威胁的系统组件清单，并与没有按照要求 5.2.1 部署反恶意软件解决方案的系统组件进行比较，核实系统组件是否符合这两项要求。	**目的** 某些系统，在某一特定时间点，目前可能不会成为恶意软件的普遍目标或受到恶意软件的影响然而，恶意软件的行业趋势可能会迅速变化，因此，组织必须了解可能影响其系统的新恶意软件—例如，通过监控供应商的安全通知和反恶意软件论坛来确定其系统是否可能受到不断发展的新恶意软件的威胁。 **良好做法** 如果实体确定一个特定的系统不容易受到任何恶意软件的影响，那么该决定应得到行业证据、供应商资源和最佳实践的支持。 以下步骤可以在定期评估期间帮助实体： • 识别以前确定为不需要恶意软件保护的所有系统类型。 • 审核行业漏洞警报和通知，以确定任何确定的系统是否存在新威胁。 • 关于系统类型是否仍然不易受恶意软件影响的书面结论。 • 为有必要进行恶意软件保护的任何系统类型添加恶意软件保护的策略。 恶意软件的趋势应包括在要求 6.3.1 的新安全漏洞识别中，并且应视需要将解决新趋势的方法纳入实体的配置标准和保护机制。

要求和测试程序		指南
规定的方法要求 **5.2.3.1** 实体的目标风险分析确定了被确认为不受恶意软件威胁的系统组件的定期评估频率，该分析根据要求 12.3.1 中规定的所有元素执行。	**规定的方法测试程序** **5.2.3.1.a** 检查该实体的目标风险分析，了解被确认为不受恶意软件威胁的系统组件的定期评估频率，核实是否根据要求 12.3.1 规定的所有元素执行了风险分析。	**目的** 各实体根据每个实体环境的复杂性和需要评估的系统类型数量等标准，确定开展评估的最佳时期。
	5.2.3.1.b 检查对确定为不受恶意软件威胁的系统组件进行定期评估的记录结果并询问相关人员，核实是否根据实体为该要求执行的目标风险分析中规定的频率执行了评估。	
定制方法目标 以解决实体风险的频率重新评估尚不清楚是否会受到恶意软件威胁的系统。		
适用性说明 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
5.3 维护和监控有效的反恶意软件机制和程序。		
规定的方法要求	**规定的方法测试程序**	**目的** 为了使反恶意软件解决方案保持有效，它需要拥有最新的安全更新、签名、威胁分析引擎以及解决方案所依赖的任何其他恶意软件保护措施。 拥有自动化更新程序，可以避免让终端用户承担手动安装更新的责任，并为反恶意软件保护机制在更新发布后尽快更新提供更大保证。 **良好做法** 反恶意软件机制应在更新发布后尽快通过可信来源进行更新。使用可信共同来源向终端用户系统分发更新，有助于确保解决方案架构的完整性和一致性。 更新可以自动下载到中心位置—例如，允许进行测试—然后再部署到各个系统组件。
5.3.1 反恶意软件解决方案通过自动更新保持时效性。	**5.3.1.a** 检查反恶意软件解决方案配置，包括软件的任何主安装，核实是否将解决方案配置为执行自动更新。	
	5.3.1.b 检查系统组件和日志，核实反恶意软件解决方案和定义是否为最新，并及时部署了该解决方案	
定制方法目标		
反恶意软件机制能够检测并解决最新的恶意软件威胁。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
5.3.2 反恶意软件解决方案： • 执行定期扫描和主动或实时扫描。 **或** • 持续对系统或流程进行行为分析。	**5.3.2.a** 检查反恶意软件解决方案配置，包括软件的任何主安装，核实该解决方案是否被配置为执行本要求中规定的至少一个元素。	定期扫描可以识别环境中存在但目前不活跃的恶意软件。一些恶意软件，例如零日恶意软件，可以在扫描解决方案能够检测到它之前进入一个环境。对系统或流程进行定期扫描或持续行为分析，有助于确保能够识别、删除并调查以前无法检测到的恶意软件，以确定它通过什么方式获取环境的权限。 **良好做法** 使用定期扫描（计划和按需）和主动、实时（访问）扫描的组合有助于确保解决驻留在 CDE 静态和动态元素中的恶意软件。如果检测到可疑活动，用户也应该能够在他们的系统上运行按需扫描–这在早期检测恶意软件方面有所帮助。 扫描应包括整个文件系统，包括所有磁盘、内存以及启动文件和启动记录（在系统重启时），以便在文件执行时检测所有恶意软件，包括可能驻留在系统上但目前没有活动的任何软件。扫描范围应包括 CDE 中的所有系统和软件，包括那些经常被忽视的系统和软件，例如电子邮件服务器、网络浏览器和即时通讯软件。 **定义** 主动或实时扫描在任何试图打开、关闭、重命名或以其他方式与文件互动时检查文件是否有恶意软件，防止恶意软件的激活。
	5.3.2.b 检查系统组件，包括所有被确定为有恶意软件风险的操作系统类型，核实是否根据本要求中规定的至少一个元素启用了解决方案。	
定制方法目标	**5.3.2.c** 检查日志和扫描结果，核实是否根据本要求中规定的至少一个元素启用了解决方案。	
恶意软件无法完成执行。		

要求和测试程序		指南
规定的方法要求 **5.3.2.1** 如果定期执行恶意软件扫描以满足要求 5.3.2，扫描的频率在实体的目标风险分析中确定，该分析根据要求 12.3.1 中规定的所有元素执行。	**规定的方法测试程序** **5.3.2.1.a** 检查实体的目标风险分析，了解定期恶意软件扫描的频率，核实是否根据要求 12.3.1 规定的所有元素执行了风险分析。 **5.3.2.1.b** 检查定期恶意软件扫描的书面结果并询问相关人员，核实是否根据实体为该要求执行的目标风险分析中规定的频率执行了扫描。	**目的** 各实体可以根据其自身对环境风险的评估，确定执行定期扫描的最佳时期。
定制方法目标 根据解决实体风险的频率执行恶意软件解决方案的扫描。		
适用性说明 **本要求适用于**资讯定期恶意软件扫描以满足要求 5.3.2 **的**实体。 ***本要求在 2025 年 3 月 31 日之前是最佳***实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。		

要求和测试程序		指南
规定的方法要求 **5.3.3** 对于可移动电子媒介，反恶意软件解决方案： • 当插入、连接或逻辑安装媒介时，执行自动扫描。 **或** • 当插入、连接或逻辑安装媒介时，持续对系统或流程进行行为分析。 **定制方法目标** 不能通过外部可移动媒介将恶意软件引入系统组件。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **5.3.3.a** 检查反恶意软件解决方案配置，核实对于可移动电子媒介，该解决方案是否被配置为执行本要求中规定的至少一个元素。 **5.3.3.b** 检查连接有可移动电子媒介的系统组件，核实是否根据本要求中规定的至少一个元素启用了解决方案。 **5.3.3.c** 检查日志和扫描结果，核实是否根据本要求中规定的至少一个元素启用了解决方案。	**目的** 便携式媒介设备作为恶意软件的一种进入方式经常被忽视。攻击者通常会将恶意软件预先加载到 USB 和闪存驱动器等便携式设备上；将受感染的设备连接到计算机上，然后触发恶意软件，将新威胁引入到环境中。
规定的方法要求 **5.3.4** 检查日志，核实是否根据要求 10.5.1 启用和保留了反恶意软件解决方案。 **定制方法目标** 反恶意软件操作的历史记录可立即获得并保留至少 12 个月。	**规定的方法测试程序** **5.3.4** 检查反恶意软件解决方案配置，核实是否根据要求 10.5.1 启用和保留了日志。	**目的** 务必跟踪反恶意软件机制的有效性—例如，通过确认是否按预期进行了更新和扫描，以及是否识别和处理了恶意软件。检查日志还允许实体确定恶意软件进入环境的具体方式，并跟踪其在实体网络内的活动。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 重要的是，防御机制应始终运行，以便实时检测到恶意软件。反恶意软件解决方案的临时启动和停止可能会使恶意软件在不被检查和发现的情况下传播。 **良好做法** 如果有合理需要暂时禁用系统的反恶意软件保护—例如，支持特定的维护活动或调查技术问题—适当的管理代表应理解采取这种行动的原因，并予以批准。对于反恶意软件机制的任何禁用或更改，包括在管理员自己的设备上的禁用或更改，都应由授权人员执行。一般认为，管理员拥有的特权可能允许他们禁用自己计算机上的反恶意软件，但当禁用此类软件时，应该要有警报机制，然后采取后续行动以确保正确程序得到遵循。 **示例** 在反恶意软件保护未激活期间，可能需要实施的其他安全措施包括在禁用反恶意软件保护时将未受保护的系统与互联网断开，并在重新启用后运行全面扫描。
5.3.5 用户不能禁用或更改反恶意软件机制，除非有明确记录并由管理层在有限时间内逐案授权。	**5.3.5.a** 检查反恶意软件配置，核实用户是否不能禁用或更改反恶意软件机制。	
定制方法目标 未经授权的人员不得修改反恶意软件机制。	**5.3.5.b** 询问负责人员并观察流程，核实任何禁用或更改反恶意软件机制的请求是否都有明确记录，并由管理层在有限的时间内逐案授权。	
适用性说明 仅当有合理技术需要时，经管理层逐案授权，才可以暂时禁用反恶意软件机制。如果出于特定目的需要禁用反恶意软件机制，必须经正式授权。在这些反恶意软件机制未被激活期间，可能还需要实施其他安全措施。		

要求和测试程序		指南
5.4 反钓鱼机制保护用户免受网络钓鱼攻击。		
规定的方法要求 **5.4.1** 制定流程和自动化机制，检测和保护人员免受网络钓鱼攻击。 **定制方法目标** 建立机制，防止和减轻网络钓鱼攻击所带来的风险。 **适用性说明** 本要求适用于自动化机制。并不打算将提供此类自动化机制的系统和服务（例如电子邮件服务器）纳入 PCI DSS 的范围。 本要求旨在保护能够访问 PCI DSS 范围内系统组件的人员。 满足这项检测和保护人员免受网络钓鱼的技术和自动控制要求，与安全意识培训的要求 12.6.3.1 有所不同。满足该要求并不同时满足为人员提供安全意识培训的要求，反之亦然。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **5.4.1** 观察已实施的流程并检查机制，核实是否制定了控制措施，以检测和保护人员免受网络钓鱼攻击。	**目的** 技术控制可以限制人员评估通信真实性的次数，也可以限制个人响应对网络钓鱼的影响。 **良好做法** 在开发反网络钓鱼控制措施时，鼓励实体考虑综合运用各种方法。例如，使用基于域的消息验证、报告和一致性（DMARC）、发件人政策框架（SPF）和域密钥识别邮件（DKIM）等反欺骗控制措施将有助于阻止钓鱼者欺骗实体的域和冒充人员。 部署用于在钓鱼邮件和恶意软件到达人员手中之前进行拦截的技术，例如链接洗涤器和服务器端反恶意软件，可以减少事件，并减少人员检查和报告网络钓鱼攻击的时间。此外，培训人员识别和报告网络钓鱼邮件，可以识别类似邮件并允许在打开之前将其删除。 建议（但不要求）在实体的整个组织中应用反网络钓鱼控制。 *（下一页继续）*

要求和测试程序		指南
		定义 网络钓鱼是社会工程的一种形式，描述了攻击者用来欺骗人员披露敏感信息的不同方法，例如用户帐户名和密码，以及帐户数据。攻击者通常会伪装自己，试图表现得像一个真正的或可信来源，引导人员发送电子邮件回复，点击网络链接，或将数据输入一个被威胁的网站。可以检测和防止网络钓鱼尝试的机制通常包含在反恶意软件解决方案中。 **更多信息** 有关网络钓鱼的更多信息，请参见以下内容： *国家网络安全中心 - 网络钓鱼攻击：保护您的组织。* *美国网络安全和基础设施安全局 - 报告钓鱼网站。*

要求 6：　开发和维护安全系统和软件

章节
6.1 确定和理解开发和维护安全系统和软件的流程和机制。
6.2 安全开发订制和定制软件。
6.3 识别并解决安全漏洞。
6.4 保护面向公众的 Web 应用程序免于攻击。
6.5 安全管理所有系统组件变更。

概述

恶意行为者可以利用安全漏洞来获得系统的特权访问。这些漏洞中有许多由供应商提供的安全补丁所修复，这些补丁必须由管理系统的实体来安装。所有系统组件必须具备所有适当的软件补丁，以防止恶意的个人和恶意软件对帐户数据的利用和威胁。

适当的软件补丁是指那些经过充分评估和测试的补丁，以确定该补丁不与现有的安全配置相冲突。对于订制和定制软件，通过应用软件生命周期（SLC）流程和安全编码技术，可以避免许多漏洞。

存储应用程序代码、系统配置或其他可能影响帐户数据或 CDE 安全的配置数据的代码库，属于 PCI DSS 评估的范围。

有关使用 PCI SSC 认证的软件和软件供应商的信息，以及使用 PCI SSC 的软件标准如何帮助满足要求 6 中的控制，请参见第 8 页的 *PCI DSS 和 PCI SSC 软件标准之间的关系*。

请参阅附录 G 了解 PCI DSS 术语的定义。

注：*要求 6 适用于所有系统组件，但关于安全开发软件的第 6.2 节除外，该节仅适用于 CDE 中包含或连接的任何系统组件上使用的订制和定制软件。*

要求和测试程序		指南
6.1 确定和理解开发和维护安全系统和软件的流程和机制。		
规定的方法要求 **6.1.1** 要求 6 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。	**规定的方法测试程序** **6.1.1** 检查文件并询问相关人员，核实是否根据本要求中规定的所有元素管理了要求 6 中确定的安全政策和操作程序。	**目的** 要求 6.1.1 涉及有效管理和维护整个要求 6 规定的各种政策和程序。虽然定义要求 6 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。
定制方法目标 受影响人员确定满足要求 6 内活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果没有正式分配角色和责任，则无法安全维护系统，其安全水平也随之降低。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。
6.1.2 记录、分配和理解执行要求 6 中活动的角色和责任。	**6.1.2.a** 检查文件，核实是否记录和分配了执行要求 6 中活动的角色和责任的描述。	
	6.1.2.b 询问负责执行要求 6 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	
定制方法目标		
分配执行要求 6 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。		

要求和测试程序		指南
6.2 安全开发订制和定制软件。		
规定的方法要求 **6.2.1** 安全开发订制和定制软件，具体如下： • 基于工业标准和/或安全开发的最佳实践。 • 根据 PCI DSS（例如，安全验证和日志记录）。 • 在软件开发生命周期的各个阶段纳入信息安全问题的考虑因素。 **定制方法目标** 在整个软件生命周期中，根据 PCI DSS 和安全开发流程开发订制和定制软件。 **适用性说明** 这适用于为实体开发或由实体开发供实体自用的所有软件。这包括订制和定制软件。这并不适用于第三方软件。	**规定的方法测试程序** **6.2.1** 检查书面软件开发程序，核实是否制定了相应流程，以包括本要求中规定的所有元素。	**目的** 如果在软件开发的需求定义、设计、分析和测试阶段不包括安全问题，则会无意中或恶意地将安全漏洞引入到生产环境中。 **良好做法** 了解应用程序如何处理敏感数据—包括何时存储、传输和存储在内存中—可以帮助确定需要保护的数据。 在开发软件时，必须考虑 PCI DSS 的要求，以便在设计上满足这些要求，而不是试图在以后对软件进行改造。 **示例** 安全软件生命周期管理方法和框架包括 PCI 安全软件框架、BSIMM、OPENSAMM，以及 NIST、ISO 和 SAFECode。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
6.2.2 从事订制和定制软件的软件开发人员至少每 12 个月接受一次培训，具体如下： • 与他们的工作职能和开发语言有关的软件安全。 • 包括安全软件设计和安全编码技术。 • 如果使用安全测试工具，包括如何使用这些工具来检测软件中的漏洞。	**6.2.2.a** 检查软件开发程序，核实是否制定了相应流程，以培训开发订制和定制软件的软件开发人员，并包括本要求中规定的所有元素。	拥有熟悉安全编码方法（包括要求 6.2.4 中确定的技术）的员工，将有助于最大限度地减少通过不良编码实践引入的安全漏洞数量。
定制方法目标	**6.2.2.b** 检查培训记录并询问相关人员，核实从事订制和定制软件的软件开发人员是否根据本要求规定的所有元素，接受了与他们的工作职能和开发语言相关的软件安全培训。	**良好做法**
软件开发人员熟知安全开发实践、软件安全以及所开发语言、框架或应用面临的攻击。相关人员在需要时能够获得援助和指导。		开发人员培训可以由内部或第三方提供。 培训应包括但不限于所使用的开发语言、安全软件设计、安全编码技术、使用发现代码中的漏洞的技术/方法、防止重新引入以前解决的漏洞的流程，以及如何使用任何自动安全测试工具来检测软件中的漏洞。 随着行业认可的安全编码实践发生变化，组织编码实践和开发人员培训可能需要更新以应对新威胁。

要求和测试程序		指南
规定的方法要求 **6.2.3** 在投入生产或向客户发布之前审核订制和定制软件，以识别和纠正潜在的编码漏洞，具体如下： • 代码审查确保代码根据安全编码准则开发。 • 代码审查寻找现有和新兴的软件漏洞。 • 在发布前实施适当纠正。 **定制方法目标** 无法通过编码漏洞利用订制和定制软件。 **适用性说明** 作为系统开发生命周期的一部分，这种对代码审查的要求适用于所有订制和定制软件（包括内部和面向公众的软件）。 面向公众的网络应用程序也应受到额外控制，以解决实施后的持续威胁和漏洞，如 PCI DSS 要求 6.4 所定义。 可以使用手动或自动流程，或两者结合执行代码审查。	**规定的方法测试程序** **6.2.3.a** 检查书面软件开发程序并询问负责人员，核实是否制定了相应程序，要求根据本要求中规定的所有元素审核所有订制和定制软件。 **6.2.3.b** 检查订制和定制软件变更的证据，核实是否根据本要求中规定的所有元素审核了代码变更。	**目的** 恶意者通过会利用订制和定制软件的安全漏洞，从而进入网络并威胁帐户数据。 存在漏洞的代码在部署或发布到生产环境中后，解决起来就更加困难，成本更加昂贵。要求管理层在发布前进行正式审核和签批，有助于确保代码得到批准，并按照政策和程序开发。 **良好做法** 以下项目应被考虑纳入代码审查中： • 搜索未记录的功能（植入工具、软件后门）。 • 确认软件是否安全地使用了外部组件的功能（数据库、框架、API 等）。例如，如果使用了提供加密功能的第三方数据库，核实它是否被安全地集成。 • 检查日志是否被正确使用，以防止敏感数据进入日志。 • 分析非安全代码结构，这些结构可能包含与要求 6.2.5 中确定的常见软件攻击有关的潜在漏洞。 • 检查应用程序的行为以检测逻辑漏洞。

要求和测试程序		指南
规定的方法要求 **6.2.3.1** 如果在发布到生产之前对订制和定制软件进行手动代码审查，则更改的代码： • 由非原代码作者进行审查，他们对代码审查技术和安全编码实践有所了解。 • 在发布之前，由管理层进行审查和批准。 **定制方法目标** 不能绕过手动代码审查流程，因为它能有效发现安全漏洞。 **适用性说明** 手动代码审查可以由具备相应知识的内部人员或具备相应知识的第三方人员执行。 被正式授予发布控制责任的个人，既不是原代码作者，也不是代码审查者，就符合作为管理层的标准。	**规定的方法测试程序** **6.2.3.1.a** 如果在发布到生产之前对订制和定制软件进行手动代码审查，则应检查书面软件开发程序并询问负责人员，核实是否制定了相应流程，以根据本要求规定的所有元素执行手动代码审查。 **6.2.3.1.b** 检查订制和定制软件变更的证据并询问相关人员进，核实是否根据本要求规定的所有元素执行了人工代码审查。	**目的** 由非原代码作者进行审查代码，他们在代码审查方面具备经验，并且对安全编码实践有所了解，可以将包含可能影响持卡人数据安全性的安全或逻辑错误的代码发布到生产环境中的可能性降至最低。要求管理层批准代码的审查，可以限制绕过该过程的可能性。 **良好做法** 拥有一个正式的审查方法和审查清单已被证明可以提高代码审查过程的质量。 代码审查是一个疲惫的过程，由于这个原因，当审查员每次只审查少量的代码时，它才是最有效的。 为了保持代码审查的有效性，监测审查员的总体工作量，让他们审查他们所熟悉的应用程序是有好处的。 可以使用手动或自动流程，或两者结合执行代码审查。 仅仅依靠手动代码审查的实体应确保审查员在发现新漏洞时通过定期培训保持其技能，并推荐新的安全编码方法。 **更多信息** 请参见 *OWASP 代码审查指南*。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 在软件开发过程中，尽早检测或预防导致脆弱代码的常见错误，可以降低这种错误进入生产并导致威胁的概率。在开发过程中嵌入正式的工程技术和工具可以及早发现这些错误。这种理念有时称为"安全左移"。 **良好做法** 对于订制和定制软件，实体必须确保代码的开发着重于预防或减轻常见的软件攻击，包括： • 试图利用常见的编码漏洞（程序错误）。 • 试图利用软件设计缺陷。 • 试图利用实施/配置缺陷。 • 枚举攻击 - 在支付中积极利用的自动攻击，并滥用识别、验证或授权机制。请参见 *PCI Perspectives 博客文章"警惕帐户测试攻击"*。 研究和记录软件工程技术或其他方法，有助于确定软件开发人员如何通过他们在软件中构建的功能或对策来防止或减轻各种软件攻击。这可能包括识别/验证机制、访问控制、输入认证程序等。开发人员应熟悉不同类型的漏洞和潜在的攻击，并在开发代码时使用措施来避免潜在的攻击载体。 **示例** 技术包括在开发周期早期扫描代码以确认不存在漏洞的自动化流程和实践。
6.2.4 确定软件工程技术或其他方法，并由软件开发人员用于使用，以防止或减轻订制和定制软件的常见攻击和相关漏洞，包括但不限于以下方面： • 注入攻击，包括 SQL、LDAP、XPath 或其他命令、参数、对象、故障或注入型缺陷。 • 针对数据和数据结构的攻击，包括试图操纵缓冲区、指针、输入数据或共享数据。 • 针对强效加密法使用的攻击，包括试图利用薄弱、非安全或不适当的强效加密法实施、算法、密文套件或操作模式。 • 针对业务逻辑的攻击，包括试图通过操纵 API、通信协议和渠道、客户端功能或其他系统/应用程序功能和资源，滥用或绕过应用程序的特性和功能。这包括跨站脚本（XSS）和跨站请求伪造（CSRF）。 • 针对访问控制机制的攻击，包括试图绕过或滥用识别、验证或授权机制，或试图利用此类机制实施中的弱点。 • 通过要求 6.3.1 规定的漏洞识别过程中确定的任何"高风险"漏洞进行攻击。	**6.2.4** 检查书面程序并询问负责的软件开发人员，核实是否确定了软件工程技术或其他方法，并由订制和定制软件的开发人员使用，以防止或减轻本要求中规定的所有常见软件攻击。	

要求和测试程序		指南
定制方法目标 不能通过常见的攻击和相关漏洞利用订制和定制软件。 **适用性说明** 这适用于为实体开发或由实体开发供实体自用的所有软件。这包括订制和定制软件。这并不适用于第三方软件。		

要求和测试程序		指南
6.3 识别并解决安全漏洞。		
规定的方法要求	**规定的方法测试程序**	**目的**
6.3.1 识别并管理安全漏洞，具体如下： • 利用行业公认的安全漏洞信息来源，包括国际和国家计算机应急响应小组（CERT）的警报，确定新的安全漏洞。 • 根据行业最佳实践并针对潜在影响，对漏洞进行风险排序。 • 风险等级至少要确定所有被认为是高风险或对环境至关重要的漏洞。 • 订制和定制软件以及第三方软件（例如操作系统和数据库）的漏洞都包括在内。	**6.3.1.a** 检查识别和管理安全漏洞的政策和程序，以核实是否根据了本要求中规定的所有元素识别和管理了安全漏洞。 **6.3.1.b** 询问负责人员，检查文件和观察过程，以核实是否根据了本要求中规定的所有元素识别和管理了安全漏洞。	分类风险（例如，分为关键、高、中或低），使组织能够更快地识别、优先处理最高风险的项目，并减少构成最大风险的漏洞被利用的可能性。 **良好做法** 评估漏洞和分配风险等级的方法将根据组织的环境和风险评估战略而有所不同。 当实体分配其风险等级时，它应考虑使用正式的、客观的、合理的方法，准确地描述与组织有关的漏洞的风险，并转化为适当的实体分配的优先解决方案。 一个组织管理漏洞的流程应与其他管理流程相结合—例如，风险管理、变更管理、补丁管理、事件响应、应用安全，以及对这些流程的适当监控和记录。这将有助于确保正确识别和解决所有漏洞。流程应支持对漏洞的持续评估。例如，一个最初被认定为低风险的漏洞后来可能会变成高风险。此外，单独被认为是低风险或中等风险的漏洞，如果存在于同一系统中，或者如果在可能导致访问 CDE 的低风险系统上被利用，则可能共同构成高风险或关键风险。 *（下一页继续）*
定制方法目标 监控、编目和风险评估可能影响帐户数据或 CDE 安全的新系统和软件漏洞。		
适用性说明 本要求并非通过为要求 11.3.1 和 11.3.2 执行的漏洞扫描来实现的，也不等同于要求 11.3.1 和 11.3.2 的漏洞扫描。本要求是一个过程，以积极监控行业来源的漏洞信息，并由实体确定与每个漏洞相关的风险等级。		

要求和测试程序		指南
		示例 国家计算机应急准备/响应小组（CERT）和供应商等一些组织会发布警报，就需要立即修补/更新的紧急漏洞向实体提出建议。 漏洞排序的标准可能包括事件响应和安全小组论坛（FIRST）或 CERT 的警报中确定的漏洞的重要性，考虑 CVSS 得分，供应商的分类和/或受影响系统的类型。 **更多信息** 可信的漏洞信息来源包括供应商网站、行业新闻组、邮件列表等。如果软件由内部开发，内部开发团队也应考虑可能影响内部开发的应用程序的新漏洞的信息来源。其他确保识别新漏洞的方法包括自动识别并在发现异常行为时发出警报的解决方案。这些程序应考虑到广泛公布的漏洞以及“零日”攻击，这些攻击针对以前未知的漏洞。 对于订制和定制的软件，组织可以从公共可信来源（例如，特殊资源和组件开发商的资源）获得有关数据库、框架、编译器、编程语言等信息。组织也可以独立分析第三方组件并识别漏洞。 *（下一页继续）*

要求和测试程序		指南
		对于控制内部开发的软件，组织可以从外部来源获得此类信息。组织可以考虑使用“漏洞回报奖励”计划，在该计划中发布信息（例如，在其网站上），以便第三方可以联系该组织提供漏洞信息。外部来源可以包括独立调查员或公司，他们向组织报告所发现的漏洞，并可能包括通用漏洞评分系统（CVSS）或 OWASP 风险评级方法等来源。
规定的方法要求 **6.3.2** 维护订制和定制软件以及纳入订制和定制软件的第三方软件组件的清单，以促进漏洞和补丁管理。 **定制方法目标** 不能在订制和定制软件中利用第三方软件组件中的已知漏洞。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **6.3.2.a** 检查文件并询问相关人员，以核实是否维护了订制和定制软件以及纳入订制和定制软件的第三方软件组件的清单，以及该清单是否被用于识别和处理漏洞。 **6.3.2.b** 检查软件文档，包括集成了第三方软件组件的订制和定制软件，并将其与清单进行比较，以核实清单是否包括订制和定制软件和第三方软件组件。	**目的** 识别并列出所有实体的订制和定制软件以及纳入实体订制和定制软件的任何第三方软件，使实体能够管理漏洞和补丁。 嵌入实体软件的第三方组件（包括数据库、API 等）的漏洞也使这些应用程序容易受到攻击。了解实体软件中使用的第三方组件，并监控安全补丁的可用性以解决已知的漏洞，这对确保软件的安全性至关重要。 **良好做法** 某实体的清单应涵盖所有支付软件组件和依赖条件，包括支持的执行平台或环境、第三方数据库、服务和其他必要功能。 许多不同类型的解决方案可以帮助管理软件清单，例如软件组成分析工具、应用程序发现工具和移动设备管理。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
6.3.3 通过安装以下适用的安全补丁/更新，保护所有系统组件免受已知漏洞的影响。 • 根据要求 6.3.1 的风险等级过程，确定关键或高度安全的补丁/更新。 • 所有其他适用的安全补丁/更新在实体确定的适当时间范围内安装（例如，在发布后三个月内）。	**6.3.3.a** 检查政策和程序，核实是否制定了相应程序，以根据本要求中规定的所有元素安装适用的安全补丁/更新来解决漏洞。	不断发现新的漏洞，这些漏洞可以允许对以前被认为安全的系统进行攻击。如果不尽快在关键系统上实施最新的安全补丁/更新，恶意行为者可以利用这些漏洞来攻击或禁用系统，或获取敏感数据的访问权限。
定制方法目标	**6.3.3.b** 检查系统组件和相关软件，并将已安装的安全补丁/更新列表与最新的安全补丁/更新信息进行比较，以核实是否根据本要求中规定的所有元素解决了漏洞。	**良好做法**
不能通过利用一个已知的漏洞威胁系统组件。		优先考虑关键基础设施的安全补丁/更新，以确保在补丁发布后尽快保护高优先级的系统和设备免受漏洞影响。 某实体的修补程序应考虑到任何重新评估漏洞和随后根据要求 6.3.1 改变漏洞的关键性的因素。例如，一个最初被认定为低风险的漏洞后来可能会变成高风险。此外，单独被认为是低风险或中等风险的漏洞，如果存在于同一系统中，或者如果在可能导致访问 CDE 的低风险系统上被利用，则可能共同构成高风险或关键风险。

要求和测试程序		指南
6.4 保护面向公众的 Web 应用程序免于攻击。		
规定的方法要求	**规定的方法测试程序**	**目的** 面向公众的网络应用程序是指那些可供公众使用的应用程序（不只限于内部使用）。这些应用程序是攻击者的主要目标，编码不良的网络应用程序为攻击者提供了便捷途径，以获取敏感数据和系统的访问权限。 **良好做法** 手动或自动漏洞安全评估工具或方法审核和/或测试应用程序的漏洞。 常见的评估工具包括专门的网络扫描器，可对网络应用程序保护进行自动分析。 当使用自动化技术解决方案时，务必包括促进及时响应解决方案产生的警报的流程，以便可以缓解任何检测到的攻击。 **示例** 网络应用程序防火墙（WAF），安装在面向公众的网络应用程序前面，以检查所有流量，这是一个自动技术解决方案的例子，可以检测和防止基于网络的攻击（例如，要求 6.2.4 中包括的攻击）。WAF 在应用层过滤和阻止非必要的流量。正确配置的 WAF 有助于防止应用层对编码或配置不当的应用程序的攻击。 *（下一页继续）*
6.4.1 对于面向公众的网络应用程序，要不断解决新的威胁和漏洞，并保护这些应用程序免于以下已知的攻击： • 通过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，具体如下： – 至少每 12 个月审核一次，并在重大变更之后审核。 – 审核由一个专门从事应用安全的实体执行。 – 审核至少包括要求 6.2.4. 中所有常见的软件攻击。 – 根据要求 6.3.1 对所有漏洞进行排序。 – 纠正所有漏洞。 – 纠正后，重新评估应用程序。 **或** • 安装自动技术解决方案，持续检测和防止基于网络的攻击，具体如下： – 安装在面向公众的网络应用程序前，以检测和防止基于网络的攻击。 – 积极运行并在适用的情况下进行更新。 – 创建检查日志。 – 配置为阻止基于网络的攻击，或产生一个警报，并立即进行调查。	**6.4.1** 对于面向公众的网络应用程序，确保以下所需方法中的任何一种已经到位： • 如果使用手动或自动漏洞安全评估工具或方法，检查书面流程，询问相关人员，并检查应用程序安全评估的记录，以核实是否根据本要求中特定于工具/方法的所有元素审核了面向公众的网络应用程序。 **或** • 如果安装了自动化技术解决方案以持续检测和防止基于网络的攻击，检查系统配置设置和检查日志并询问负责人员，核实是否根据本要求中针对该解决方案的所有元素安装了自动化技术解决方案。	

要求和测试程序		指南
定制方法目标 保护面向公众的网络应用程序免受恶意攻击。 **适用性说明** 本评估与要求 11.3.1 和 11.3.2 的漏洞扫描不同。 本要求将在 2025 年 3 月 31 日要求 6.4.2 生效后被要求 6.4.2 所取代。		自动技术解决方案的另一个例子是运行时应用程序自我保护（RASP）技术。如果实施得当，RASP 解决方案可以检测并阻止软件在执行过程中的异常行为。WAF 通常监控应用程序周边，而 RASP 解决方案则监控和阻止应用程序内的行为。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
6.4.2 对于面向公众的网络应用程序，部署一个自动化技术解决方案，以持续检测和防止基于网络的攻击，至少要具备以下条件： • 安装在面向公众的网络应用程序前，并被配置为检测和防止基于网络的攻击。 • 积极运行并在适用的情况下进行更新。 • 创建检查日志。 • 配置为阻止基于网络的攻击，或产生一个警报，并立即进行调查。	**6.4.2** 对于面向公众的网络应用程序，检查系统配置设置和检查日志，并询问负责人员，以核实检测和防止基于网络的攻击的自动化技术解决方案的制定是否按照本要求规定的所有元素。	面向公众的网络应用程序是攻击者的主要目标，编码不良的网络应用程序为攻击者提供了便捷途径，以获取敏感数据和系统的访问权限。 **良好做法** 当使用自动化技术解决方案时，务必包括促进及时响应解决方案产生的警报的流程，以便可以缓解任何检测到的攻击。这类解决方案也可用于自动缓解，例如，速率限制控制，可用于缓解蛮力攻击和枚举攻击。 **示例** 网络应用程序防火墙（WAF），可以是内部的，也可以是基于云的，安装在面向公众的网络应用程序前面，以检查所有流量，这是一个自动技术解决方案的例子，可以检测和防止基于网络的攻击（例如，要求 6.2.4 中包括的攻击）。WAF 在应用层过滤和阻止非必要的流量。正确配置的 WAF 有助于防止应用层对编码或配置不当的应用程序的攻击。
定制方法目标		
实时保护面向公众的网络应用程序免受恶意攻击。		
适用性说明		
这项新要求一旦达到生效日期，将取代要求 6.4.1。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求 **6.4.3** 管理所有在消费者的浏览器中加载和执行的支付页面脚本，具体如下： • 实施一种方法来确认每个脚本都经过授权。 • 实施一种方法来保证每个脚本的完整性。 • 保留所有脚本的清单，并以书面形式说明为什么每个脚本是必要的。 **定制方法目标** 当支付页面在消费者的浏览器中呈现时，未经授权的代码不能出现在该页面中。 **适用性说明** 本要求适用于从实体环境中加载的所有脚本以及从第三方和第四方加载的脚本。 ***本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。***	**规定的方法测试程序** **6.4.3.a** 检查政策和程序，核实是否制定了相应程序，根据本要求规定的所有元素管理在消费者浏览器中加载和执行的所有支付页面脚本。 **6.4.3.b** 询问负责人员，检查库存记录和系统配置，以核实是否根据本要求规定的所有元素管理了所有在消费者浏览器中加载和执行的支付页面脚本。	**目的** 对于支付页面中加载和执行的脚本，其功能可以在实体不知情的情况下改变，也可以具有加载额外外部脚本的功能（例如，广告和跟踪、标签管理系统）。 这种看似无害的脚本可以被潜在的攻击者用来上传恶意脚本，从而从消费者浏览器中读取和渗出持卡人数据。 确保所有这些脚本的功能都被理解为是支付页面操作所必需的，从而最大限度地减少可能被篡改的脚本数量。 确保脚本已被明确授权，可以减少不必要的脚本在未经适当管理部门批准的情况下被添加到支付页面的概率。 使用防止篡改脚本的技术，可以最大限度地减少脚本被修改以进行未经授权的行为的概率，例如从支付页面上盗取持卡人数据。 **良好做法** 可以通过手动或自动（如工作流）流程授权脚本。 如果支付页面将被加载到内联框架（IFRAME）中，使用父页面的内容安全策略（CSP）限制支付页面可以加载的位置，可以帮助防止未经授权的内容被替换为支付页面。 *（下一页继续）*

要求和测试程序		指南
		定义 本要求中的“必要”是指，实体对每个脚本的审核证明并确认为什么支付页面的功能需要接受支付交易。 **示例** 可以通过几种不同的机制执行脚本的完整性，包括但不限于： • 子资源完整性（SRI），它允许消费者浏览器认证一个脚本没有被篡改过。 • CSP，它限制消费者浏览器可以从哪些地方加载脚本，并将帐户数据传送到哪些地方。 • 专有的脚本或标签管理系统，可以防止恶意的脚本执行。

要求和测试程序		指南
6.5 安全管理所有系统组件变更。		
规定的方法要求	**规定的方法测试程序**	**目的**
6.5.1 根据既定的程序变更生产环境中的所有系统组件，其中包括： • 变更的原因和描述。 • 记录安全影响。 • 记录授权方批准的变更。 • 测试以核实该变更不会对系统安全产生不利影响。 • 对于订制和定制软件变更，测试所有更新以在其部署到生产中之前符合要求 6.2.4。 • 处理故障并返回到安全状态的程序。	**6.5.1.a** 检查书面变更控制程序，以核实是否制定了相应程序，以便生产环境中所有系统组件的变更包括本要求中规定的所有元素。	变更管理程序必须适用于所有变更，包括在生产环境中对任何系统组件的增加、移除或修改。务必记录变更的原因和变更的描述，以便相关各方理解并同意变更的必要性。同样，记录变更的影响允许所有受影响的各方为任何处理变更作出适当计划。
定制方法目标	**6.5.1.b** 检查系统组件的最近变更，并将这些变更追溯到相关变更控制文件。对于所检查的每项变更，核实是否根据本要求中规定的所有元素实施了该变更。	**良好做法**
跟踪、授权所有变更并对其影响和安全性进行评估，同时对变更进行管理，以避免对系统组件的安全产生意外影响。		授权方予以批准，确认变更属于合法，并且变更经组织批准。变更应该由具有适当权力和知识的个人批准，以了解变更的影响。 实体执行彻底测试，确认环境的安全性不会因为实施变更而有所降低，并且所有现有的安全控制在变更后仍然存在或被同等或更强的安全控制所取代。要执行的特定测试将根据变更的类型和受影响的系统组件而有所不同。 对于每项变更，务必制定书面程序,以解决任何故障，并提供指示，说明如何在变更失败或对应用程序或系统的安全产生不利影响时返回到安全状态。这些程序将允许应用程序或系统恢复到其先前的安全状态。

要求和测试程序		指南
规定的方法要求 **6.5.2** 在完成重大变更后，确认所有相关的 PCI DSS 要求是否在所有新的或变更后的系统和网络上实施，文件是否视情况进行更新。 **定制方法目标** 在发生重大变更后，核实所有系统组件是否符合适用的 PCI DSS 要求。 **适用性说明** 根据要求 12.5.2，也应该在实体的年度 PCI DSS 范围确认活动中记录和反映这些重大变更。	**规定的方法测试程序** **6.5.2** 检查重大变更的文件，询问相关人员，并观察受影响的系统/网络，以核实该实体确认的适用 PCI DSS 要求是否在所有新的或变更后的系统和网络上实施，文件是否视情况进行更新。	**目的** 拥有分析重大变更的流程有助于确保所有适当的 PCI DSS 控制措施适用于范围内环境中增加或改变的任何系统或网络，并确保继续满足 PCI DSS 要求以确保环境安全。 **良好做法** 将这种认证纳入到变更管理流程中，有助于确保设备清单和配置标准保持最新，并在需要时应用安全控制。 **示例** 可能受影响的适用 PCI DSS 要求包括但不限于： • 更新网络图和数据流程图以反映变更。 • 根据配置标准对系统进行配置，更改所有默认密码并禁用多余的服务。 • 系统通过所需的控制受到保护—例如，文件完整性监控（FIM）、反恶意软件、补丁和检查日志。 • 不存储敏感验证数据，记录所有帐户数据存储并将其纳入数据保留政策和程序。 • 新系统包括在每季度的漏洞扫描过程中。 • 根据要求 11.3.1.3 和 11.3.2.1，在发生重大变化后，对系统进行扫描以检测是否有内部和外部漏洞。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 由于生产前环境的状态不断变化，它们的安全性往往低于生产环境。 **良好做法** 组织必须清楚地了解哪些环境是测试环境或开发环境，以及这些环境如何在网络和应用程序层面上进行互动。 **定义** 生产前环境包括开发、测试、用户验收测试（UAT）等。即使生产基础设施被用来促进测试或开发，生产环境仍然需要（在逻辑上或物理上）与生产前功能分离，以便因生产前活动而引入的漏洞不会对生产系统产生不利影响。
6.5.3 生产前环境与生产环境隔离开来，并通过访问控制来实施分离。	**6.5.3.a** 检查政策和程序，核实是否制定了相应程序，通过强制隔离的访问控制，将生产前环境与生产环境隔离开来。	
	6.5.3.b 检查网络文件和网络安全控制配置，以核实生产前环境是否与生产环境隔离开来。	
定制方法目标	**6.5.3.c** 检查访问控制设置，核实是否制定了访问控制，以在生产前环境和生产环境之间强制隔离。	
生产前环境不能将风险和漏洞引入生产环境。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
6.5.4 角色和功能在生产和生产前环境之间隔离开来，以提供问责制机制，从而只部署经过审核和批准的变更。	**6.5.4.a** 检查政策和程序，核实是否制定了相应程序，以将角色和功能隔离开来并提供问责机制，从而只部署经过审核和批准的变更。	在生产环境和生产前环境之间分离角色和功能旨在减少能够访问生产环境和帐户数据的人员数量，从而将未经授权、无意或不适当地访问数据和系统组件的风险降至最低，并帮助确保访问权限仅限于那些有业务需求的个人。 这种控制的意图是将关键活动隔离开来，以提供监督和审核，捕捉错误，并将欺诈或盗窃的机会降到最低（因为需要两人串通起来才能隐藏一项活动）。 将角色和职能隔离开来，也称为职责隔离或分离，是保护实体资产的一个关键的内部控制概念。
定制方法目标	**6.5.4.b** 观察程序并询问相关人员，以核实已实施的控制措施是否将角色和功能隔离开来并提供问责机制，以便只部署经过审核和批准的变更。	
确定和管理区分生产前和生产活动的工作角色和责任，以最大限度地减少未经授权、非故意或不适当的行动的风险。		
适用性说明		
在人员有限的环境中，个人执行多种角色或功能，可以通过提供问责机制的额外程序控制来实现这一目标。例如，一名开发人员可能也是一名管理员，他在开发环境中使用一个具有高级权限的管理员级帐户，而对于他们的开发人员角色，他们使用一个具有用户级访问生产环境的单独帐户。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 在受保护的 CDE 之外使用实时 PAN，使恶意者有机会获得持卡人数据的未授权访问权限。 **良好做法** 实体可以最大限度地减少他们对实时 PAN 的存储，只在为特定和规定的测试目的严格需要时在生产前存储它们，并在使用后安全地删除该数据。 如果实体需要专门为测试目的设计的 PAN，可以从收单机构获得。 **定义** 实时 PAN 是指有可能被用来进行支付交易的有效 PAN（不是测试 PAN）。此外，当支付卡过期时，相同的 PAN 经常以不同的到期日被重新使用。在将所有 PAN 移出 PCI DSS 范围之前，必须核实其是否不能进行支付交易。该实体有责任确认 PAN 不是实时的。
6.5.5 实时 PAN 不在生产前环境中使用，除非这些环境包含在 CDE 中，并根据所有适用的 PCI DSS 要求进行保护。	**6.5.5.a** 检查政策和程序，核实是否制定了相应流程，以使实时 PAN 不在生产前环境中使用，除非这些环境包含在 CDE 中，并根据所有适用的 PCI DSS 要求进行保护。	
	6.5.5.b 观察测试流程并询问相关人员，核实是否制定了相应程序，以确保在生产前环境中不使用实时 PAN，除非这些环境处于 CDE 中，并根据所有适用的 PCI DSS 要求进行保护。	
定制方法目标	**6.5.5.c** 检查生产前测试数据，核实实时 PAN 不在生产前环境中使用，除非这些环境处于 CDE 中，并根据所有适用的 PCI DSS 要求进行保护。	
实时 PAN 不能出现在非 CDE 的生产前环境中。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
6.5.6 在系统投入生产前，移除系统组件中的测试数据和测试帐户。	**6.5.6.a** 检查政策和程序，核实是否制定了相应程序，以在系统投入生产前移除系统组件中的测试数据和测试帐户。	这些数据可能会泄露有关应用程序或系统运作的信息，对于未经授权的个人来说，是一个易于利用来获取系统的访问权限的目标。拥有这些信息可能会促进系统和相关帐户数据的威胁。
	6.5.6.b 观察现成软件和内部应用程序的测试过程，并询问工作人员，以核实在系统投入生产之前，测试数据和测试帐户是否已被移除。	
定制方法目标	**6.5.6.c** 检查最近安装或更新的现成软件和内部应用程序的数据和帐户，以核实在生产的系统上是否没有测试数据或测试帐户。	
测试数据和测试帐户不能存在于生产环境中。		

实施强有力的访问控制措施

要求 7:　　根据"必须知道"原则限制系统组件和持卡人数据的访问权限

章节
7.1 确定并理解根据"必须知道"原则限制系统组件和持卡人数据的访问权限的程序和机制。
7.2 适当确定和分配系统组件和数据的访问权限。
7.3 通过访问控制系统管理系统组件和数据的访问权限。

概述

由于无效的访问控制规则和定义，未经授权的个人可能获得关键数据或系统的访问权限。为了确保关键数据只能由授权人员访问，必须建立相应系统和流程，根据"必须知道"原则和工作职责限制访问权限。

"访问"或"访问权限"是由提供用户访问系统、应用程序和数据的规则创建的，而"权限"允许用户执行与该系统、应用程序或数据有关的特定操作或功能。例如，某名用户可能拥有特定数据的访问权限，但他们是否只能阅读该数据，或者也能更改或删除该数据，这由用户分配的权限决定。

"必须知道"是指只提供执行工作所需的最少数据的访问权限。

"最小权限"是指只提供执行工作所需的最低级别的权限。

这些要求适用于用户帐户和雇员、承包商、顾问以及内部和外部供应商和其他第三方（例如，提供支持或维护服务的人）的访问权限。部分要求也适用于实体使用的应用程序和系统帐户（也称为 "服务帐户"）。

这些要求不适用于消费者（持卡人）。

请参阅附录 G 了解 PCI DSS 术语的定义。

要求和测试程序		指南
7.1 确定并理解根据“必须知道”原则限制系统组件和持卡人数据的访问权限的程序和机制。		
规定的方法要求 **7.1.1** 要求 7 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。 **定制方法目标** 受影响人员确定满足要求 7 的活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。	**规定的方法测试程序** **7.1.1** 检查文件并询问相关人员，以核实是否根据本要求中规定的所有元素管理了要求 7 中确定的安全政策和操作程序。	**目的** 要求 7.1.1 涉及有效管理和维护整个要求 7 规定的各种政策和程序。虽然定义要求 7 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。

要求和测试程序		指南
规定的方法要求 **7.1.2** 记录、分配和理解执行要求 7 中活动的角色和责任。 **定制方法目标** 分配执行要求 7 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。	**规定的方法测试程序** **7.1.2.a** 检查文件，以核实是否记录和分配了执行要求 7 中活动的角色和责任的描述。 **7.1.2.b** 询问负责执行要求 7 中的活动的人员，以核实是否分配了角色和责任，这些角色和责任是否被理解。	**目的** 如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。

要求和测试程序		指南
7.2 适当地确定和分配系统组件和数据的访问权限。		
规定的方法要求	**规定的方法测试程序**	**目的**
7.2.1 制定了一个访问控制模型，包括授予访问权限，具体如下： • 根据实体的业务和访问需求，进行适当访问。 • 系统组件和数据资源的访问权限，基于用户的工作分类和功能。 • 执行工作职能所需的最小权限（例如，用户、管理员）。	**7.2.1.a** 检查书面政策和程序并询问相关人员，以核实是否根据本要求规定的所有元素制定了访问控制模型。	定义一个适合实体技术和访问控制理念的访问控制模型，支持以一致和统一的方式分配访问权限，并减少错误的可能性，例如授予过多的权利。
定制方法目标	**7.2.1.b** 检查访问控制模型设置，以核实是否根据本要求规定的所有元素适当确定了访问需求。	**良好做法**
根据工作职能，按照最小权限和“必须知道”原则，确定访问要求。		确定访问需求时需要考虑的一个因素是职责分离原则。该原则是为了防止欺诈和滥用或盗窃资源。例如，1）在不同的个人和/或职能部门之间划分任务关键职能和信息系统支持职能，2）建立角色，使信息系统支持活动由不同的职能部门/个人执行（例如，系统管理、编程、配置管理、质量保证和测试以及网络安全），以及 3）确保管理访问控制职能的安全人员不同时管理审计职能。 在个人执行多种功能的环境中，例如管理和安全操作，职责的分配方式必须使任何个人在没有独立检查点的情况下无法对某过程进行端到端的控制。例如，配置的责任和批准修改的责任可以分配给不同的人。 *（下一页继续）*

要求和测试程序		指南
		定义 访问控制模型的关键因素包括： • 需要保护的资源（需要访问的系统/设备/数据）、 • 需要访问该资源的工作职能（例如，系统管理员、呼叫中心人员、店员），以及 • 每个工作职能需要执行的活动（例如，读/写或查询）。 在确定工作职能、资源和每个工作职能的活动后，个人便可获得相应的访问权限。 **示例** 实体可以考虑的访问控制模型包括基于角色的访问控制（RBAC）和基于属性的访问控制（ABAC）。一个给定实体所使用的访问控制模式取决于他们的业务和访问需求。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
7.2.2 根据以下情况分配访问权限给用户，包括特权用户： • 工作分类和职能。 • 履行工作职责所需的最小权限。	**7.2.2.a** 检查政策和程序，以核实它们是否根据本要求规定的所有元素为用户分配了访问权限。	分配最小权限有助于防止缺乏了解应用程序的用户错误地或意外地改变应用程序配置或改变其安全设置。如果未经授权的人员获取用户 ID 的访问权限，强制执行最小权限还有助于将损害范围降到最低。
	7.2.2.b 检查用户访问设置，包括特权用户的访问设置，并询问负责管理人员，以核实所分配的特权是否符合本要求中规定的所有元素。	**良好做法**
定制方法目标	**7.2.2.c** 询问负责分配访问权限的人员，以核实特权用户的访问权限是否按照本要求规定的所有元素分配。	通过分配给一个或几个功能来授予用户访问权限。根据具体的用户职能和工作所需的最小范围来分配访问权限。
系统和数据的访问权限仅限于执行工作职能所需的访问权限，例如相关访问角色中所确定的那样。		在分配特权访问时，重要的是只给个人分配他们执行工作所需的权限（“最小权限”）。例如，不应该为数据库管理员或备份管理员分配与整个系统管理员相同的权限。 在确定用户职能的需求（根据 PCI DSS 要求 7.2.1）后，通过使用已创建的角色，可以轻松地根据个人的工作分类和职能授予个人访问权限。 各实体可能希望考虑使用特权访问管理（PAM），这是一种仅在需要特权时授予特权帐户访问权限的方法，一旦不再需要该权限，将立即撤销。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
7.2.3 授权人员批准所需的特权。	**7.2.3.a** 检查政策和程序，核实是否制定了相应流程，以由授权人员批准所有特权。	书面批准（例如，书面或电子形式），保证那些拥有访问权限和特权的人是已知的，并经管理层授权，而且他们的访问权限对其工作职能来说是必要的。
	7.2.3.b 检查用户 ID 和分配的权限，并与书面批准进行比较，以核实： • 所分配的权限是否有书面批准。 • 该批准是否由授权人员作出。 • 指定的权限是否与分配给个人的角色相符。	
定制方法目标		
如果没有适当的书面授权，不能向用户授予访问权限。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
7.2.4 审核所有用户帐户和相关访问权限，包括第三方/供应商帐户，具体如下： • 至少每 6 个月审核一次。 • 确保用户帐户和访问权限根据工作职能保持适当。 • 处理任何不适当的访问权限。 • 管理层确认访问权限仍然适当。	**7.2.4.a** 检查政策和程序，核实它们是否确定了相应流程，以根据本要求规定的所有元素审核所有用户帐户和相关访问权限，包括第三方/供应商帐户。	定期审核访问权限，有助于发现在用户工作职责变更、系统功能变更或其他修改后剩余的过度访问权限。如果没有适时撤销过度用户权限，恶意用户可能会将其用于未经授权的访问。 这种审核提供了另一个机会，以确保所有离职用户的帐户已被删除（如果在离职时遗漏了任何帐户），以及确保任何不再需要访问的第三方的访问权限已被终止。
定制方法目标	**7.2.4.b** 询问负责人员，检查用户帐户定期审核的书面结果，以核实所有结果是否符合本要求规定的所有元素。	**良好做法**
管理层定期审核帐户权限分配是否正确，并对违规情况进行补救。		当一个用户转到一个新的角色或一个新的部门时，通常不再需要与他们以前的角色相关的特权和访问权限。继续访问不再需要的特权或功能可能会带来滥用或错误的风险。因此，当职责发生变化时，重新认证访问权限的流程有助于确保用户的访问权限适合于用户的新职责。 各实体可以考虑实施一个定期的、可重复的流程，以审核访问权限，并指定“数据所有者”，后者负责管理和监控与其工作职能相关的数据的访问权限，同时确保用户访问权限保持最新和适当。举例来说，直属经理可以每月审核团队的访问权限，而高级经理则每季度审核他们小组的访问权限，两者都视需要对访问权限进行更新。这些最佳实践的目的是支持和促进至少每 6 个月执行一次审核。
适用性说明		
本要求适用于所有用户帐户和相关访问权限，包括人员和第三方/供应商使用的帐户，以及用于访问第三方云服务的帐户。 关于应用程序和系统帐户的控制，请参见要求 7.2.5 和 7.2.5.1 以及 8.6.1 至 8.6.3。 ***本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。***		

要求和测试程序		指南
规定的方法要求 **7.2.5** 分配和管理所有应用程序和系统帐户和相关访问权限，具体如下： • 基于系统或应用程序可操作性所需的最小权限。 • 访问权限仅限于特别需要使用它们的系统、应用程序或流程。 **定制方法目标** 授予应用程序和系统帐户的访问权限只限于该应用程序或系统可操作性所需的访问权限。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **7.2.5.a** 检查政策和程序，核实它们是否确定了相应流程，以根据本要求规定的所有元素管理和分配所有应用程序和系统帐户及相关访问权限。 **7.2.5.b** 检查与系统和应用程序帐户相关的权限并询问负责人员，以核实是否根据本要求中规定的所有元素分配和管理了应用程序和系统帐户以及相关访问权限。	**目的** 务必为应用程序或系统帐户建立适当的访问级别。如果这些帐户被威胁，恶意用户将获得与授予应用程序或系统相同的访问级别。因此，必须确保根据用户帐户相同的基础授予系统和应用程序帐户的有限访问权限。 **良好做法** 各实体可考虑在设置这些应用程序和系统帐户时建立一个基线，包括适用于本组织的以下内容： • 确保该帐户不是特权组的成员，例如域管理员、本地管理员或根用户。 • 限制该帐户可以在哪些计算机上使用。 • 限制使用时间。 • 删除任何额外设置，如 VPN 访问和远程访问。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
7.2.5.1 审核所有应用程序和系统帐户的访问以及相关访问权限，具体如下： • 定期执行（按照实体的目标风险分析中定义的频率，即根据要求 12.3.1 中规定的所有元素执行）。 • 对于正在执行的功能来说，应用程序/系统访问仍然适当。 • 处理任何不适当的访问权限。 • 管理层确认访问权限仍然适当。	**7.2.5.1.a** 检查政策和程序，核实它们是否确定了相应流程，以根据本要求规定的所有元素审核所有应用程序和系统帐户及相关访问权限。	定期审核访问权限，有助于发现在系统功能变更或其他应用或系统修改发生后剩余的过度访问权限。如果过度的权限不再需要时没有撤销，恶意用户可能会将其用于未经授权的访问。
定制方法目标	**7.2.5.1.b** 检查实体的目标风险分析，了解应用程序和系统帐户及相关访问权限的定期审核频率，以核实是否根据要求 12.3.1 规定的所有元素执行了风险分析。	
管理层定期审核应用程序和系统帐户的权限分配是否正确，并对违规情况进行补救。	**7.2.5.1.c** 询问负责人员，检查系统和应用帐户及相关权限的定期审查的书面结果，以核实是否根据本要求中规定的所有元素执行了审核。	
适用性说明		
本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
7.2.6 限制所有持卡人数据查询存储库的用户访问权限，具体如下： • 通过应用程序或其他程序性方法，根据用户角色和最小权限进行访问和允许的操作。 • 只有负责管理员可以直接访问或查询 CHD 存储库。	**7.2.6.a** 检查政策和程序并询问相关人员，核实是否制定了相应流程，以根据本要求规定的所有元素授予持卡人数据查询存储库的用户访问权限。 **7.2.6.b** 检查持卡人数据查询存储库的配置设置，以核实它们是否符合本要求中规定的所有元素。	滥用持卡人数据存储库的查询访问权限一直是数据泄露的一个常见原因。限制管理员的这种访问，可以减少这种访问被未经授权的用户滥用的风险。 **定义** “程序性方法”是指通过数据库存储程序等方式授予访问权限，允许用户对表中的数据执行受控操作，而不是通过终端用户直接、未经过滤地访问数据存储库（负责管理员除外，他们需要直接访问数据库以履行其管理职责）。 **良好做法** 典型的用户操作包括移动、复制和删除数据。授予访问权限时还要考虑需要的权限范围。例如，可以授予访问权限给特定对象，例如数据元素、文件、表、索引、视图和存储程序。授予持卡人数据存储库的访问权限应遵循与授予所有其他访问权限相同的程序，也就是说，它是基于角色的，权限只分配给执行其工作职能所需的每个用户。
定制方法目标		
禁止对持卡人数据存储库进行未经过滤的直接查询访问，除非由授权管理员执行。		
适用性说明		
本要求适用于控制持卡人数据查询存储库的用户访问权限。 关于应用程序和系统帐户的控制，请参见要求 7.2.5 和 7.2.5.1 以及 8.6.1 至 8.6.3。		

要求和测试程序		指南
7.3 通过访问控制系统管理系统组件和数据的访问权限。		
规定的方法要求 **7.3.1** 建立访问控制系统，该系统根据用户的“必须知道”原则限制访问权限，并涵盖所有系统组件。 **定制方法目标** 通过专门为此目的建立的机制来管理访问权限和特权。	**规定的方法测试程序** **7.3.1** 检查供应商文件和系统设置，以核实每个系统组件的访问权限是否通过访问控制系统予以管理，该系统根据用户的“必须知道”原则限制访问权限，并涵盖所有系统组件。	**目的** 如果没有一个机制来限制基于用户需求的访问权限，用户可能会在不知情的情况下获得持卡人数据的访问权限。访问控制系统自动化限制访问和分配权限的流程。
规定的方法要求 **7.3.2** 访问控制系统被配置为执行基于工作分类和功能分配给个人、应用程序和系统的权限。 **定制方法目标** 系统、应用程序和数据的个人帐户访问权限和权限只继承自组成员资格。	**规定的方法测试程序** **7.3.2** 检查供应商文件和系统设置，以核实访问控制系统是否被配置为执行基于工作分类和功能分配给个人、应用程序和系统的权限。	**目的** 通过访问控制系统限制特权访问，减少在向个人、应用程序和系统分配权限时出现错误的机会。
规定的方法要求 **7.3.3** 访问控制系统默认设置为“拒绝所有”。 **定制方法目标** 除非明确许可，否则禁止访问权限和特权。	**规定的方法测试程序** **7.3.3** 检查供应商文件和系统设置，核实访问控制系统是否默认设置为“拒绝所有”。	**目的** 默认的“拒绝所有”设置确保没有人员获得访问权限，除非建立一个专门授予这种访问权限的规则。 **良好做法** 务必检查访问控制系统的默认配置，因为有些系统默认设置为“允许所有”，从而允许访问权限，除非/直到编写了专门拒绝访问权限的规则。

要求 8：　识别用户并验证系统组件的访问权限

章节	
8.1	确定和理解识别用户和验证系统组件的访问权限的流程和机制。
8.2	在帐户的整个生命周期中严格管理用户身份和相关用户和管理员帐户。
8.3	建立和管理用户和管理员的强效验证。
8.4	实施多因素验证（MFA），以确保 CDE 的安全访问权限。
8.5	配置多因素验证（MFA）系统以防止滥用。
8.6	严格管理应用程序和系统帐户和相关验证因素的使用。

概述

识别和验证用户的两个基本原则是：1）在计算机系统上建立个人或流程的身份；2）证明或核实与该身份相关的用户是否为该用户声称的人。

识别计算机系统上的个人或流程是通过一个标识符，例如用户、系统或应用 ID，将身份与个人或流程联系起来执行的。这些 ID（也被称为“帐户”）从根本上建立了个人或流程的身份，为每个人或流程分配了唯一标识，以将一个用户或流程与另一个用户或流程区分开来。一旦可以唯一识别每个用户或流程，它就能确保该身份必须对所执行的操作负责。当这种问责到位时，所执行的操作可以被追踪到已知和授权的用户和流程。

用来证明或核实身份的元素被称为验证因素。验证因素是：1）所知，如密码或口令；2）所有，如令牌设备或智能卡等；或 3）个人特征，如生物特征等

ID 和验证因素合称为验证凭证，用于获得与用户、应用程序、系统或服务帐户相关的权利和特权。

（下一页继续）

这些身份和验证的要求是基于行业公认的安全原则和最佳实践，以支持支付生态系统。*NIST 特别出版物 800-63《数字身份指南》*提供了关于数字身份和验证因素的可接受框架的额外信息。需要注意的是，*NIST《数字身份指南》*为美国联邦机构而设，应该完整地阅读它。 这些指南中规定的许多概念和方法预计将相互配合，而不是作为独立的参数。

注：*除非要求中另有说明，这些要求适用于****所有系统组件上的所有帐户****，除非在个别要求中特别指出，包括但不限于：*

- *销售点帐户*
- *具有管理能力的帐户*
- *系统和应用程序帐户*
- *用于查看或访问持卡人数据或访问在于持卡人数据的系统的所有帐户。*

这包括雇员、承包商、顾问、内部和外部供应商以及其他第三方（例如，用于提供支持或维护服务）使用的帐户。

某些要求不旨在适用于一次只能访问一个卡号的用户帐户，以促进单一交易（如销售点终端收银区使用的 ID）。当项目不适用时，会在具体要求中直接注明。

这些要求不适用于消费者（持卡人）使用的帐户。

请参阅附录 G 了解 PCI DSS 术语的定义。

要求和测试程序		指南
8.1 确定和理解识别用户和验证系统组件的访问权限的流程和机制。		
规定的方法要求 **8.1.1** 要求 8 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。 **定制方法目标** 受影响人员确定满足要求 8 的活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。	**规定的方法测试程序** **8.1.1** 检查文件并询问相关人员，以核实是否根据本要求中规定的所有元素管理了要求 8 中确定的安全政策和操作程序。	**目的** 要求 8.1.1 涉及有效管理和维护整个要求 8 规定的各种政策和程序。虽然定义要求 8 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。
8.1.2 记录、分配和理解执行要求 8 中活动的角色和责任。	**8.1.2.a** 检查文件，以核实是否记录和分配了执行要求 8 中活动的角色和责任的描述。	
	8.1.2.b 询问负责执行要求 8 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	
定制方法目标		
分配执行要求 8 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。		

要求和测试程序		指南
8.2 在帐户的整个生命周期中严格管理用户身份和相关用户和管理员帐户。		
规定的方法要求 **8.2.1** 在允许访问系统组件或持卡人数据之前，为所有用户分配唯一 ID。 **定制方法目标** 所有用户执行的所有操作都归属于个人。 **适用性说明** 本要求不旨在适用于销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。	**规定的方法测试程序** **8.2.1.a** 询问负责人员，核实是否为所有用户分配了唯一 ID，用于访问系统组件和持卡人数据。 **8.2.1.b** 检查检查日志和其他证据，核实是否可以唯一地识别系统组件和持卡人数据的访问权限，并与个人相关联。	**目的** 追踪在计算机系统上执行的操作到个人的能力建立了问责制和可追溯性，是建立有效访问控制的基础。 通过确保唯一识别每个用户，而不是用一个 ID 给几个员工使用，组织可以保持个人对操作的责任和每个员工在检查日志中的有效记录。此外，当发生误用或恶意行为时，这将有助于问题的解决和遏制。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
8.2.2 组、共享或通用帐户，或其他共享验证凭证仅在必要时例外使用，并按以下方式管理： • 除非在特殊情况下需要，否则将防止帐户使用。 • 使用仅限于特殊情况下所需的时间。 • 记录使用的商业理由。 • 使用由管理层明确批准。 • 在授予帐户访问权限之前，必须先确认个别用户身份。 • 采取的每项行动都可归于个别用户。	**8.2.2.a** 检查系统组件上的用户帐户列表和适用文件，以核实共享验证凭证是否仅在必要时例外使用，并按照本要求中规定的所有元素进行管理。 **8.2.2.b** 检查验证政策和程序，核实是否制定了共享验证凭证的相应流程，使其仅在必要时例外使用，并按照本要求规定的所有元素进行管理。 **8.2.2.c** 询问系统管理员，以核实共享验证凭证是否仅在必要时例外使用，并按照本要求中规定的所有元素进行管理。	组、共享或通用（或默认）帐户通常与软件或操作系统一起交付—例如，根用户或与特定职能相关的特权，如管理员。 如果多个用户共享相同的验证凭证（例如，用户帐户和密码），就不可能将系统访问和活动追踪到某个人。因此，某实体无法对个人的行为进行问责，或对个人的行为进行有效的记录，因为一个给定的操作可能是由群体中任何知道用户 ID 和相关验证因素的人执行。 将个人与帐户所执行的操作联系起来的能力，对于提供个人责任和追踪谁执行了某项操作、执行了什么操作以及该操作何时执行，至关重要。
定制方法目标		**良好做法**
使用通用、系统或共享 ID 的用户所执行的所有操作都归属于个人。		如果因任何原因使用共享帐户，需要建立强有力的管理控制，以保持个人的责任和可追溯性。
适用性说明		**示例**
本要求不旨在适用于销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。		工具和技术可以促进这些类型帐户的管理和安全保障，并在授予帐户访问权之前确认个人用户身份。各实体可以考虑密码管理器或其他系统管理的控制，例如 *sudo* 命令。 一个特殊情况的例子是，所有其他验证方法均已失效，需要一个共享帐户供紧急使用或“打破玻璃”管理员访问权限。

要求和测试程序		指南
规定的方法要求 **8.2.3** ***仅针对服务供应商的额外要求：***如果服务提供商拥有客户站点的远程访问权限，则将使用每个客户站点的唯一验证因素。 **定制方法目标** 用于一个客户的服务提供商凭证不能用于任何其他客户。 **适用性说明** 本要求仅在被评估实体是服务提供商的情况下适用。本要求不旨在适用于服务提供商访问他们自己的共享服务环境，在这个环境中，托管了多个客户环境。 如果服务提供商的员工使用共享验证因素来远程访问客户站点，这些因素对于每个客户必须是唯一的，并根据要求 8.2.2 进行管理。	**规定的方法测试程序** **8.2.3** ***仅针对服务提供商评估的额外测试程序：***检查验证政策和程序并询问相关人员，核实拥有客户站点远程访问权限的服务提供商是否使用每个客户站点远程访问的唯一验证因素。	**目的** 如果服务提供商拥有客户站点的远程访问权限，他们通常使用这种访问权限来支持 POS POI 系统或提供其他远程服务。 如果某服务提供商使用相同的验证因素来访问多个客户，那么如果攻击者威胁了这一个因素，就可以轻松威胁该服务提供商的所有客户。 犯罪分子知道这一点，故意以服务提供商为目标，寻找共享验证因素，让他们通过该单一因素远程访问许多商户。 **示例** 多因素机制等技术，为每个连接提供唯一凭证（如一次性密码），也可以满足这项要求的意图。

要求和测试程序		指南
规定的方法要求 **8.2.4** 管理用户 ID、验证因素和其他标识符对象的增加、删除和修改，具体如下： • 经适当的批准后授权。 • 仅以书面批准上指定的权限来实施。 **定制方法目标** 如果没有适当授权，则不会有用户 ID 和验证因素的生命周期事件。 **适用性说明** 本要求适用于所有用户帐户，包括雇员、承包商、顾问、临时工和第三方供应商。	**规定的方法测试程序** **8.2.4** 检查帐户生命周期各个阶段（添加、修改和删除）的授书面授权并检查系统设置，以核实该活动是否已根据本要求规定的所有元素予以管理。	**目的** 必须控制用户 ID 的生命周期（添加、删除和修改），以便只有授权帐户可以执行职能，操作是可检查的，并且权限只限于所需的任务。 攻击者通常会威胁现有帐户，然后升级该帐户的权限，以执行未经授权的操作，或者他们可能会创建新的 ID，在后台继续他们的活动。当用户帐户在非常规变更过程或未经相应授权的情况下被创建或变更时，检测和响应非常重要。
规定的方法要求 **8.2.5** 立即撤销离职用户的访问权限。 **定制方法目标** 不能使用离职用户的帐户。	**规定的方法测试程序** **8.2.5.a** 检查离职用户的信息来源，并审核当前的用户访问列表（包括本地和远程访问），以核实离职用户 ID 是否已被停用或从访问列表中删除。 **8.2.5.b** 询问负责人员，核实是否已为终止用户退回或停用所有物理验证因素，例如，智能卡、令牌等。	**目的** 如果员工或第三方/供应商已离开公司，但仍可通过其用户帐户获得网络的访问权限，则可能发生持卡人数据的不必要的或恶意访问—无论是由前雇员还是由利用旧的和/或未使用的帐户的恶意用户。

要求和测试程序		指南
规定的方法要求 **8.2.6** 非活跃用户帐户在不活跃的 90 天内被删除或禁用。 **定制方法目标** 不能使用非活跃用户帐户。	**规定的方法测试程序** **8.2.6** 检查用户帐户和最后一次登录信息，并询问相关人员，以核实任何非活跃用户帐户是否在不活跃的 90 天内被删除或禁用。	**目的** 不常使用的帐户往往是攻击的目标，因为任何变更，例如更改的密码，都不太可能被发现。因此，攻击者可能更容易利用这些帐户，并用于访问持卡人数据。 **良好做法** 如果可以合理地预期将在很长一段时间内不使用一个帐户，如长期休假，那么该帐户应在休假开始后立即禁用，而不是等待 90 天。
规定的方法要求 **8.2.7** 管理第三方使用的帐户，通过远程访问权限访问、支持或维护系统组件，具体如下： • 只在需要的时间段内启用，不使用时禁用。 • 监控使用情况，防止意外活动。 **定制方法目标** 除非明确授权，不能使用第三方远程访问权限，并由管理层监督使用情况。	**规定的方法测试程序** **8.2.7.** 询问相关人员，检查管理帐户的文件，并检查证据，以核实是否根据本要求中规定的所有元素管理了第三方用于远程访问的帐户。	**目的** 允许第三方全天候访问实体的系统和网络，以备他们需要提供支持，会增加未经授权的访问的机会。这种访问可能导致第三方环境中未经授权的用户或恶意者使用始终可用的外部入口点进入一个实体的网络。如果第三方确实需要全天候的访问权限，则应记录、证明、监控并与具体的服务原因相联系。 **良好做法** 只在需要的时间段内启用访问权限，一旦不再需要，就立即禁用，这有助于防止这些连接的滥用。此外，考虑根据第三方的服务合同，为他们指定一个访问的开始和停止日期。 监控第三方访问有助于确保第三方仅在批准的时间范围内访问必要的系统。应该跟踪和解决任何使用第三方帐户的异常活动。

要求和测试程序		指南
规定的方法要求 **8.2.8** 如果用户会话闲置超过 15 分钟，用户需要重新验证以重新激活终端或会话。 **定制方法目标** 只有授权用户可以使用用户会话。 **适用性说明** 本要求不旨在适用于销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。 这项要求并不是为了在控制台/计算机无人看管时免于合法活动发生。	**规定的方法测试程序** **8.2.8** 检查系统配置设置，核实用户会话的系统/会话闲置超时功能是否被设置为 15 分钟或更短时间。	**目的** 当用户离开一台可以访问系统组件或持卡人数据的开放机器时，存在这样的风险，即该机器可能在用户不在时被他人使用，导致未经授权的帐户访问和/或滥用。 **良好做法** 重新验证可以在系统层面上运用，以保护在该机器上运行的所有会话，或者在应用程序层面上运用。 各实体可能还想考虑连续进行分期控制，以便随着时间的推移进一步限制无人看管会话的访问。例如，屏幕保护程序可以在 15 分钟后激活，一小时后注销用户。 然而，超时控制必须对访问和暴露的风险与用户面临的影响和访问的目的进行平衡。 如果用户需要在无人看管的计算机上运行某程序，用户可以登录计算机启动该程序，然后“锁定”计算机，以便在计算机无人看管时，其他人不能使用该用户的登录信息。 **示例** 满足该要求的一个方法是配置一个自动屏幕保护程序，在控制台闲置 15 分钟后启动，并要求登录的用户输入密码以解锁屏幕。

要求和测试程序		指南
8.3 建立和管理用户和管理员的强效验证。		
规定的方法要求 **8.3.1** 通过以下至少一个验证因素对所有用户和管理员的系统组件访问权限进行验证： • 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。 **定制方法目标** 除非结合用户身份和验证因素，否则无法访问帐户。 **适用性说明** 本要求不旨在适用于销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。 这项要求并不取代多因素验证（MFA）要求，但适用于那些不受 MFA 要求约束的范围内系统。 如果数字证书对特定用户来说是唯一的，那么它就是“所有”的一个有效选择。	**规定的方法测试程序** **8.3.1.a** 检查描述验证因素的文件，核实是否通过本要求中规定的至少一个验证因素对所有用户和管理员的系统组件访问权限进行验证。 **8.3.1.b** 对于每一类系统组件所使用的每一类认证因素，观察验证情况，核实验证功能是否与书面验证因素一致。	**目的** 当与唯一 ID 一并使用时，验证因素有助于保护用户 ID 免于威胁，因为攻击者需要拥有唯一 ID 并威胁相关验证因素。 **良好做法** 恶意者威胁系统的一个常见方法是利用薄弱或并不存在的验证因素（例如，密码/口令）。要求强效验证因素有助于防止这种攻击。 **更多信息** 关于使用令牌、智能卡或生物识别技术作为验证因素的更多信息，请参见 *fidoalliance.org*。

要求和测试程序		指南
规定的方法要求 **8.3.2** 在传输和存储所有系统组件期间，使用强效加密法使所有验证因素不可读。	**规定的方法测试程序** **8.3.2.a** 检查供应商文件和系统配置设置，核实是否在传输和存储期间，使用强效加密法使所有验证因素不可读。 **8.3.2.b** 检查验证因素的存储库，核实它们在存储期间是否不可读。 **8.3.2.c** 检查数据传输，核实验证因素在传输期间是否不可读。	**目的** 长期以来，网络设备和应用程序在网络上传输未加密的、可读的验证因素（如密码和口令）和/或在不加密的情况下存储这些值。因此，恶意者可以在传输过程中使用“嗅探器”轻易地拦截这些信息，或者直接访问存储这些信息所在文件的未加密验证因素，然后使用这些数据来获得未经授权的访问。
定制方法目标 不能从截获的通信或存储的数据中获得、导出或重复使用明文验证因素。		
规定的方法要求 **8.3.3** 在修改任何验证因素之前先对用户身份进行核实。	**规定的方法测试程序** **8.3.3** 检查修改验证因素的相应程序并观察安全人员，核实当用户要求修改验证因素时，是否在修改验证因素之前先对用户身份进行核实。	**目的** 恶意者使用“社会工程”技术来冒充系统的用户—例如，致电给服务台并充当合法用户—来改变验证因素，以便他们可以使用有效的用户 ID。 要求正确识别用户的身份，可以减少此类攻击成功的概率。 **良好做法** 修改需要核实用户身份的验证因素包括但不限于执行密码重设、提供新的硬件或软件令牌以及生成新的密钥。 **示例** 核实用户身份的方法包括安全问题/答案、基于知识的信息，以及使用已知的和先前建立的电话号码回拨用户。
定制方法目标 未经授权的个人不能通过冒充授权用户的身份获得系统访问权限。		

要求和测试程序		指南
规定的方法要求 **8.3.4** 限制无效的验证尝试，具体如下： • 在不超过 10 次尝试后锁定用户 ID。 • 将锁定时间设置为至少 30 分钟或直到用户身份得到确认。 **定制方法目标** 在线蛮力攻击无法猜出验证因素。 **适用性说明** 本要求不旨在适用于销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。	**规定的方法测试程序** **8.3.4.a** 检查系统配置设置，核实验证参数是否设置为规定在不超过 10 次无效登录尝试后锁定用户帐户。 **8.3.4.b** 检查系统配置设置，以核实密码参数是否被设置为要求一旦用户帐户被锁定，它至少保持锁定状态 30 分钟或直到用户身份得到确认。	**目的** 如果没有帐户锁定机制，攻击者可以通过手动或自动工具（例如，密码破解）不断尝试猜测密码，直到攻击者成功并获得用户帐户的访问权限。 如果帐户由于攻击者不断尝试猜测密码而被锁定，那么延迟重新激活已锁帐户的控制措施可以阻止恶意者猜测密码，因为他们必须停止至少 30 分钟，直到帐户被重新激活。 **良好做法** 在重新激活已锁帐户之前，应该确认用户的身份。例如，管理员或服务台人员可以验证实际帐户所有者是否要求重新激活，或者可能有帐户所有者用来核实其身份的密码重置自助服务机制。
规定的方法要求 **8.3.5** 如果密码/口令被用作满足要求 8.3.1 的验证因素，则为每个用户进行设置和重置，具体如下： • 首次使用和重置时设为唯一值。 • 强制在首次使用后立即更改。 **定制方法目标** 未经授权的用户不能使用分配给用户的初始或重置密码/口令。	**规定的方法测试程序** **8.3.5** 检查设置和重置密码/口令的程序（如果用作满足要求 8.3.1 的验证因素）并观察安全人员，核实是否根据本要求中规定的所有元素设置和重置了密码/口令。	**目的** 如果每个新用户都使用相同的密码/口令，那么内部用户、前雇员或恶意者可能知道或轻松发现该值，并在授权用户尝试使用该密码之前利用该值获得帐户的访问权限。

要求和测试程序		指南
规定的方法要求 **8.3.6** 如果密码/口令被用作满足要求 8.3.1 的验证因素，它们应满足以下最低复杂程度： • 最小长度为 12 个字符（或者如果系统不支持 12 个字符，则最小长度为 8 个字符）。 • 同时包含数字和字母字符。 **定制方法目标** 无论是在线还是离线蛮力攻击，都无法核实猜中的密码/口令。 **适用性说明** 这项要求不旨在适用于： • 销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。 • 应用程序或系统帐户，由第 8.6 节中的要求所规定。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。* 2025 年 3 月 31 日前，根据 PCI DSS v3.2.1 要求 8.2.3，密码长度必须至少为七个字符。	**规定的方法测试程序** **8.3.6** 检查系统配置设置，核实是否根据本要求中规定的所有元素设置了用户密码/口令复杂性参数。	**目的** 强效密码/口令可能是进入网络的第一道防线，因为恶意者通常会首先尝试使用薄弱、静态或并不存在的密码寻找帐户。如果密码很短或易于猜测，恶意者轻松便可找到这些薄弱的帐户，并以有效的用户 ID 为幌子威胁网络。 **良好做法** 密码/口令强度取决于密码/口令的复杂性、长度和随机性。密码/口令应该足够复杂，这样攻击者就不可能猜到或发现其数值。除了本要求所列出的最低标准外，各实体可以考虑通过要求使用特殊字符和大小写字符来增加复杂性。额外复杂性会增加离线蛮力攻击散列密码/口令所需的时间。 另一个提高密码抗猜测攻击能力的方法是将建议的密码/口令与不良密码列表进行比较，并让用户为列表中的任何密码提供新密码。

要求和测试程序		指南
规定的方法要求 **8.3.7** 个人不得提交与最后使用的四个密码/口令中的任何一个相同的新密码/口令。 **定制方法目标** 在至少 12 个月内，以前使用的密码不能被用来访问帐户。 **适用性说明** 本要求不旨在适用于销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。	**规定的方法测试程序** **8.3.7** 检查系统配置设置，核实密码参数是否被设置为要求新的密码/口令不能与之前使用的四个密码/口令相同。	**目的** 如果不保留密码历史记录，更改密码的有效性就会降低，因为可以反复使用以前的密码。要求在一段时间内不能重复使用密码，可以减少被猜中或被蛮力破解的密码在未来被重复使用的可能性。 密码或口令以前可能因为怀疑遭到威胁或因为密码或口令超出有效使用期而被更改，无论哪种情况，都解释了为什么不应该重复使用以前使用的密码。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
8.3.8 记录验证政策和程序，并传达给所有用户，包括： • 关于选择强效验证因素的指南。 • 关于用户应如何保护他们的验证因素的指南。 • 不要重复使用以前使用过的密码/口令的指示。 • 如果怀疑或知道密码/口令已被威胁，应指示更改密码/口令，以及如何报告该事件。	**8.3.8.a** 检查程序并询问相关人员，以核实认证政策和程序是否已分发给所有用户。 **8.3.8.b** 审核分发给用户的验证政策和程序，并核实其是否包括本要求中规定的元素。 **8.3.8.c** 询问用户，核实他们是否熟悉验证政策和程序。	将验证政策和程序传达给所有用户，有助于他们理解并遵守这些政策。 **良好做法** 关于选择强密码的指导可能包括建议帮助人员选择难以猜测的密码，这些密码不包含字典内的单词或关于用户的信息，例如用户 ID、家庭成员的名字、出生日期等。 保护验证因素的指导可能包括不写下密码或不将其保存在非安全文件中，并对可能试图利用其密码的恶意者保持警惕（例如，致电给员工并要求其提供密码，以便来电者能够“解决一个问题”）。 另外，实体可以实施一些程序来确认密码是否符合密码政策，例如，将密码选择与不可接受的密码列表进行比较，并让用户为任何与列表中的密码相匹配的密码选择新的密码。如果密码有可能不再安全，指示用户更改密码，可以防止恶意用户使用正规密码来获得未经授权的访问。
定制方法目标		
用户对正确使用验证因素有所了解，并在需要时能获得帮助和指导。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
8.3.9 如果密码/口令被用作用户访问的唯一验证因素（即，在任何单因素验证实施中），那么： • 密码/口令至少每 90 天更换一次。 **或** • 动态分析帐户的安全状况，并相应地自动确定资源的实时访问情况。	**8.3.9** 如果密码/口令被用作用户访问的唯一验证因素，检查系统配置设置，以核实是否根据本要求中规定的一个元素管理了密码/口令。	可以使用单一验证因素，例如密码/口令、令牌设备或智能卡，或生物识别属性，提供非 CDE 的范围内系统组件的访问权限。当密码/口令用于这种访问的唯一验证因素时，需要额外控制来保护密码/口令的完整性。 **良好做法** 密码/口令如果长期有效而不作更改，恶意者就有更多的时间来破解密码/口令。定期更改密码，恶意者就没有更多的时间来破解密码/口令，以及更少的时间来使用被威胁密码。 使用密码/口令作为唯一验证因素，一旦被威胁，就会产生单点故障。因此，在这些实施中，需要进行控制，以尽量减少通过被威胁密码/口令进行恶意活动的时间。 动态分析帐户安全状况是另一种选择，可以更快速地检测和响应，以解决潜在的被威胁凭证。这种分析需要一些数据点，其中可能包括设备的完整性、位置、访问时间和访问的资源，以实时确定是否可以向帐户授予所请求资源的访问权限。因此，如果怀疑验证凭证遭到泄露，就可阻止访问并封锁帐户。 **更多信息** 有关使用动态分析管理资源的用户访问的信息，请参阅 NIST SP 800-207 零信任安全架构。
定制方法目标		
不能无限期地使用一个未被检测到的被威胁密码/口令。		
适用性说明		
本要求适用于非 CDE 中的范围内系统组件，因为这些组件不受 MFA 要求的约束。 本要求不旨在适用于销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。 这一要求不适用于服务提供商的客户帐户，但适用于服务提供商人员的帐户。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
8.3.10 ***仅针对服务供应商的额外要求：***如果密码/口令被用作客户用户访问持卡人数据的唯一验证因素（即，在任何单因素验证实施中），那么向客户用户提供指导，包括： • 关于客户定期更改其用户密码/口令的指导。 • 关于何时以及在何种情况下更改密码/口令的指导。	**8.3.10** ***仅针对服务提供商评估的额外测试程序：***如果密码/口令被用作客户用户访问持卡人数据的唯一验证因素，检查提供给客户用户的指导，以核实该指导是否包括本要求中规定的所有元素。	使用密码/口令作为唯一验证因素，一旦被威胁，就会产生单点故障。因此，在这些实施中，需要进行控制，以尽量减少通过被威胁密码/口令进行恶意活动的时间。 **良好做法** 密码/口令如果长期有效而不作更改，恶意者就有更多的时间来破解密码/口令。定期更改密码，恶意者就没有更多的时间来破解密码/口令，以及更少的时间来使用被威胁密码。
定制方法目标		
不能无限期地使用服务提供商客户的密码/口令。		
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。本要求不适用于消费者用户访问其自身支付卡信息的帐户。 一旦 8.3.10.1 生效，这项针对服务提供商的要求将被 8.3.10.1 要求所取代。		

要求和测试程序		指南
规定的方法要求 **8.3.10.1** ***仅针对服务供应商的额外要求：***如果密码/口令被用作客户用户访问的唯一验证因素（即，在任何单因素验证实施中），那么： • 密码/口令至少每 90 天更换一次。 **或** • 动态分析帐户的安全状况，并相应地自动确定资源的实时访问情况。 **定制方法目标** 不能无限期地使用服务提供商客户的密码/口令。 **适用性说明** 本要求仅在被评估实体是服务提供商的情况下适用。本要求不适用于消费者用户访问其自身支付卡信息的帐户。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。* 在该要求于 2025 年 3 月 31 日生效之前，服务提供商可以满足要求 8.3.10 或 8.3.10.1。	**规定的方法测试程序** **8.3.10.1** ***仅针对服务提供商评估的额外测试程序：***如果密码/口令被用作客户用户访问的唯一验证因素，检查系统配置设置，以核实是否根据本要求中规定的一个元素管理了密码/口令。	**目的** 使用密码/口令作为唯一验证因素，一旦被威胁，就会产生单点故障。因此，在这些实施中，需要进行控制，以尽量减少通过被威胁密码/口令进行恶意活动的时间。 **良好做法** 密码/口令如果长期有效而不作更改，恶意者就有更多的时间来破解密码/口令。定期更改密码，恶意者就没有更多的时间来破解密码/口令，以及更少的时间来使用被威胁密码。 动态分析帐户安全状况是另一种选择，可以更快速地检测和响应，以解决潜在的被威胁凭证。这种分析需要一些数据点，其中可能包括设备的完整性、位置、访问时间和访问的资源，以实时确定是否可以向帐户授予所请求资源的访问权限。因此，如果怀疑帐户凭证遭到泄露，就可阻止访问并封锁帐户。 **更多信息** 有关使用动态分析管理资源的用户访问的信息，请参阅 *NIST SP 800-207 零信任安全架构*。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果多个用户可以使用诸如令牌、智能卡和证书等验证因素，则可能无法识别使用该验证机制的个人。 **良好做法** 拥有物理和/或逻辑控制（例如，PIN 码、生物识别数据或密码）来唯一地验证帐户的用户，将防止未经授权的用户通过使用共享验证因素来获得用户帐户的访问权限。
8.3.11 使用了如物理或逻辑安全令牌、智能卡或证书等验证因素： • 因素被分配给个别用户，而不是在多个用户之间共享。 • 物理和/或逻辑控制确保只有预期用户可以使用该因素来获得访问权限。	**8.3.11.a** 检查验证政策和程序，核实是否制定了使用诸如物理安全令牌、智能卡和证书等验证因素的程序，并包括本要求中规定的所有元素。	
	8.3.11.b 询问安全人员，以核实验证因素是否分配给个别用户，而不是在多个用户之间共享。	
定制方法目标 验证因素不能被任何非指定用户使用。	**8.3.11.c** 检查系统配置设置和/或观察物理控制（如适用），以核实是否实施了控制，以确保只有预期用户可以使用该因素来获得访问权限。	

要求和测试程序		指南
8.4 实施多因素验证（MFA），以确保 CDE 的安全访问权限。		
规定的方法要求 **8.4.1** 对于具有管理权限的人员，为 CDE 的所有非控制台访问权限实施了 MFA。 **定制方法目标** 不能通过使用单一的验证因素来获得 CDE 的管理访问权限。 **适用性说明** 对非控制台管理访问的 MFA 要求适用于所有通过非控制台连接（即通过网络接口发生的逻辑访问，而不是通过直接的物理连接）访问 CDE 的具有较高和较多权限的人员。 MFA 被视为是用于非 CDE 的范围内系统组件的非终端管理访问权限的最佳实践。	**规定的方法测试程序** **8.4.1.a** 检查网络和/或系统配置，以核实对于具有管理权限的人员，是否为 CDE 的所有非控制台访问权限实施了 MFA。 **8.4.1.b** 观察登录 CDE 的管理人员，并核实是否需要 MFA。	**目的** 要求一个以上的验证因素，可以减少攻击者通过伪装成合法用户获得系统访问权限的概率，因为攻击者需要对多个验证因素进行威胁。对于一直以来采用单一验证因素的环境中尤其如此，因为在这些环境中，验证因素为用户所知，例如密码或口令。 **定义** 一个因素使用两次（例如，使用两个单独的密码）不被视为多因素验证。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
8.4.2 为所有 CDE 的访问权限实施 MFA。	**8.4.2.a** 检查网络和/或系统配置，以核实是否为所有 CDE 的访问权限实施了 MFA。	要求一个以上的验证因素，可以减少攻击者通过伪装成合法用户获得系统访问权限的概率，因为攻击者需要对多个验证因素进行威胁。对于一直以来采用单一验证因素的环境中尤其如此，因为在这些环境中，验证因素为用户所知，例如密码或口令。
	8.4.2.b 观察登录 CDE 的相关人员并检查证据，以核实是否需要 MFA。	**定义**
定制方法目标		一个因素使用两次（例如，使用两个单独的密码）不被视为多因素验证。
不能通过使用单一的验证因素来获得 CDE 的访问权限。		
适用性说明		
本要求不适用于： • 执行自动化功能的应用程序或系统帐户。 • 销售点终端上的用户帐户，这些帐户一次只能访问一个卡号以促进单一交易（如销售点终端收银区使用的 ID）。 要求 8.4.2 和 8.4.3 中规定的两种访问类型都需要 MFA。因此，对一种访问类型应用 MFA 并不能取代对另一种访问类型应用另一个 MFA 实例的需要。如果某人首先通过远程访问连接到实体的网络，随后从网络内启动连接到 CDE，根据这一要求，该人将使用 MFA 进行两次验证，一次是通过远程访问连接到实体的网络，另一次是从实体的网络通过非控制台管理访问权限连接到 CDE。		

（下一页继续）

要求和测试程序		指南
MFA 要求适用于所有类型的系统组件，包括云、托管系统和内部应用程序、网络安全设备、工作站、服务器和端点，并包括直接访问实体的网络或系统，以及基于网络访问应用程序或功能。 对于 CDE 的远程访问权限，可以在网络或系统/应用程序层面实施 MFA，未必一定要在两个层面都应用 MFA。例如，如果在用户连接到 CDE 网络时使用了 MFA，那么在用户登录 CDE 内的每个系统或应用时就不一定要使用 MFA。 ***本要求在 2025 年 3 月 31 日之前是最佳****实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
8.4.3 为来自非实体网络、可能访问或影响 CDE 的所有远程网络访问权限实施 MFA，具体如下： • 所有人员（包括用户和管理员）的所有远程访问权限都来自于非实体网络。 • 第三方和供应商的所有远程访问。	**8.4.3.a** 检查远程访问服务器和系统的网络和/或系统配置，以核实 MFA 的需要是否符合本要求中规定的所有元素。	要求一个以上的验证因素，可以减少攻击者通过伪装成合法用户获得系统访问权限的概率，因为攻击者需要对多个验证因素进行威胁。对于一直以来采用单一验证因素的环境中尤其如此，因为在这些环境中，验证因素为用户所知，例如密码或口令。
定制方法目标	**8.4.3.b** 观察远程连接到网络的人员（如用户和管理员），以核实是否需要多因素验证。	**定义**
不能通过使用单一验证因素获得实体网络的远程访问权限。		多因素验证 (MFA)要求个人在获得访问权限之前，至少出示要求 8.3.1 中规定的三个验证因素中的其中两个。一个因素使用两次（例如，使用两个单独的密码）不被视为多因素验证。
适用性说明		
来自非实体网络的远程访问的 MFA 要求适用于所有可以远程访问网络的用户帐户，其中远程访问权限导致或可能导致对 CDE 的访问。 如果远程访问实体网络的一部分，并与 CDE 适当隔离，使远程用户不能访问或影响 CDE，则无需为该部分网络的远程访问权限实施 MFA。然而，对于任何可以访问 CDE 的网络远程访问权限，需要实施 MFA，并且建议为实体网络的所有远程访问权限实施 MFA。 MFA 要求适用于所有类型的系统组件，包括云、托管系统和内部应用程序、网络安全设备、工作站、服务器和端点，并包括直接访问实体的网络或系统，以及基于网络访问应用程序或功能。		

要求和测试程序		指南
8.5 配置多因素验证(MFA)系统以防止滥用。		
规定的方法要求 **8.5.1** 实施 MFA 系统，具体如下： • MFA 系统不易受到回放攻击的影响。 • MFA 系统不能被任何用户绕过，包括管理用户，除非有明确记录，并在有限的时间内由管理层在例外情况下授权。 • 至少使用两种不同类型的验证因素。 • 在授予访问权限之前，所有验证因素都必须成功。	**规定的方法测试程序** **8.5.1.a** 检查供应商的系统文件，核实 MFA 系统是否不易受到回放攻击的影响。 **8.5.1.b** 检查 MFA 实施的系统配置，以核实是否根据本要求中规定的所有元素配置了该配置。 **8.5.1.c** 询问负责人员并观察程序，以核实任何绕过 MFA 的请求是否有明确记录，并在有限的时间内由管理层在例外情况下授权。 **8.5.1.d** 观察登录 CDE 中系统组件的人员，以核实是否只有在所有验证因素都成功后才会授予访问权限。 **8.5.1.e** 观察从非实体网络远程连接的人员，以核实是否只有在所有验证因素都成功后才会授予访问权限。	**目的** 攻击者可以绕过配置不良的 MFA 系统。因此，本要求解决了 MFA 系统的配置问题，该系统为访问 CDE 中系统组件的用户提供了 MFA。 **定义** 一种类型的因素使用两次（例如，使用两个单独的密码）不被视为多因素验证。 **更多信息** 关于 MFA 系统和功能的更多信息，请参考以下指南： PCI SSC 的*信息补充：多因素验证* PCI SSC 关于此主题的常见问题解答（FAQ）
定制方法目标 MFA 系统能够抵御攻击，并严格控制任何管理人员的越权行为。		
适用性说明 ***本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。***		

要求和测试程序		指南
8.6 严格管理应用程序和系统帐户和相关验证因素的使用。		
规定的方法要求 **8.6.1** 如果系统或应用程序使用的帐户可用于交互式登录，则对其进行管理，具体如下： • 除非在特殊情况下需要，否则将阻止交互式使用。 • 交互式使用仅限于特殊情况下所需的时间。 • 记录交互式使用的商业理由。 • 交互式使用由管理层明确批准。 • 在授予帐户访问权限之前，必须先确认个别用户身份。 • 采取的每项行动都可归于个别用户。 **定制方法目标** 当交互式使用时，将帐户指定为系统或应用程序帐户的所有操作均已授权并归属于个人。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **8.6.1** 检查可以交互使用的应用程序和系统帐户，并询问管理人员，以核实是否根据本要求中规定的所有元素管理了应用程序和系统帐户。	**目的** 同于个人用户帐户，系统和应用程序帐户需要问责制和严格管理，以确保它们只用于预期目的，不被滥用。 攻击者经常威胁系统或应用程序帐户，以获得持卡人数据的访问权限。 **良好做法** 在可能情况下，配置系统和应用程序帐户为不允许交互式登录，以防止未经授权的个人登录并使用该帐户及其相关的系统权限，并限制该帐户可使用的机器和设备。 **定义** 系统或应用程序帐户是那些在计算机系统或应用程序上执行流程或执行任务的帐户，通常不是个人登录的帐户。这些帐户通常具有执行专门任务或功能所需的更高权限。 交互式登录是指某人以与普通用户帐户相同的方式登录系统或应用程序帐户的能力。以这种方式使用系统和应用程序帐户，意味着用户无需对采取的行动负责，记录无法追溯。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
8.6.2 任何可用于交互式登录的应用程序和系统帐户的密码/口令不在脚本、配置/属性文件或制订和定制源代码中硬编码。	**8.6.2.a** 询问相关人员并检查系统开发程序，以核实是否为可用于交互式登录的应用程序和系统帐户制定了相应流程，规定密码/口令不在脚本、配置/属性文件或制订和定制源代码中硬编码。	不适当地保护应用程序和系统帐户使用的密码/口令，特别是当这些帐户可用于交互式登录时，会增加未经授权使用这些特权帐户的风险和成功率。
	8.6.2.b 检查可用于交互式登录的应用程序和系统帐户的脚本、配置/属性文件以及制订和定制源代码，以核实这些帐户的密码/口令是否存在。	**良好做法**
定制方法目标		由于怀疑或确认泄露而改变这些值，可能特别难以实施。
未经授权的人员不能使用应用程序和系统帐户所使用的密码/口令。		工具可以促进应用程序和系统帐户的验证因素的管理和安全保障。例如，考虑密码管理器或其他系统管理的控制。
适用性说明		
根据 PCI DSS 要求 8.3.2，要求对存储的密码/口令进行加密。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
8.6.3 保护任何应用程序和系统帐户的密码/口令免受滥用，具体如下： • 定期更改密码/口令（按照实体的目标风险分析中确定的频率，即根据要求 12.3.1 中规定的所有元素执行），并在怀疑或确认受到威胁时更改。 • 构建具有足够复杂性的密码/口令，以适合于该实体更改密码/口令的频率。	**8.6.3.a** 检查政策和程序，核实是否制定了相应程序，以根据本要求中规定的所有元素保护应用程序或系统帐户的密码/口令免于滥用。 **8.6.3.b** 检查实体的目标风险分析，了解用于交互式登录应用程序和系统帐户的密码/口令的更改频率和复杂性，以核实是否根据要求 12.3.1 中规定的所有元素执行了风险分析并确定了： • 定期更改应用程序和系统密码/口令的频率。 • 密码/口令的复杂性，以及相对于更改频率而言，复杂性是否适当。	相比于用户帐户，系统和应用程序帐户具有更多的内在安全风险，因为它们通常在高安全环境下运行，可以访问通常不会授予用户帐户（访问权限）的系统，例如数据库的编程访问权限等。因此，必须特别考虑保护用于应用程序和系统帐户的密码/口令。 **良好做法** 各实体在确定如何保护应用程序和系统密码/口令免遭滥用时，应考虑以下风险因素： • 密码/口令存储的安全性如何（例如，它们是否被存储在密码管理器中）。 • 工作人员流动。 • 拥有验证因素访问权限的人数。 • 帐户是否可用于交互式登录。 • 是否动态分析了帐户的安全状况，并相应地自动确定资源的实时访问情况（请参见要求 8.3.9）。 所有这些元素都会影响应用程序和系统帐户的风险水平，并可能影响到系统和应用程序帐户所访问的系统的安全性。 *（下一页继续）*
定制方法目标	**8.6.3.c** 询问负责人员并检查系统配置设置，以核实是否根据本要求中规定的所有元素保护了任何可用于交互式登录的应用程序和系统帐户的密码/口令免于滥用。	
不能无限期使用应用程序和系统帐户使用的密码/口令，并且其结构能够抵御蛮力攻击和猜测攻击。		
适用性说明		
本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。		

要求和测试程序		指南
		各实体应将其选择的应用程序和系统密码/口令的更改频率与他们选择的这些密码/口令的复杂性联系起来–即，当密码/口令不经常更换时，复杂性应更加严格，而当更改频率较高时，可以不那么严格。例如，当密码/口令的复杂性被设为由大小写字母、数字和特殊字符组成的 36 个字母数字字符时，较长的更换频率是合理的。 最佳做法是考虑每年至少更换一次密码，密码/口令的长度至少为 15 个字符，密码/口令的复杂性被设为由大小写字母、数字和特殊字符组成的母数字字符。 **更多信息** 关于不同格式的密码/口令强度的可变性和等价性，请参见行业标准（例如，当前版本的 *NIST SP 800-63 数字身份指南*）。

要求 9:　　限制持卡人数据的实体访问权限

章节
9.1 确定并理解限制持卡人数据的实体访问权限的流程和机制。
9.2 实体访问控制管理进入含有持卡人数据的设施和系统。
9.3 授权和管理人员和访客的实体访问权限。
9.4 安全存储、访问、分发和销毁含有持卡人数据的媒体。
9.5 保护交互点（POI）设备免于篡改和未经授权的替代。

概述

任何存储、处理或传输持卡人数据的持卡人数据或系统的实体访问权限，都为个人访问和/或删除包含持卡人数据的系统或硬拷贝提供了机会；因此，实体访问权限应受到适当的限制。

要求 9 中提到了三个不同的区域。

1. 特别提到敏感区域的要求旨在仅适用于这些区域。
2. 特别提到持卡人数据环境（CDE）的要求旨在适用于整个 CDE，包括 CDE 所在的任何敏感区域。
3. 特别提到设施的要求是指在 CDE 和敏感区域所在的商业场所（例如建筑物）的物理边界上可以更广泛地管理的控制类型。这些控制通常存在于 CDE 或敏感区域之外，例如，识别、标记和记录访客的警卫台。使用“设施”一词是为了确认这些控制可能存在于设施内的不同位置，例如，在建筑物入口处或在数据中心或办公空间的内部入口处。

关于“媒体”、“人员”、“敏感区域”和其他 PCI DSS 术语的定义，请参考附录 G。

要求和测试程序		指南
9.1 确定并理解限制持卡人数据的实体访问权限的流程和机制。		
规定的方法要求 **9.1.1** 要求 9 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。 **定制方法目标** 受影响人员确定满足要求 9 的活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。	**规定的方法测试程序** **9.1.1** 检查文件并询问相关人员，以核实是否根据本要求中规定的所有元素管理了要求 9 中确定的安全政策和操作程序。	**目的** 要求 9.1.1 涉及有效管理和维护整个要求 9 规定的各种政策和程序。虽然定义要求 9 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。 政策和程序，包括更新，都积极传达给所有受影响的人员，并得到操作程序的支持，该程序描述了执行活动的方法。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。
9.1.2 记录、分配和理解执行要求 9 中活动的角色和责任。	**9.1.2.a** 检查文件，以核实是否记录和分配了执行要求 9 中活动的角色和责任的描述。	
	9.1.2.b 询问负责执行要求 9 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	
定制方法目标		
分配执行要求 9 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。		

要求和测试程序		指南
9.2 实体访问控制物理访问控制对进入包含持卡人数据的设施和系统进行管理。		
规定的方法要求 **9.2.1** 制定了适当的设施进入控制，以限制 CDE 系统的物理访问权限。 **定制方法目标** 未经授权的人员不能物理访问 CDE 的系统组件。	**规定的方法测试程序** **9.2.1** 观察进入控制并询问负责人员，核实是否制定了物理安全控制，以限制 CDE 系统的访问权限。	**目的** 如果没有物理访问控制，未经授权的人员有可能获得 CDE 和敏感信息的访问权限，或者可能改变系统配置，将漏洞引入到网络中，或者破坏或盗窃设备。因此，这项要求的目的是通过物理安全控制，例如标记阅读器或其他机制（例如锁和钥匙），来控制 CDE 的物理访问权限。 **良好做法** 无论哪种机制满足这一要求，它必须足以让组织核实是否只有经授权的人员被授予访问权限。 **示例** 设施进入控制包括在 CDE 的每个计算机房、数据中心和其他具有系统的物理区域的物理安全控制。它还可以包括标记阅读器或其他管理物理访问控制的设备，例如锁和钥匙以及所有持有钥匙的个人的最新名单。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 维护进入和离开敏感区域的个人的详细信息，可以帮助调查物理违规行为，方法是识别物理访问敏感区域的个人，以及他们进入和离开的时间。 **良好做法** 无论哪种机制符合这一要求，都应有效监控敏感区域的所有入口和出口点。 试图获得敏感区域的访问权限的犯罪分子往往会试图禁用或绕过监控控制。为了保护这些控制不被篡改，可以将录像机安置在不被人发现的地方，并/或对其进行监控以发现篡改行为。同样，可以监控物理访问控制机制或安装物理保护装置，以防止恶意者对它们进行破坏或禁用。
9.2.1.1 使用摄像机或物理访问控制机制（或两者）监控 CDE 内敏感区域的个人物理访问权限，具体如下： • 监控 CDE 内敏感区域的入口和出口点。 • 保护监控设备或机制免于篡改或禁用。 • 审核收集到的数据，并与其他条目相关联。 • 收集的数据至少保存三个月，除非法律另有限制。	**9.2.1.1.a** 观察 CDE 内敏感区域的各个物理接入点，以核实是否制定了视频摄像头或物理访问控制机制（或两者）来监控入口和出口点。	
	9.2.1.1.b 观察 CDE 内敏感区域的各个物理接入点，以核实录像机或物理访问控制机制（或两者）是否受到保护免于篡改或禁用。	
定制方法目标 对于个人进入和离开敏感区域的实际情况，保留可信的、可核实的记录。	**9.2.1.1.c** 观察物理访问控制机制和/或检查录像机并询问负责人员，以核实： • 是否审核了从录像机和/或物理访问控制机制收集的数据，并与其他条目相关联。 • 收集的数据是否至少保存三个月。	

要求和测试程序		指南
规定的方法要求 **9.2.2** 实施物理和/或逻辑控制，以限制使用设施内可公开使用的网络插座。 **定制方法目标** 未经授权的设备不能从设施内的公共区域连接到该实体的网络。	**规定的方法测试程序** **9.2.2** 询问负责人员并观察可公开使用的网络插座的位置，核实是否制定了物理和/或逻辑控制，以限制设施内公共网络插座的访问权限。	**目的** 限制网络插座（或网络端口）的访问权限将防止恶意者插入现成的网络插座并获得 CDE 或连接到 CDE 的系统的访问权限。 **良好做法** 无论使用逻辑控制还是物理控制，或者两者结合使用，都应该防止未经明确授权的个人或设备能够连接到网络。 **示例** 满足这一要求的方法包括：可以禁用位于公共区域和访客可以进入的区域的网络插座，只有在网络访问被明确授权时才可以启用。另外，还可以实施相应流程，以确保访客在有网络插座的区域一直有专人陪同。
规定的方法要求 **9.2.3** 限制设施内的无线接入点、网关、网络/通信硬件和电信线路的物理访问权限。 **定制方法目标** 未经授权的人员不能访问物理网络设备。	**规定的方法测试程序** **9.2.3** 询问负责人员并观察硬件和线路的位置，以核实是否限制了设施内的无线接入点、网关、网络/通信硬件和电信线路的物理访问权限。	**目的** 如果没有对无线组件和设备以及计算机网络和电信设备和线路的访问进行适当的物理安全保护，恶意用户可以获得该实体的网络资源的访问权限。此外，他们可以将自己的设备连接到网络上，以获得 CDE 或连接到 CDE 的系统的未经授权访问权限。 此外，确保网络和通信硬件安全，可以防止恶意用户拦截网络流量或将他们自己的设备实际连接到有线网络资源。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
9.2.4 不使用时，通过锁定来限制敏感区域的控制台的访问权限。	**9.2.4** 观察系统管理员试图登录敏感区域的控制台，并核实它们是否被“锁定”以防止未经授权的使用。	锁定控制台的登录屏幕，防止未经授权的人员获得敏感信息的访问权限，改变系统配置，将漏洞引入网络，或破坏记录。
定制方法目标		
未经授权的人员不能使用敏感区域内的物理控制台。		

要求和测试程序		指南
9.3 授权和管理人员和访客的实体访问权限。		
规定的方法要求	**规定的方法测试程序**	**目的** 建立授予、管理和在不再需要时取消访问的程序，以确保防止非授权人员获得载有持卡人数据的区域的访问权限。此外，必须限制实际标记系统和标记材料的访问权限，以防止未经授权的人员制作自己的标记和/或设置自己的访问规则。 **良好做法** 从视觉上识别实际存在的人员，以及该人员是访客还是雇员，这一点非常重要。 **示例** 识别人员的一种方法是为他们分配标记。
9.3.1 实施相应程序，以授权和管理相关人员获得 CDE 的物理访问权限，包括： • 识别人员的身份。 • 管理个人实体访问要求的变更。 • 撤销或终止人员身份。 • 将对识别过程或系统的访问限制在授权人员范围内。	**9.3.1.a** 检查书面程序，以核实是否按照本要求中规定的所有元素制定了授权和管理人员访问 CDE 的程序。	
	9.3.1.b 观察身份识别方法（如身份标记和其过程，以核实是否明确识别了 CDE 中的人员。	
定制方法目标	**9.3.1.c** 观察流程以核实身份识别过程的访问权限（如标记系统）是否只限于经授权的人员。	
确定和执行访问物理 CDE 的要求，以识别并授权相关人员。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
9.3.1.1 控制人员在 CDE 内敏感区域的实际访问权限，具体如下： • 是否授权了访问权限，并以个人工作职能为基础。 • 访问权限在离职时立即撤销。 • 所有物理访问机制，例如密钥、访问卡等，在离职时退回或禁用。	**9.3.1.1.a** 观察 CDE 内敏感区域的人员并询问负责人员，检查物理访问控制清单，以核实： • 是否授权了敏感区域的访问权限。 • 访问权限是否为个人工作职能所需。	控制敏感区域的物理访问权限有助于确保只对具有合法业务需求的授权人员授予访问权限。 **良好做法** 在可能的情况下，组织应制定政策和程序，确保人员在离开组织之前，归还所有物理访问机制，或在他们离开时尽快禁用。这将确保人员在离职后无法获得敏感区域的物理访问权限。
	9.3.1.1.b 观察程序并询问相关人员，以核实所有人员的访问权限是否在离职时立即被撤销。	
定制方法目标	**9.3.1.1.c** 对于离职人员，检查物理访问控制清单并询问负责人员，以核实是否已退回或禁用所有物理访问机制（例如密钥、访问卡等）。	
未经授权的人员不能访问敏感区域。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
9.3.2 实施相应程序，以授权和管理访客获得 CDE 的访问权限，包括： • 访客在进入前必须获得授权。 • 访客在任何时候都有专人陪同。 • 访客身份明确，并获得标记或其他过期的身份证明。 • 访客标记或其他身份证明能明显区分访客和工作人员。	**9.3.2.a** 检查书面程序并询问相关人员，核实是否制定了相应程序，以根据本要求规定的所有元素授权和管理访客获得 CDE 的访问权限。	访客控制对于减少未经授权的恶意人员获得设施和潜在持卡人数据的访问权限能力非常重要。 访客控制确保访客可以被识别为访客，以便工作人员能够监控他们的活动，并且他们的访问被限制在其合法访问的时间内。
	9.3.2.b 观察当访客出现在 CDE 的过程并询问相关人员，以核实访客： • 是否在进入 CDE 前已获得授权。 • 在 CDE 内任何时候都有专人陪同。	
	9.3.2.c 观察访客标记或其他身份证明的使用情况，以核实标记或其他身份证明不允许在没有专人陪同的情况下访问 CDE。	
	9.3.2.d 观察 CDE 中的访客，以核实： • 所有访客都使用了访客标记或其他身份证明。 • 访客标记或身份证明能轻易地将访客与工作人员区分开来。	
定制方法目标	**9.3.2.e** 检查访客标记或其他身份证明，并观察标记系统中的证据，以核实访客标记或其他身份证明是否已过期。	
确定和执行访客访问 CDE 的要求。访客在 CDE 内不能超过任何允许的授权物理访问。		

要求和测试程序		指南
规定的方法要求 **9.3.3** 在访客离开设施之前或在到期之日交出或停用访客标记或身份证明。 **定制方法目标** 过期后不能再使用访客身份证明或标记。	**规定的方法测试程序** **9.3.3** 观察访客离开设施的情况并询问相关人员，以核实是否在访客离开设施之前或在到期之日交出或停用访客标记或其他身份证明。	**目的** 确保访客标记在访问期满或结束后被归还或停用，以防止恶意人士在访问结束后使用先前授权的通行证进入大楼。
规定的方法要求 **9.3.4** 访客日志用于保持设施内和敏感区域内访客活动的实际记录，包括： • 访客的姓名和所代表的组织。 • 访问的日期和时间。 • 授权实际访问权限的人员的姓名。 • 保留该记录至少三个月，除非法律另有限制。 **定制方法目标** 保留能够识别个人身份的访客访问记录。	**规定的方法测试程序** **9.3.4.a** 检查访客日志并询问负责人员，以核实是否使用了访客日志记录了设施和敏感区域的实际访问权限。 **9.3.4.b** 检查访客日志，核实日志是否包含： • 访客的姓名和所代表的组织。 • 授权实际访问权限的人员。 • 访问的日期和时间。 **9.3.4.c** 检查访客日志的存储位置并询问负责人员，以核实日志是否至少保留了三个月（除非法律另有限制）。	**目的** 记录访客最低限度信息的访客日志易于维护且成本低廉。它将有助于识别建筑物或房间的历史性物理访问权限以及持卡人数据的潜在访问权限。 **良好做法** 在记录访问日期和时间时，包括进入和离开的时间被认为是最佳做法，因为它提供了有用的跟踪信息，并保证了访客在一天结束时已经离开。确认访客的身份证（驾驶执照等）与他们在访客日志上的名字相符也是很好的做法。

要求和测试程序		指南
9.4 安全存储、访问、分发和销毁含有持卡人数据的媒体。		
规定的方法要求 9.4.1 所有带有持卡人数据的媒体都被存储在一个安全的实体位置。 **定制方法目标** 未经授权的人员不能查阅带有持卡人数据的媒体。	**规定的方法测试程序** **9.4.1** 检查文件，核实是否确定了保护持卡人数据的相应程序，包括对所有媒体进行物理保护的控制	**目的** 物理保护媒体的控制旨在防止未经授权的人员获得任何媒体上持卡人数据的访问权限。如果持卡人数据在可移动或便携式媒体上、打印出来或留在某人的办公桌上时没有受到保护，则很容易被未经授权的人查看、复制或扫描。
9.4.1.1 带有持卡人数据的离线媒体备份被存储在一个安全的位置。 **定制方法目标** 未经授权的人员不能查阅离线备份。	**9.4.1. 1.a** 检查文件，核实是否制定了相应程序，以在安全位置对带有持卡人数据的离线媒体备份进行物理保护。 **9.4.1.1.b** 检查日志或其他文件并询问存储地点的负责人员，以核实离线媒体备份是否存储在安全位置。	**目的** 物理保护媒体的控制旨在防止未经授权的人员获得任何媒体上持卡人数据的访问权限。如果持卡人数据在可移动或便携式媒体上、打印出来或留在某人的办公桌上时没有受到保护，则很容易被未经授权的人查看、复制或扫描。 如果存储在不安全的设施中，包含持卡人数据的备份可能很容易丢失、被盗，或被恶意复制。 **良好做法** 对于安全存储备份媒体，一个良好的做法是将媒体存储在一个非现场设施中，例如备用或备份站点或商业存储设施。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 定期审核存储设施，使组织能够及时解决所发现的安全问题，将潜在风险降到最低。该实体必须了解存储媒体所在区域的安全性。
9.4.1.2 至少每 12 个月审核一次存有持卡人数据的离线媒体备份位置的安全性。	**9.4.1.2.a** 检查文件，核实是否制定了相应程序，以至少每 12 个月审核一次存有持卡人数据的离线媒体备份位置的安全性。	
	9.4.1.2.b 检查书面程序、日志或其他文件并询问存储地点的负责人员，以核实存储位置的安全性是否至少每 12 个月审核一次。	
定制方法目标		
通过检查定期核实保护离线备份的安全控制。		
规定的方法要求	**规定的方法测试程序**	**目的** 未确定为机密的媒体可能无法得到充分保护，或者可能丢失或被盗。 **良好做法** 重要的是，要对媒体进行标识，使其分类状态一目了然。但这并不意味着媒体需要贴上“机密”标签。
9.4.2 所有载有持卡人数据的媒体都要根据数据的敏感性进行分类。	**9.4.2.a** 检查文件，核实是否制定了相应程序，以根据数据的敏感性对载有持卡人数据的媒体进行分类。	
	9.4.2.b 检查媒体日志或其他文件，以核实是否根据数据的敏感性对所有媒体进行了分类。	
定制方法目标		
适当地分类和保护媒体。		

要求和测试程序		指南
规定的方法要求 **9.4.3** 保护设施外发送的载有持卡人数据的媒体，具体如下： • 记录设施外发送的媒体。 • 通过安全的快递公司或其他可以准确追踪的交付方式发送媒体。 • 场外追踪记录包括有关媒体位置的详细信息。 **定制方法目标** 在设施外运输时，对媒体进行安全保护和追踪。	**规定的方法测试程序** **9.4.3.a** 检查文件，核实是否制定了相应程序，以根据本要求中规定的所有元素保护了设施外发送的媒体。 **9.4.3.b** 询问相关人员并检查记录，以核实记录了所有设施外发送的媒体，并通过安全的快递公司或其他可追踪的交付方式发送。 **9.4.3.c** 检查所有媒体的场外追踪记录，以核实是否记录了追踪细节。	**目的** 如果通过非可追踪的方法（例如普通邮件）发送，媒体可能会丢失或被盗。使用安全的快递公司运送任何载有持卡人数据的媒体，允许组织使用他们的跟踪系统来维护库存和运输位置。
规定的方法要求 **9.4.4** 管理层批准所有含有持卡人数据的媒体移出设施（包括当媒体被分发给个人时）。 **定制方法目标** 未经负责人员的批准，媒体不能离开设施。	**规定的方法测试程序** **9.4.4.a** 检查文件，核实是否制定了相应程序，以确保管理层批准了移出设施的媒体。 **9.4.4.b** 检查场外媒体追踪日志并询问负责人员，核实所有移出设施的媒体（包括分发给个人的媒体）是否均获得适当的管理授权。	**目的** 如果没有严格程序来确保所有媒体的移动在从安全区域移出之前得到批准，那么媒体将无法被追踪或得到适当保护，其位置也将不为人知，导致媒体丢失或被盗。

要求和测试程序		指南
适用性说明 批准媒体移动的个人应具有适当的管理权限来授予此批准。然而，并不特别要求这些个人的头衔中包括“经理”。		
规定的方法要求 **9.4.5** 保留所有含有持卡人数据的电子媒体的库存日志。 **定制方法目标** 保留存储电子媒体的准确清单。	**规定的方法测试程序** **9.4.5.a** 检查文件，核实是否制定了相应程序，以保留电子媒体库存日志。 **9.4.5.b** 检查电子媒体库存日志并询问负责人员，核实是否保留了该日志。	**目的** 如果没有仔细的盘点方法和存储控制，可能会无期限地没有注意到被盗或丢失的电子媒体。
规定的方法要求 **9.4.5.1** 至少每 12 个月对含有持卡人数据的电子媒体进行一次清点。 **定制方法目标** 定期核实媒体清单。	**规定的方法测试程序** **9.4.5.1.a** 检查文件，核实是否制定了相应程序，以至少每 12 个月对含有持卡人数据的电子媒体进行一次盘点。 **9.4.5.1.b** 检查电子媒体盘点日志并询问相关人员，以核实是否至少每 12 个月执行了一次电子媒体盘点。	**目的** 如果没有仔细的盘点方法和存储控制，可能会无期限地没有注意到被盗或丢失的电子媒体。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
9.4.6 当因业务或法律原因不再需要载有持卡人数据的硬拷贝材料时，将按以下方式进行销毁： • 材料被交叉切碎、焚烧或粉碎，从而无法重建持卡人数据。 • 材料在销毁前被储存在安全储存容器中。	**9.4.6.a** 检查定期媒体销毁政策，以核实是否制定了相应程序，当因业务或法律原因不再需要载有持卡人数据的硬拷贝材料时，将按照本要求规定的所有元素进行销毁。	如果不采取步骤在处置前销毁硬拷贝媒体上的信息，恶意者可能会检索被处置媒体中的信息，导致数据威胁。例如，恶意者可能会使用一种被称为“垃圾搜寻”的技术，他们在垃圾箱和回收箱中寻找带有信息的硬拷贝材料，以便用来发动攻击。 保护用来存放即将被销毁的材料的存储容器，可以防止在收集材料的过程中捕获敏感信息。
	9.4.6.b 观察流程并询问相关人员，以核实是否交叉粉碎、焚烧或粉碎了硬拷贝材料，从而无法重建持卡人数据。	**良好做法** 考虑在“待粉碎”的容器上加锁，以防止对其内容物的访问，或防止对容器内部的实体访问。
定制方法目标 不能从已被销毁或待销毁的媒体中恢复持卡人数据。	**9.4.6.c** 观察用于存放含有将被销毁的信息的材料的容器，以核实这些容器是否安全。	**更多信息** 请参见 *NIST 特别出版物 800-88，修订版 1。媒体消毒指南。*
适用性说明 当因业务或法律原因不再需要媒体时，这些关于媒体销毁的要求与 PCI DSS 要求 3.2.1 是分开的、不同的，后者是在根据实体的持卡人数据保留政策不再需要时安全地删除持卡人数据。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
9.4.7 当因业务或法律原因不再需要载有持卡人数据的电子媒体时，将通过以下方式之一进行销毁： • 销毁电子媒体。 • 不可恢复持卡人数据，从而无法重建。	**9.4.7.a** 检查定期媒体销毁政策，以核实是否制定了相应程序，当因业务或法律原因不再需要持卡人数据时，将按照本要求规定的所有元素进行销毁。	如果不采取措施在不再需要时销毁电子媒体上的信息，恶意者可能会检索被处置媒体中的信息，导致数据威胁。例如，恶意者可能会使用一种被称为“垃圾搜寻”的技术，他们在垃圾箱和回收箱中寻找硬拷贝材料，以便用来发动攻击。
定制方法目标	**9.4.7.b** 观察媒体销毁流程并询问负责人员，以核实是否通过本要求中规定的其中一种方法销毁了载有持卡人数据的电子媒体。	**良好做法**
不能从已被删除或销毁的媒体中恢复持卡人数据。		大多数操作系统中的删除功能允许恢复删除的数据，因此，应使用专门的安全删除功能或应用程序来使数据无法恢复。
适用性说明		**示例**
当因业务或法律原因不再需要媒体时，这些关于媒体销毁的要求与 PCI DSS 要求 3.2.1 是分开的、不同的，后者是在根据实体的持卡人数据保留政策不再需要时安全地删除持卡人数据。		安全销毁电子媒体的方法包括根据行业公认的安全删除标准进行安全擦拭、消磁或物理销毁（如研磨或粉碎硬盘）。
		更多信息
		请参见 *NIST 特别出版物 800-88，修订版 1。媒体消毒指南*

要求和测试程序		指南
9.5 保护交互点（POI）设备免于篡改和未经授权的替代。		
规定的方法要求	**规定的方法测试程序**	**目的**
9.5.1 通过与支付卡形式因素的直接物理互动来获取支付卡数据的 POI 设备应该受到保护，防止篡改和未经授权的替代，包括以下内容： • 备存一份 POI 设备的清单。 • 定期检查 POI 设备，查看是否有篡改或未经授权的替代行为。 • 培训人员注意可疑行为，并报告设备的篡改或未经授权的替代行为。	**9.5.1** 检查书面政策和程序，以核实是否制定了相应流程，包括本要求中规定的所有元素。	犯罪分子试图通过偷窃和/或操纵读卡设备和终端来窃取支付卡数据。犯罪分子会试图偷窃设备，以便他们可以学习如何入侵这些设备，而且他们经常试图利用欺诈性的设备取代合法的设备，在每次输入支付卡时向他们发送支付卡数据。 他们还试图在设备的外部添加“盗刷”组件，这些组件的目的是在支付卡数据进入设备之前捕获这些数据—例如，在合法的读卡器上附加一个额外的读卡器，从而捕获支付卡数据两次：一次由犯罪分子的组件捕获，另一次由设备的合法组件捕获。通过这种方式，在犯罪分子“盗刷”支付卡数据的过程中，交易仍然可以不受干扰地完成。
定制方法目标		**更多信息**
实体已经确定了保护和管理交互点设备的程序。受影响人员确定管理和保护 POI 设备的期望、控制和监督，并由其遵守。		PCI SSC 网站提供更多关于防止盗刷的最佳实践。
适用性说明		
这些要求适用于在实体信用卡交易中使用的已部署 POI 设备（即，支付卡的形式因素，例如刷卡、点卡或蘸卡）。本要求并不旨在适用于手动 PAN 键入组件，如计算机键盘。 本要求建议但不要求适用于手动 PAN 键入组件，如计算机键盘。 本要求不适用于商业现成（COTS）设备（例如，智能手机或平板电脑），这些设备是为大众市场销售而设计的移动商家自有设备。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
9.5.1.1 保留最新的 POI 设备清单，包括： • 设备的品牌和型号。 • 设备的位置。 • 设备序列号或其他独特的识别方法。	**9.5.1.1.a** 检查 POI 设备的清单，以核实它是否包括本要求中规定的所有元素。	保持最新的 POI 设备清单有助于企业追踪设备的位置，并在设备失踪或丢失时快速识别。 **良好做法** 保持设备清单的方法可以是自动的（例如，设备管理系统）或手动的（例如，记录在电子或纸质记录中）。对于即将获得的设备，位置可以包括分配给该设备的人员的名字。 **示例** 维护设备位置的方法包括确定设备所在的场地或设施的地址。
	9.5.1.1.b 观察 POI 设备和设备位置，并与列表中的设备进行比较，以核实该列表是否准确、最新。	
定制方法目标	**9.5.1.1.c** 询问相关人员，以核实当添加、重新安置、退役设备等时是否更新了 POI 设备的清单。	
无论任何时候，记录和了解 POI 设备的标识和位置。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 定期检查设备将有助于组织通过外部证据更快发现篡改行为—例如，增加一个读卡器或更换一台设备，从而将使用欺诈性设备的潜在影响降到最低。 **良好做法** 定期检查的方法包括检查序列号或其他设备特征，并将这些信息与 POI 设备清单进行比较，以核实设备是否没有被替换成欺诈性设备。 **示例** 检查的类型将取决于设备的情况。例如，可以使用已知安全的设备的照片来比较设备的当前外观和它的原始外观，检查它是否有变化。另一个选择可能是使用安全标记笔，例如紫外光标记笔，标记设备表面和设备开口，这样任何篡改或更换都显而易见。犯罪分子往往会更换设备的外壳，以掩盖他们的篡改行为，这些方法可能有助于发现这种活动。设备供应商也可以提供安全指导和"怎么做"指南，以帮助确定设备是否已被篡改。 设备可能已被篡改或替换的迹象包括： • 插入设备的意外附件或电缆。 • 安全标签缺失或改变。 • 外壳破损或颜色不同。 • 序列号或其他外部标记的改变。
9.5.1.2 定期检查 POI 装置的表面，以检测篡改和未经授权的替换。	**9.5.1.2.a** 检查书面程序，核实是否制定了相应流程，以定期检查 POI 装置的表面，以检测篡改和未经授权的替换。	
	9.5.1.2.b 询问负责人员并观察检查流程，以核实： • 人员了解检查装置的程序。 • 定期检查所有装置，确认是否有篡改和未经授权的替换的证据。	
定制方法目标		
不能篡改交互点设备，不能在没有授权的情况下替换交互点设备，也不能在没有及时检测的情况下安装盗刷附件。		

要求和测试程序		指南
规定的方法要求 **9.5.1.2.1** 实体的目标风险分析确定了定期 POI 设备检查的频率和执行的检查类型，该分析根据要求 12.3.1 中规定的所有元素执行。 **定制方法目标** 检查 POI 设备，其频率应与实体的风险相符。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **9.5.1.2.1.a** 检查实体的目标风险分析，了解定期 POI 设备检查的频率和检查的类型，以核实是否根据要求 12.3.1 规定的所有元素执行了风险分析。 **9.5.1.2.1.b** 检查书面的定期设备检查结果并询问相关人员，以核实执行的 POI 设备检查的频率和类型与该实体为该要求执行的目标风险分析中所确定的内容相符。	**目的** 各实体最适合根据设备运行的环境来确定 POI 设备的检查频率。 **良好做法** 检查频率将取决于各种因素，例如设备的位置以及设备是否有人看管。例如，相比于保存在安全区域或在公众可查阅的情况下受到监督的设备，留在公共区域而没有组织人员监督的设备可能接受更频繁的检查。此外，许多 POI 供应商在其用户文件中包含了关于应多长时间检查一次 POI 设备的指导，以及检查的内容–实体应查阅其供应商的文件，并将这些建议纳入其定期检查中。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 犯罪分子通常会冒充经授权的维护人员来获取 POI 设备的访问权限。 **良好做法** 人员培训应包括对任何前来进行 POI 维护的人保持警惕并进行询问，以确保他们获得授权并拥有有效的工作单，包括任何代理人、维护或修理人员、技术人员、服务提供商或其他第三方。在提供访问权限之前，应始终核实所有请求访问设备的第三方—例如，通过与管理层核实或打电话给 POI 维护公司（例如供应商或收单机构）进行核实。许多犯罪分子会试图通过穿着打扮来欺骗工作人员（例如，携带工具箱和穿着工作服），也可能对设备的位置有所了解，因此应培训工作人员始终遵循相应程序。 犯罪分子使用的另一个伎俩是发送一个“新”的 POI 设备，并说明如何与合法设备进行交换，然后“归还”合法设备。犯罪分子甚至可能提供回邮到他们指定的地址。因此，相关人员在安装设备或将其用于业务之前，应始终与他们的经理或供应商核实该设备是否合法，并来自一个可信赖的来源。 **示例** 人员应当注意的可疑行为包括不明人士试图拔掉或打开设备。 确保工作人员了解报告可疑行为的机制以及向谁报告这种行为—例如，经理或安全人员—将有助于减少设备被篡改或替代的可能性和潜在影响。
9.5.1.3 为 POI 环境中的人员提供培训，使其认识到试图篡改或更换 POI 设备的行为，并包括： • 在授予任何第三方人员修改设备或排除故障的权限之前，核实他们的身份是否为所声称的维修或维护人员。 • 确保未经核实的情况下不安装、更换或退回设备的程序。 • 注意设备周围的可疑行为。 • 向有关人员报告可疑行为和设备被篡改或替换的迹象。	**9.5.1.3.a** 审核 POI 环境中人员的培训材料，以核实它们是否包括本要求中规定的所有元素。 **9.5.1.3.b** 询问 POI 环境中的人员，以核实他们是否接受过培训，并了解本要求中规定的所有元素的程序。	
定制方法目标 人员了解针对 POI 设备的攻击类型、实体的技术和程序对策，并能在需要时获得援助和指导。		

定期监控和测试网络

要求 10:　　记录并监控系统组件和持卡人数据的所有访问权限

章节
10.1 确定并记录用于记录和监控系统组件和持卡人数据的所有访问权限的程序和机制。
10.2 实施检查日志，以支持检测异常和可疑活动，以及对事件进行取证分析。
10.3 保护检查日志不被破坏和未经授权的修改。
10.4 审核检查日志，以确定异常或可疑的活动。
10.5 保留检查日志历史，并可用于分析。
10.6 时间同步机制支持所有系统的一致时间设置。
10.7 及时检测、报告和响应关键安全控制系统的故障。

概述

日志机制和跟踪用户活动的能力对于预防、检测或减少数据威胁的影响至关重要。日志存在于所有系统组件和持卡人数据环境（CDE），可以在出错时进行全面的跟踪、报警和分析。如果没有系统活动日志，就很难甚至不可能确定威胁的原因。

这项要求适用于用户活动，包括雇员、承包商、顾问、内部和外部供应商以及其他第三方（例如，提供支持或维护服务的人）的活动。

这些要求不适用于消费者（持卡人）的用户活动。

请参阅附录 G 了解 PCI DSS 术语的定义。

要求和测试程序		指南
10.1 确定并记录用于记录和监控系统组件和持卡人数据的所有访问权限的程序和机制。		
规定的方法要求 **10.1.1** 要求 10 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。 **定制方法目标** 受影响人员确定满足要求 10 的活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。	**规定的方法测试程序** **10.1.1** 检查文件并询问相关人员，以核实是否根据本要求中规定的所有元素管理了要求 10 中确定的安全政策和操作程序。	**目的** 要求 10.1.1 涉及有效管理和维护整个要求 10 规定的各种政策和程序。虽然定义要求 10 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。
10.1.2 记录、分配和理解执行要求 10 中活动的角色和责任。	**10.1.2.a** 检查文件，以核实是否记录和分配了执行要求 10 中活动的角色和责任的描述。	
	10.1.2.b 询问负责执行要求 10 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	
定制方法目标		
分配执行要求 10 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。		

要求和测试程序		指南
10.2 实施检查日志，以支持检测异常和可疑活动，以及对事件的取证分析。		
规定的方法要求 **10.2.1** 所有系统组件和持卡人数据的检查日志都已启用并处于活动状态。 **定制方法目标** 获取影响系统组件和持卡人数据的所有活动的记录。	**规定的方法测试程序** **10.2.1** 询问系统管理员并检查系统配置，以核实所有系统组件的检查日志是否已被启用并处于活动状态。	**目的** 所有系统组件都必须有检查日志。检查日志向系统管理员发出警报，为其他监控机制提供数据，例如入侵检测系统（IDS）和安全信息与事件监控系统（SIEM）工具，并为事后调查提供历史记录。 记录和分析与安全有关的事件使企业能够识别和追踪潜在的恶意活动。 **良好做法** 当一个实体考虑在他们的日志中记录哪些信息时，重要的是要记住，存储在检查日志中的信息是敏感信息，应该按照本标准的要求加以保护。应注意只在检查日志中存储必要信息，以将风险降到最低。
规定的方法要求 **10.2.1.1** 检查日志捕获持卡人数据的所有个人用户访问权限。 **定制方法目标** 采集持卡人数据的所有个人用户访问权限的记录。	**规定的方法测试程序** **10.2.1.1** 检查检查日志配置和日志数据，以核实是否记录了持卡人数据的所有个人用户访问权限。	**目的** 拥有一个将用户访问权限与所访问的系统组件联系起来的程序或系统至关重要。恶意者可以了拥有 CDE 中系统的访问权限的用户帐户，或者他们可以创建一个新的、未经授权的帐户来访问持卡人数据。 **良好做法** 所有个人访问持卡人数据的记录可以确定哪些帐户可能已经被威胁或被滥用。

要求和测试程序		指南
规定的方法要求 **10.2.1.2** 检查日志捕获任何具有管理权限的个人所采取的所有行动，包括对应用程序或系统帐户的任何互动使用。 **定制方法目标** 采集具有较高权限的个人执行的所有行动的记录。	**规定的方法测试程序** **10.2.1.2** 检查检查日志配置和日志数据，以核实是否记录了任何具有管理访问权限的个人所采取的所有行动，包括对应用程序或系统帐户的任何互动使用。	**目的** 具有更高访问权限的帐户，例如“管理员”或“根用户”帐户，有可能对系统的安全或操作功能产生重大影响。如果没有所执行活动的日志，组织就无法将管理错误或误用权限导致的任何问题追溯到具体的行动和帐户。 **定义** 具有管理权限的帐户是指那些被分配有特定权限或能力的帐户，以管理系统、网络和/或应用程序。被视为是管理的功能或活动超出了普通用户作为常规业务功能的一部分所执行的功能或活动。
规定的方法要求 **10.2.1.3** 检查日志采集检查日志的所有访问权限。 **定制方法目标** 获取检查日志的所有访问记录。	**规定的方法测试程序** **10.2.1.3** 检查检查日志配置和日志数据，以核实是否采集了检查日志的访问权限。	**目的** 恶意用户经常试图改变检查日志以隐藏他们的行为。访问记录允许组织追踪任何不一致或潜在的篡改日志到个人帐户。日志识别检查日志的更改、添加和删除，这有助于追溯未经授权人员采取的步骤。
规定的方法要求 **10.2.1.4** 检查日志捕获所有无效的逻辑访问尝试。 **定制方法目标** 采集所有无效访问尝试的记录。	**规定的方法测试程序** **10.2.1.4** 检查检查日志配置和日志数据，以核实是否采集了无效的逻辑访问尝试。	**目的** 恶意者往往会对目标系统进行多次访问尝试。多次无效的登录尝试可能表明一个未经授权的用户试图“蛮力”或猜测密码。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
10.2.1.5 检查日志采集身份和验证凭证的所有变更，包括但不限于： • 创建新的帐户。 • 特权的提升。 • 所有具有管理访问权限的帐户的变更、增加或删除。	**10.2.1.5** 检查检查日志配置和日志数据，以核实是否根据本要求中规定的所有元素采集了识别和验证凭证的变更。	记录验证凭证的变更（包括具有管理权限的帐户的权限提升、添加和删除），提供活动的剩余证据。 恶意用户可能试图操纵验证凭证以绕过它们或冒充有效帐户。
定制方法目标		
采集识别和验证凭证的所有变更的记录。		
规定的方法要求	**规定的方法测试程序**	**目的**
10.2.1.6 检查日志采集以下内容： • 所有新检查日志的初始化，以及 • 所有启动、停止或暂停现有检查日志的行为。	**10.2.1.6** 检查检查日志配置和日志数据，以核实是否采集了本要求中规定的所有元素。	在执行非法活动之前关闭或暂停检查日志是那些希望避免被发现的恶意用户的常见做法。检查日志的初始化可能表明，用户禁用了日志功能以隐藏他们的行为。
定制方法目标		
采集检查日志活动状态的所有变化的记录。		
规定的方法要求	**规定的方法测试程序**	**目的**
10.2.1.7 检查日志采集所有系统级对象的创建和删除情况。	**10.2.1.7** 检查检查日志配置和日志数据，以核实是否采集了所有系统级对象的创建和删除情况。	恶意软件，例如恶意软件，经常在目标系统上创建或替换系统级对象，以控制该系统的某项功能或操作。通过记录创建或删除系统级对象的时间，将更容易确定是否授权了此类修改。
定制方法目标		
采集表明系统已从其预定功能中被修改的更改记录。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
10.2.2 检查日志记录了每个可审计事件的细节，包括： • 用户识别。 • 事件的类型。 • 日期和时间。 • 成功和失败指示。 • 事件的起源。 • 受影响数据、系统组件、资源或服务的身份或名称（例如，名称和协议）。	**10.2.2** 询问相关人员并检查检查日志配置和日志数据，以核实本要求中规定的所有元素是否都包含在每个可审计事件（从 10.2.1.1 到 10.2.1.7）的日志条目中。	通过记录 10.2.1.1 至 10.2.1.7 的可检查事件的详细信息，可以快速识别潜在威胁，并提供足够的详细信息，以便对可疑活动进行跟踪。
定制方法目标		
采集足够数据，以便能够识别成功和失败的尝试，以及要求 10.2.1 中列出的每个事件的人、事、时间、地点和方式。		

要求和测试程序		指南
10.3 保护检查日志不被破坏和未经授权的修改。		
规定的方法要求 **10.3.1** 检查日志文件的读取权限仅限于有工作需要的人。 **定制方法目标** 未经授权的人员不能查阅存储的活动记录。	**规定的方法测试程序** **10.3.1** 询问系统管理员并检查系统配置和权限，以核实是否只有工作需要的个人拥有检查日志文件的读取权限。	**目的** 检查日志文件包含敏感信息，日志文件的读取访问权限必须仅限于有有效业务需求的人。这种访问包括源系统上的检查日志文件，以及存储它们的其他地方。 **良好做法** 充分保护检查日志，包括强大的访问控制，只根据“需要知道”来限制日志的访问权限，并使用物理或网络隔离来使日志更难找到和修改。
规定的方法要求 **10.3.2** 保护检查日志文件免于个人修改。 **定制方法目标** 工作人员不能修改存储的活动记录。	**规定的方法测试程序** **10.3.2** 检查系统配置和权限，并询问系统管理员，以核实是否通过访问控制机制、物理隔离和/或网络隔离，保护当前检查日志文件免于个人修改。	**目的** 通常情况下，进入网络的恶意人员会试图编辑检查日志以隐藏他们的活动。如果不充分保护检查日志，就不能保证其完整性、精确性、和完整性，而且检查日志在威胁后作为调查工具也会失去作用。因此，检查日志应该在原始系统以及存储它们的其他地方上受到保护。 **良好做法** 各实体应尝试防止日志暴露在公众可访问的位置上。

<table>
<tr><th colspan="2">要求和测试程序</th><th>指南</th></tr>
<tr><td>规定的方法要求</td><td>规定的方法测试程序</td><td rowspan="2">目的
及时将日志备份到一个集中的日志服务器或难以修改的媒体上，使日志得到保护，即使生成日志的系统受到威胁。
从面向外部的技术（例如无线、网络安全控制、DNS 和邮件服务器）写入日志，可以减少这些日志丢失或被更改的风险。
良好做法
每个实体决定了备份日志文件的最佳方式，无论是通过一个或多个集中的日志服务器还是其他安全媒体。日志可以直接写入、卸载，或从外部系统复制到安全的内部系统或媒体。</td></tr>
<tr><td>10.3.3 检查日志文件，包括那些面向外部的技术，及时备份到安全的集中内部日志服务器或其他难以修改的媒体。

定制方法目标
存储的活动记录是安全的，并保存在一个集中的位置，以防止未经授权的修改。</td><td>10.3.3 检查备份配置或日志文件，以核实当前的检查日志文件，包括那些面向外部的技术，是否及时备份到安全的集中内部日志服务器或其他难以修改的媒体。</td></tr>
<tr><td>规定的方法要求</td><td>规定的方法测试程序</td><td rowspan="2">目的
文件完整性监控或变更检测系统检查关键文件的变更，并在发现变更时予以通知。出于文件完整性监控的目的，实体通常会监控那些不定期更改的文件，但当更改时，表明可能存在威胁。
良好做法
用于监控检查日志变更的软件应被配置为在改变或删除现有日志数据或文件时提供警报。然而，被添加到检查日志的新日志数据不应产生警报。</td></tr>
<tr><td>10.3.4 文件完整性监控或变更检测机制用于检查日志，以确保在没有产生警报的情况下不能改变现有的日志数据。

定制方法目标
在不产生警报的情况下，不能修改存储的活动记录。</td><td>10.3.4 检查系统设置、受监控的文件和监控活动的结果，以核实文件完整性监控或变更检测软件是否用于检查日志。</td></tr>
</table>

要求和测试程序		指南
10.4 审核检查日志，以确定异常或可疑的活动。		
规定的方法要求	**规定的方法测试程序**	**目的**
10.4.1 以下检查日志每天至少审核一次： • 所有安全事件。 • 所有存储、处理或传输 CHD 和/或 SAD 的系统组件的日志。 • 所有关键系统组件的日志。 • 所有执行安全功能的服务器和系统组件的日志（例如，网络安全控制、入侵检测系统/入侵防御系统（IDS/IPS）、验证服务器）。	**10.4.1.a** 检查安全政策和程序，核实是否制定了相应程序，以至少每天审核一次本要求中规定的所有元素。 **10.4.1.b** 观察程序并询问相关人员，以核实本要求中规定的所有元素是否至少每天审核一次。	有许多漏洞在被检测到的前几个月前早已发生。定期的日志审核意味着可以快速识别和积极处理事件。 **良好做法** 每天检查日志（一周 7 天，一年 365 天，包括节假日）可以最大限度地减少潜在漏洞的时间和暴露程度。日志采集、解析和警报工具、集中的日志管理系统、事件日志分析器以及安全信息和事件管理（SIEM）解决方案是可以用来满足这一要求的自动化工具的例子。 每天审核安全事件—例如，识别可疑或异常活动的通知或警报，以及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，对于识别潜在问题是必要的。 每个组织对“安全事件”的判断会有所不同，可能包括对技术类型、位置和设备功能的考虑。各组织可能还希望保持一个“正常”流量的基线，以帮助识别异常行为。 使用第三方服务提供商执行日志审核服务的实体有责任向服务提供商提供有关实体环境的背景信息，以便其了解实体的环境，拥有实体的 “正常 ”流量基线，并能够检测潜在的安全问题，提供准确的例外和异常通知。
定制方法目标		
迅速识别潜在的可疑或异常活动，以将影响降至最低。		

要求和测试程序		指南
规定的方法要求 **10.4.1.1** 使用自动化机制来执行检查日志审核。 **定制方法目标** 通过一个可重复的、一致的机制来识别潜在的可疑或异常的活动。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **10.4.1.1** 检查日志审核机制并询问相关人员，以核实是否使用了自动化机制来执行日志审核。	**目的** 由于产生了大量的日志数据，即使是一两个系统，也很难执行人工日志审核。然而，使用日志采集、解析和警报工具、集中的日志管理系统、事件日志分析器以及安全信息和事件管理（SIEM）解决方案可以通过识别需要审核的日志事件来帮助促进这一流程。 **良好做法** 实体应通过定期审核工具设置和更新设置以反映任何变化，使日志工具与环境中的任何变化保持一致。
规定的方法要求 **10.4.2** 定期审核所有其他系统组件（未在要求 10.4.1 中指定的组件）的日志。 **定制方法目标** 根据实体确定的风险，审核其他系统组件（未包括在 10.4.1 中）的潜在可疑或异常活动。 **适用性说明** 本要求适用于不包括在要求 10.4.1 中的所有其他范围内系统组件。	**规定的方法测试程序** **10.4.2.a** 检查安全政策和程序，核实是否制定了相应程序，以定期审核所有其他系统组件的日志。 **10.4.2.b** 检查书面日志审核结果并询问相关人员，以核实是否定期执行了日志审核。	**目的** 定期审核所有其他系统组件的日志（未在要求 10.4.1 中指定），有助于识别潜在问题的迹象或通过较不关键的系统访问关键系统的企图。

要求和测试程序		指南
规定的方法要求 **10.4.2.1** 实体的目标风险分析确定了所有其他系统组件（未在要求 10.4.1 中确定）的定期日志审核频率，核实是否根据要求 12.3.1 规定的所有元素执行了风险分析。	**规定的方法测试程序** **10.4.2.1.a** 检查该实体的目标风险分析，了解所有其他系统组件（未在要求 10.4.1 中规定）的定期日志审查频率，核实是否根据要求 12.3.1 规定的所有元素执行了风险分析。	**目的** 各实体可以根据每个实体环境的复杂性、需要评估的系统类型的数量以及这些系统的功能等标准来确定审核这些日志的最佳时期。
	10.4.2.1.b 检查所有其他系统组件（未在要求 10.4.1 中规定）的定期日志审查的书面结果并询问相关人员，核实是否根据实体为该要求执行的目标风险分析中规定的频率执行了日志审查。	
定制方法目标 以解决实体风险的频率执行较低风险系统组件的日志审查。		
适用性说明 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 如果不对日志审查过程中发现的例外和异常情况进行调查，实体可能不知道其网络中发生的未经授权和潜在的恶意活动。 **良好做法** 各实体在制定其规定和管理例外和异常情况的流程时，应考虑如何解决以下问题： • 如何记录日志审核活动， • 如何排序和优先处理异常情况和异常现象， • 应该制定哪些程序，以报告和逐级上报异常情况和异常现象，以及 • 调查任何补救任务的负责人员。
10.4.3 处理审核过程中发现的异常情况和异常现象。	**10.4.3.a** 检查安全政策和程序，核实是否制定了相应流程，以处理审核过程中发现的异常情况和异常现象。	
	10.4.3.b 观察流程并询问相关人员，以核实在发现异常情况和异常现象后它们是否得到解决。	
定制方法目标		
处理可疑的或异常的活动。		

要求和测试程序		指南
10.5 保留检查日志历史，并可提供用于分析目的。		
规定的方法要求	**规定的方法测试程序**	**良好做法** 有必要保留历史审核日志至少 12 个月，因为人们往往会忽视威胁很长一段时间。有了集中存储的日志历史记录，调查人员便可更好地确定潜在漏洞发生的时长，以及可能受到影响的系统。通过可即时提供的三个月日志，实体可以快速识别并最大限度地降低数据漏洞的影响。 **示例** 允许可即时提供日志的方法包括在线存储日志、归档日志或从备份中快速恢复日志。
10.5.1 保留检查日志历史至少 12 个月，确保可即时提供至少最近三个月的检查日志历史用于分析目的。	**10.5.1.a** 检查文件以核实是否确定了以下内容： • 检查日志保留政策。 • 保留检查日志历史至少 12 个月，并且可即时在线提供至少最近三个月的日志历史的相应程序。	
	10.5.1.b 检查检查日志历史的配置，询问相关人员并检查检查日志，以核实检查日志历史是否保留了至少 12 个月。	
定制方法目标 可即时提供活动历史记录以支持事件响应，并至少保留 12 个月。	**10.5.1.c** 询问相关人员并观察相应流程，核实是否可即时提供至少最近三个月的检查日志历史用于分析目的。	

要求和测试程序		指南
10.6 时间同步机制支持所有系统的一致时间设置。		
规定的方法要求 **10.6.1** 使用时间同步技术同步系统时钟和时间。 **定制方法目标** 在所有系统建立共同时间。 **适用性说明** 保持时间同步技术的时效性包括根据 PCI DSS 要求 6.3.1 和 6.3.3 管理漏洞和修补技术。	**规定的方法测试程序** **10.6.1** 检查系统配置设置，以核实是否实施了时间同步技术并保持最新。	**目的** 时间同步技术用于同步多个系统的时钟。当不能正确同步时钟时，比较来自不同系统的日志文件和建立事件的确切顺序可能会很困难，甚至不可能，这对于漏洞发生后的取证分析至关重要。 对于事故后取证团队来说，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于确定系统遭到威胁的具体方式至关重要。 **示例** 网络时间协议（NTP）是时间同步技术的一个示例。
规定的方法要求 **10.6.2** 配置系统为正确和一致的时间，如下所示： • 一个或多个指定的时间服务器正在使用。 • 只有指定的中央时间服务器接收来自外部来源的时间。 • 从外部来源接收的时间是基于国际原子时或协调世界时（UTC）。 • 指定的时间服务器只接受来自特定行业认可的外部来源的时间更新。 • 如果有一个以上指定的时间服务器，时间服务器之间相互对等，以保持准确的时间。 • 内部系统只接收来自指定中央时间服务器的时间信息。	**规定的方法测试程序** **10.6.2** 检查用于获取、分配和存储正确时间的系统配置设置，以核实是否根据本要求中规定的所有元素配置了这些设置。	**目的** 使用信誉良好的时间服务器是时间同步过程的一个关键组成部分。 接受来自特定的、行业认可的外部来源的时间更新，有助于防止恶意者更改系统的时间设置。 **良好做法** 防止未经授权使用内部时间服务器的另一个选择是用对称密钥加密更新，并创建访问控制列表，指定将获得时间更新的客户机的 IP 地址。

<table>
<tr><th colspan="2">要求和测试程序</th><th>指南</th></tr>
<tr><td colspan="2">定制方法目标

所有系统的时间都是准确、一致的。</td><td></td></tr>
<tr><td>规定的方法要求

10.6.3 时间同步设置和数据的保护方法如下：
• 只有业务需求的人员才能访问时间数据。
• 记录、监控和审核任何对关键系统上时间设置所做的更改。</td><td>规定的方法测试程序

10.6.3.a 检查系统配置和时间同步设置，以核实是否只有业务需求的人员才能访问时间数据。

10.6.3.b 检查系统配置和时间同步设置和日志，并观察流程，以核实是否记录、监控和审核了任何对关键系统上时间设置所做的更改。</td><td rowspan="2">目的

攻击者会试图更改时间配置来隐藏他们的活动。因此，限制管理员更改或修改时间同步配置或系统时间的能力，将减少攻击者成功更改时间配置的概率。</td></tr>
<tr><td colspan="2">定制方法目标

未经授权的人员不得修改系统时间设置。</td></tr>
</table>

要求和测试程序		指南
10.7 及时检测、报告和响应关键安全控制系统的故障。		
规定的方法要求	**规定的方法测试程序**	**目的**
10.7.1 ***仅针对服务提供者的额外要求：*** 及时检测、警报和处理关键安全控制系统故障，包括但不限于以下关键安全控制系统的故障： • 网络安全控制。 • IDS/IPS。 • FIM。 • 反恶意软件解决方案。 • 实体访问控制。 • 逻辑访问控制。 • 检查日志机制。 • 分段控制（如果使用）。	**10.7.1.a** ***仅针对服务提供商评估的额外测试程序：*** 检查文件，核实是否制定了相应流程，以及及时检测和处理关键安全控制系统故障，包括但不限于本要求中规定的所有元素的故障。	如果没有正式的程序来检测关键安全控制故障并发出警报，可能在很长一段时间内不会发现故障，并为攻击者提供充足的时间来威胁系统组件并从 CDE 窃取帐户数据。
定制方法目标	**10.7.1.b** ***仅针对服务提供商评估的额外测试程序：*** 观察检测和警报程序并询问相关人员，以核实是否检测和报告了关键安全控制系统的故障，并且关键安全控制每次发生故障时是否都会产生警报。	**良好做法**
及时检测并处理关键安全控制系统的故障。		故障的具体类型可能有所不同，取决于设备系统组件的功能和使用的技术。典型的故障包括系统停止执行其安全功能或不按预期方式运行，如防火墙删除其所有规则或离线。
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。从 2025 年 3 月 31 日起，这项要求将被要求 10.7.2 所取代。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
10.7.2 及时检测、警报和处理关键安全控制系统故障，包括但不限于以下关键安全控制系统的故障： • 网络安全控制。 • IDS/IPS。 • 变更检测机制。 • 反恶意软件解决方案。 • 实体访问控制。 • 逻辑访问控制。 • 检查日志机制。 • 分段控制（如果使用）。 • 检查日志审核机制。 • 自动化安全测试工具（如果使用）。	**10.7.2.a** 检查文件，核实是否制定了相应流程，以及时检测和处理关键安全控制系统故障，包括但不限于本要求中规定的所有元素的故障。	如果没有正式的程序来检测关键安全控制故障并发出警报，可能在很长一段时间内不会发现故障，并为攻击者提供充足的时间来威胁系统组件并从 CDE 窃取帐户数据。
定制方法目标	**10.7.2.b** 观察检测和警报程序并询问相关人员，以核实是否检测和报告了关键安全控制系统的故障，并且关键安全控制每次发生故障时是否都会产生警报。	**良好做法**
及时检测并处理关键安全控制系统的故障。		故障的具体类型可能有所不同，取决于设备系统组件的功能和使用的技术。然而，典型的故障包括系统不再执行其安全功能或不按预期方式运作—例如，防火墙删除其规则或离线。
适用性说明		
本要求将适用于包括服务提供商在内的所有实体，并从 2025 年 3 月 31 日起取代要求 10.7.1。它包括不在要求 10.7.1 中的另外两个关键安全控制系统。 ***本要求在 2025 年 3 月 31 日之前是最佳****实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
10.7.3 任何关键安全控制系统会在每次故障发生时作出及时响应，包括但不限于： • 恢复安全功能。 • 识别并记录安全故障的持续时间（从开始到结束的日期和时间）。 • 识别并记录故障的原因，并记录所需的补救措施。 • 识别并解决故障期间出现的任何安全问题。 • 确定是否由于安全故障而需要采取进一步行动。 • 实施控制以防止故障原因再次发生。 • 恢复安全控制监控。	**10.7.3.a** 检查文件并询问相关人员，核实是否制定并实施了相应流程，以应对任何关键安全控制系统故障，并至少包括本要求中规定的所有元素。	如果没有快速、有效响应关键安全控制系统的故障警报，攻击者可能会利用这段时间插入恶意软件，获得系统控制权，或窃取实体环境中的数据。
定制方法目标	**10.7.3.b** 检查记录，核实是否记录了关键安全控制系统故障，其中包括： • 识别故障的原因： • 安全故障的持续时间（开始和结束的日期和时间）。 • 解决根本原因所需的补救措施的细节。	**良好做法**
分析、控制和解决关键安全控制系统故障，并恢复安全控制，以将影响降至最低。解决由此产生的安全问题，并采取措施以防止再次发生。		书面证据（例如，问题管理系统内的记录）应支持应对安全故障的现有流程和程序。此外，工作人员应了解他们在发生故障时的责任。应在书面证据中记录对故障采取的相应行动和应对措施。
适用性说明		
在 2025 年 3 月 31 日之前，本要求仅在被评估实体是服务提供商的情况下适用，在未来生效日期后本要求将适用于所有实体。 ***本要求是当前 v3.2.1*** 的要求，仅适用于服务提供商。然而，该要求在 2025 年 3 月 31 日之前是所有其他实体的最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。		

要求 11: 定期测试系统和网络的安全性

章节
11.1 确定并理解用于定期测试系统和网络的安全性的程序和机制。
11.2 识别并监控无线接入点，并处理未经授权的无线接入点。
11.3 定期识别、优先排序并处理外部和内部的漏洞。
11.4 定期执行外部和内部穿透测试，并纠正可利用的漏洞和安全弱点。
11.5 检测并响应网络入侵和意外的文件变更。
11.6 检测并响应支付页面上未经授权的变更。

概述

恶意者和研究人员不断发现漏洞，并通过新的软件将其引入。应经常测试系统组件、流程以及订制和定制软件，以确保安全控制能够持续反映不断变化的环境。

请参阅附录 G 了解 PCI DSS 术语的定义。

要求和测试程序		指南
11.1 确定并理解用于定期测试系统和网络的安全性的程序和机制。		
规定的方法要求 **11.1.1** 要求 11 中确定的所有安全政策和操作程序都： • 有文件记录。 • 保持时效性。 • 在使用中。 • 为所有受影响的各方所了解。 **定制方法目标** 受影响人员确定满足要求 11 内活动的期望、控制和监督，并由其遵守。所有支持性活动都可重复一致适用，并符合管理层的意图。	**规定的方法测试程序** **11.1.1** 检查文件和询问相关人员，以核实是否根据本要求中规定的所有元素管理了安全政策和操作程序。	**目的** 要求 11.1.1 涉及有效管理和维护整个要求 11 规定的各种政策和程序。虽然定义要求 11 中规定的具体政策或程序很重要，但同样重要的是确保适当地记录、维护和传播这些政策或程序。 **良好做法** 视情况更新政策和程序，以应对流程、技术和业务目标的变化，这一点很重要。出于这个原因，考虑在变化发生后尽快更新这些文件，而不仅仅是在定期周期内。 **定义** 安全政策定义了实体的安全目标和原则。操作程序描述了如何执行活动，并确定了为以一致的方式并根据政策目标实现预期结果而遵循的控制、方法和流程。

要求和测试程序		指南
规定的方法要求 **11.1.2** 记录、分配和理解执行要求 11 中活动的角色和责任 **定制方法目标** 分配执行要求 11 中所有活动的日常责任。人员要对这些要求的成功和持续运行负责。	**规定的方法测试程序** **11.1.2.a** 检查文件，核实是否记录和分配了执行要求 11 中活动的角色和责任的描述。 **11.1.2.b** 询问负责执行要求 11 中的活动的人员，以核实是否按照文件规定分配了角色和责任，这些角色和责任是否被理解。	**目的** 如果没有正式分配角色和责任，相关人员可能不知道他们的日常责任，关键活动可能不会发生。 **良好做法** 可以将角色和责任记录在政策和程序中，也可以保存在单独的文件中。 作为沟通角色和责任的一部分，实体可以考虑让人员承认他们接受并理解所分配的角色和责任。 **示例** 记录角色和责任的一种方法是责任分配矩阵，包括谁负责、谁问责、谁咨询、谁知情（也称为 RACI 矩阵）。

要求和测试程序		指南
11.2 识别并监控无线接入点，并处理未经授权的无线接入点。		
规定的方法要求	**规定的方法测试程序**	**目的**
11.2.1 管理经授权的和未经授权的无线接入点，具体如下： • 检测是否存在无线（Wi-Fi）接入点。 • 检测和识别所有授权的和未经授权的无线接入点。 • 测试、检测和识别至少每三个月进行一次。 • 如果使用自动化监控，则通过生成的警报通知人员。	**11.2.1.a** 检查政策和程序，核实是否制定了相应流程，以根据本要求中规定的所有元素管理经授权和未经授权的无线接入点。 **11.2.1.b** 检查正在使用的方法和由此产生的文件并询问相关人员，核实是否制定了相应流程，以根据本要求中规定的所有元素检测和识别经授权和未经授权的无线接入点。 **11.2.1.c** 检查无线评估结果并询问相关人员，以核实是否按照本要求规定的所有元素执行了无线评估。 **11.2.1.d** 如果使用自动化监测，检查配置设置，以核实配置是否会产生警报以通知相关人员。	实施和/或利用网络中的无线技术是恶意用户未经授权访问网络和持卡人数据的常见途径。未经授权的无线设备可以隐藏在计算机或其他系统组件中，或附着在计算机或其他系统组件上。这些设备也可以直接连接到网络端口，连接到网络设备，如交换机或路由器，或作为无线接口卡插入系统组件内。 如果无线设备或网络是在公司不知情的情况下安装的，它可以让攻击者轻易地"隐身"进入网络。检测和清除这种未经授权的接入点，可以减少这种设备被用于攻击的持续时间和可能性。
定制方法目标		**良好做法**
定期识别并处理未经授权的无线接入点。		环境的规模和复杂性将决定将要使用哪些适当工具和流程，为未在环境中安装非法无线接入点这一论点提供充分保证。 例如，对购物中心一个独立的零售亭进行详细的物理检查，其中所有的通信组件都包含在防篡改和防窃启的外壳中，可能足以保证一个非法无线接入点没有被连接或安装。然而，在有多个节点的环境中（如在大型零售店、呼叫中心、服务器室或数据中心），详细的物理检查可能很难。在这种情况下，可以结合多种方法，如结合无线分析器的结果执行物理系统检查。
适用性说明		*（下一页继续）*
即使存在禁止使用无线技术的政策，本要求亦适用，因为攻击者不会阅读并遵守公司政策。 用于满足该要求的方法必须足以检测和识别经授权和未经授权的设备，包括连接到本身是经授权的设备上的未经授权设备。		

要求和测试程序		指南
		定义 这也称为非法接入点检测。 **示例** 可使用的方法包括但不限于无线网络扫描、系统组件和基础设施的物理/逻辑检查、网络访问控制（NAC）或无线 IDS/IPS。NAC 和无线 IDS/IPS 是自动化监测工具的例子。
规定的方法要求 **11.2.2** 保留一份经授权无线接入点清单，包括书面业务理由。 **定制方法目标** 未经授权的无线接入点不会被误认为是经授权的无线接入点。	**规定的方法测试程序** **11.2.2** 检查文件以核实是否保留了一份经授权无线接入点清单，以及是否为所有授权无线接入点记录了业务理由。	**目的** 经授权无线接入点清单可以帮助管理员在检测到未经授权的无线接入点时迅速响应。这有助于主动地减少恶意者对 CDE 的威胁。 **良好做法** 如果使用无线扫描器，同样重要的是要有一个确定的已知接入点列表，这些接入点虽然没有连接到公司的网络，但在扫描时通常会被检测到。这些非公司的设备经常出现在多租户建筑或相互靠近的企业中。然而，重要的是要核实这些设备没有连接到实体的网络端口或通过另一个网络连接的设备，并给出一个类似于附近企业的 SSID。扫描结果应注意此类设备以及如何确定这些设备可以被“忽略”。 此外，如果检测到任何被确定为对 CDE 构成威胁的未经授权的无线接入点，应按照要求 12.10.1 的实体的事件响应计划进行管理。

要求和测试程序		指南
11.3 定期识别、优先处理和解决外部和内部漏洞。		
规定的方法要求	**规定的方法测试程序**	**目的**
11.3.1 执行内部漏洞扫描，具体如下： • 至少每三个月执行一次。 • 解决高风险和关键漏洞（根据要求 6.3.1 中定义的实体的漏洞风险等级）。 • 重新执行扫描，确认所有高风险和关键漏洞（如上所述）均已得到解决。 • 扫描工具保持最新的漏洞信息。 • 扫描工作由合格人员执行，存在组织对测试人员的独立性。	**11.3.1.a** 检查过去 12 个月的内部扫描报告结果，以核实最近 12 个月内是否至少每三个月进行一次内部扫描。	及时识别并处理漏洞，减少漏洞被利用的可能性，以及系统组件或持卡人数据被威胁的可能性。至少每三个月执行一次漏洞扫描，提供这种检测和识别。
	11.3.1.b 检查过去 12 个月内每次扫描和重新扫描的内部扫描报告结果，以核实是否解决了所有高风险和关键漏洞（在 PCI DSS 要求 6.3.1 中确定的）。	**良好做法** 应最优先级解决对环境造成最大风险的漏洞（例如，根据要求 6.3.1 被列为高等级或关键等级）。 可以为季度扫描过程结合多个扫描报告，以显示扫描了所有系统，并且解决了所有适用漏洞，这是三个月的漏洞扫描周期的一部分。然而，可能需要额外的文件来核实是否正在解决未修复的漏洞。 虽然要求至少每三个月扫描一次，但根据网络的复杂性、变更频率以及使用的设备、软件和操作系统的类型，建议更频繁地进行扫描。
	11.3.1.c 检查扫描工具配置并询问有关人员，核实扫描工具是否保持了最新的漏洞信息。	
	11.3.1.d 询问负责人员，以核实扫描是否由合格的内部资源或合格的外部第三方执行，并且存在组织对测试人员的独立性。	
定制方法目标		**定义**
使用自动化工具定期核实所有系统组件的安全状况，该工具旨在检测网络内部运行的漏洞。根据正式的风险评估框架，评估和纠正检测到的漏洞。		漏洞扫描是针对外部和内部设备和服务器运行的自动化工具、技术和/或方法的组合，旨在暴露应用程序、操作系统和网络设备中可能被恶意人员发现和利用的潜在漏洞。
（下一页继续）		

<table>
<tr><th colspan="2">要求和测试程序</th><th>指南</th></tr>
<tr><td colspan="2">适用性说明

不要求使用 QSA 或 ASV 执行内部漏洞扫描。

内部漏洞扫描可由合格的内部工作人员进行，他们应合理地独立于被扫描的系统组件（例如，网络管理员不应负责扫描网络），或者实体可选择由专门从事漏洞扫描的公司执行内部漏洞扫描。</td><td></td></tr>
<tr><td>规定的方法要求

11.3.1.1 管理所有其他适用漏洞（根据要求 6.3.1 中实体的漏洞风险等级，那些未被列为高风险或关键的漏洞），具体如下：

• 根据实体的目标风险分析中定义的风险处理，即根据要求 12.3.1 中规定的所有元素执行。

• 视情况重新执行扫描。

定制方法目标

根据实体风险的频率处理等级较低的漏洞（低于高风险或关键）。</td><td>规定的方法测试程序

11.3.1.1.a 检查实体的目标风险分析，该分析确定了解决所有其他适用漏洞的风险（根据要求 6.3.1 中实体的漏洞风险等级，那些未被列为高风险或关键的漏洞），以核实是否根据要求 12.3.1 中规定的所有元素执行了风险分析。

11.3.1.1.b 访谈负责人员并检查内部扫描报告结果或其他文件，以核实是否根据实体的目标风险分析中定义的风险处理了所有其他适用漏洞（根据要求 6.3.1 中实体的漏洞风险等级，那些未被列为高风险或关键的漏洞），并且扫描过程是否包括必要的重新扫描，以确认漏洞已被处理。</td><td>目的

所有漏洞，无论其严重程度如何，都提供了一个潜在的攻击途径，因此必须定期解决，并且必须更快解决暴露出最多风险的漏洞，以限制潜在的攻击窗口。</td></tr>
</table>

要求和测试程序		指南
适用性说明 处理低风险漏洞的时间框架取决于要求 12.3.1 的风险分析结果，其中包括（最低限度）识别受保护的资产、威胁以及威胁发生的可能性和/或影响。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		
规定的方法要求 **11.3.1.2** 通过经验证扫描执行内部漏洞扫描，具体如下： • 记录无法接受经验证扫描凭证的系统。 • 对于那些接受扫描凭证的系统，使用了足够的权限。 • 如果用于经验证扫描的帐户可用于交互式登录，则按照要求 8.2.2 对其进行管理。	**规定的方法测试程序** **11.3.1.2.a** 检查扫描工具配置，以核实在那些接受扫描凭证的系统中，经验证扫描是否被用于内部扫描，并具备足够的权限。 **11.3.1.2.b** 检查扫描报告结果并询问相关人员，以核实是否执行了认证扫描。 **11.3.1.2.c** 如果用于经验证扫描的帐户可用于交互式登录，则检查帐户并询问有关人员，以核实是否根据要求 8.2.2 中规定的所有元素管理了帐户。 **11.3.1.2.d** 检查文件，以核实是否确定了无法接受经验证扫描凭证的系统。	**目的** 通过经验证扫描，可以更深入地了解一个实体的漏洞情况，因为它可以检测到未经验证的扫描所不能检测的漏洞。攻击者可能会利用实体没有意识到的漏洞，因为某些漏洞只有通过经验证扫描才能检测到。 经验证扫描可以产生关于某组织的漏洞的大量额外信息。 **良好做法** 用于这些扫描的凭证应被视为极高权限。它们应该按照 PCI DSS 要求 7 和 8 进行保护和控制（除了那些关于多因素验证和应用程序和系统帐户的要求）。
定制方法目标 用于检测漏洞的自动化工具可以检测每个系统的本地漏洞，这些漏洞在远程是不可见的。		

要求和测试程序		指南
适用性说明 经验证扫描工具可以基于主机或基于网络。 足够的“权限”是指访问系统资源所需的权限，以便可以彻底执行扫描，检测已知的漏洞。 这项要求不适用于不能接受扫描凭证的系统组件。可能不接受扫描凭证的系统的示例包括一些网络和安全设备、大型机和容器。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		
规定的方法要求 **11.3.1.3** 内部漏洞扫描在任何重大变更后执行，具体如下： • 解决高风险和关键漏洞（根据要求 6.3.1 中定义的实体的漏洞风险等级）。 • 视情况重新执行扫描。 • 扫描由合格人员执行，存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。 **定制方法目标** 在网络或系统发生重大变更后，通过使用旨在检测网络内部运行的漏洞的自动化工具，对所有系统组件的安全状况进行核实。根据正式的风险评估框架，评估和纠正检测到的漏洞。	**规定的方法测试程序** **11.3.1.3.a** 检查变更控制文件和内部扫描报告，以核实是否在任何重大变更后扫描了系统组件。 **11.3.1.3.b** 询问相关人员并检查内部扫描和重新扫描报告，以核实是否在重大变更后执行了内部扫描，以及要求 6.3.1 中确定的高风险和关键漏洞是否得到解决。 **11.3.1.3.c** 询问有关人员，以核实内部扫描是否由合格的内部资源或合格的外部第三方执行，并且存在组织对测试人员的独立性。	**目的** 在任何重大变更后对环境进行扫描，确保变更已适当完成，使环境的安全性不会因为变更而受到威胁。 **良好做法** 实体应在重大变更后执行扫描（作为要求 6.5.2 规定的变更过程的一部分），并在变更被视为完成之前执行。必须扫描所有受变更影响的系统组件。

要求和测试程序		指南
适用性说明 要求 11.3.1.2 规定的经验证内部漏洞扫描无需在重大变更后执行。		
规定的方法要求 **11.3.2** 执行外部漏洞扫描，具体如下： • 至少每三个月执行一次。 • 由 PCI SSC 授权的扫描供应商（ASV）执行。 • 解决漏洞，并且满足 ASV 计划指南中关于合格扫描的要求。 • 视需要重新执行扫描，以确认漏洞是否已按照 ASV 计划指南中关于合格扫描的要求得到解决。	**规定的方法测试程序** **11.3.2.a** 检查过去 12 个月的 ASV 扫描报告，以核实最近 12 个月内是否至少每三个月进行一次外部漏洞扫描。 **11.3.2.b** 检查过去 12 个月内每次扫描和重新扫描的 ASV 扫描报告，以核实是否解决了漏洞，以及是否符合 ASV 计划指南中关于合格扫描的要求。 **11.3.2.c** 检查 ASV 扫描报告，核实扫描是否由 PCI SSC 授权的扫描供应商（ASV）执行。	**目的** 攻击者经常寻找未补丁或易受攻击的外部服务器，这些服务器可被利用来发动定向攻击。组织必须确保定期扫描这些面向外部的设备是否存在弱点，并修补或补救漏洞，从而保护实体。 由于外部网络受到威胁的风险更大，因此必须由 PCI SSC 授权的扫描供应商（ASV）至少每三个月执行一次外部漏洞扫描。 **良好做法** 虽然要求至少每三个月扫描一次，但根据网络的复杂性、变更频率以及使用的设备、软件和操作系统的类型，建议更频繁地进行扫描。 可以结合多个扫描报告，以显示扫描了所有系统，并且解决了所有适用漏洞，这是三个月的漏洞扫描周期的一部分。然而，正在解决可能需要额外文件来核实未被修复的漏洞。
定制方法目标 这项要求不适用于定制方法。		
适用性说明 对于最初的 PCI DSS 遵从性，如果评估商确认存在以下情况，则不要求在 12 个月内完成四次合格扫描：1）最近的扫描结果是合格扫描，2）实体有书面政策和程序，要求至少每三个月扫描一次，以及 3）扫描结果中指出的漏洞已在重新扫描中得到纠正。 *（下一页继续）*		

要求和测试程序		指南
然而，对于最初的 PCI DSS 评估后的后续年份，必须至少每三个月进行一次合格扫描。 ASV 扫描工具可以扫描大量的网络类型和拓扑结构。任何有关目标环境的细节（例如，负载平衡器、第三方供应商、ISP、特定配置、使用的协议、扫描干扰）都应该由 ASV 和扫描客户共同解决。 请参考 PCI SSC 网站上发布的 *ASV 计划指南*，了解扫描客户的责任、扫描准备等。		
规定的方法要求 **11.3.2.1** 外部扫描在任何重大变更后执行，具体如下： • 解决了由 CVSS 评为 4.0 或更高的漏洞。 • 视情况重新执行扫描。 • 扫描由合格人员执行，存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。 **定制方法目标** 在网络或系统发生重大变更后，通过使用旨在检测网络外部运行的漏洞的工具，对所有系统组件的安全状况进行核实。根据正式的风险评估框架，评估和纠正检测到的漏洞。	**规定的方法测试程序** **11.3.2.1.a** 检查变更控制文件和外部扫描报告，以核实是否在任何重大变更后扫描了系统组件。 **11.3.2.1.b** 询问相关人员并检查外部扫描和重新扫描报告，以核实是否在重大变更后进行了外部扫描，以及由 CVSS 评为 4.0 或更高的漏洞是否得到解决。 **11.3.2.1.c** 询问有关人员，以核实外部扫描是否由合格的内部资源或合格的外部第三方执行，并且存在组织对测试人员的独立性。	**目的** 在任何重大变更后对环境进行扫描，确保变更已适当完成，使环境的安全性不会因为变更而受到威胁。 **良好做法** 实体应将在重大变更后执行扫描的需求作为变更过程的一部分，并在变更被视为完成之前执行。必须扫描所有受变更影响的系统组件。

要求和测试程序		指南
11.4 定期执行外部和内部穿透测试，并纠正可利用的漏洞和安全弱点。		
规定的方法要求 **11.4.1** 实体定义、记录和实施穿透测试方法，包括： • 行业公认的穿透测试方法。 • 覆盖整个 CDE 周界和关键系统。 • 测试网络内部和外部。 • 测试以认证任何分段和范围缩小控制。 • 应用层穿透测试，至少识别要求 6.2.4 中列出的漏洞。 • 网络层穿透测试，包括支持网络功能的所有组件以及操作系统。 • 审核并考虑过去 12 个月内经历的威胁和漏洞。 • 评估和处理穿透测试期间发现的可利用漏洞和安全弱点所带来的风险的书面方法。 • 穿透测试结果和补救活动结果至少保留 12 个月。 **定制方法目标** 确定彻底技术测试的正式方法，这种测试试图通过合格的手动攻击者的模拟攻击方法来利用漏洞和安全弱点。	**规定的方法测试程序** **11.4.1** 检查文件并询问相关人员，以核实该实体定义、记录和实施的穿透测试方法是否包括本要求中规定的所有元素。	**目的** 攻击者花费大量时间寻找外部和内部漏洞，利用这些漏洞获得对持卡人数据的访问，然后渗漏这些数据。因此，实体需要彻底测试其网络，就像攻击者所做的那样。这种测试使实体能够识别和补救可能被利用来威胁实体的网络和数据的弱点，然后采取适当措施来保护网络和系统组件免受这种攻击。 **良好做法** 穿透测试技术将根据组织的需求和结构而有所不同，并应适合于被测试的环境—例如，模糊、注入和伪造测试可能是合适的。测试的类型、深度和复杂性将取决于具体环境和组织的需求。 **定义** 穿透测试模拟真实世界的攻击情况，旨在确定在向测试人员提供不同数量的信息的情况下，攻击者能在多大程度上穿透到一个环境中。这使得某实体能够更好地了解其潜在的风险，并制定策略来抵御攻击。穿透测试与漏洞扫描不同，因为穿透测试是一个活跃过程，通常包括利用已确定的漏洞。 仅仅扫描漏洞并不是穿透测试，如果仅仅关注于尝试利用漏洞扫描中发现的漏洞，那么穿透测试也是不够的。执行漏洞扫描可能是第一步，但它并不是穿透测试人员规划测试策略的唯一步骤。 *(下一页继续)*

要求和测试程序		指南
适用性说明 测试网络内部（或“内部穿透测试”）是指从 CDE 内部和从可信和不可信的内部网络进入 CDE 的测试。 测试网络外部（或“外部”穿透测试）是指测试可信网络的暴露外部边界，以及连接到公共网络基础设施或可访问公共网络基础设施的关键系统。		即使漏洞扫描无法检测到已知漏洞，穿透测试人员通常也会彻底了解系统来识别可能的安全漏洞。 穿透测试是一个高度手动的过程。虽然可能会使用一些自动化工具，但测试人员利用他们对系统的了解来获得进入环境的机会。通常情况下，测试人员会将几种类型的漏洞连在一起，目的是为了冲破层层防御。例如，如果测试人员找到了进入应用程序服务器的方法，则测试人员就会把被威胁的服务器作为一个点，根据该服务器所能访问的资源进行新的攻击。通过这种方式，测试人员可以模拟攻击者所使用的技术，以确定环境中的潜在弱点领域。还应考虑对安全监控和检测方法进行测试—例如，确认日志和文件完整性监控机制的有效性。 **更多信息** 更多指南，请参考*信息补充：穿透测试指南*。 行业公认的穿透测试方法包括： *开放源代码安全测试方法和手册（OSSTMM）* *开放网络应用安全项目（OWASP）穿透测试计划。*

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
11.4.2 执行内部穿透测试，具体如下： • 根据实体规定的方法执行。 • 至少每 12 个月执行一次 • 在任何重要的基础设施或应用程序升级或变更之后执行 • 由合格的内部资源或合格的外部第三方执行。 • 存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。	**11.4.2.a** 检查最近一次内部穿透测试的工作范围和结果，以核实穿透测试是否按照本要求中规定的所有元素执行。 **11.4.2.b** 询问相关人员，核实内部穿透测试是否由合格的内部资源或合格的外部第三方执行，并且存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。	内部穿透测试有两个目的。首先，就像外部穿透测试一样，它可以发现漏洞和错误配置，这些漏洞和错误配置可以被设法获得某种程度的内部网络访问的攻击者所利用，无论该攻击者是进行未授权活动的授权用户，还是设法穿透实体周边的外部攻击者。 其次，内部穿透测试还可以帮助实体发现他们的变更控制过程中的失效位置，方法是通过检测以前未知的系统。此外，它还能核实 CDE 内许多控制的运行状态。 穿透测试并不是真正的“测试”，因为穿透测试的结果并不能划分为“通过”或“失败”。 测试的最佳结果是某实体不知道的漏洞和错误配置的目录，并且穿透测试人员在攻击者发现它们之前就已经发现了它们。没有结果的穿透测试通常表明穿透测试人员的缺点，并非对该实体的安全状况的正面反映。 **良好做法** 在选择合格的资源执行穿透测试时，一些考虑因素包括： • 特定的穿透测试证书，这可能表明测试人员的技能水平和能力。 *(下一页继续)*
定制方法目标		
根据实体确定的方法，通过技术测试对内部系统防御进行核实，以应对不断变化的新攻击和威胁，并确保重大变更不会引入未知漏洞。		

要求和测试程序		指南
规定的方法要求 **11.4.3** 执行外部穿透测试，具体如下： • 根据实体规定的方法执行 • 至少每 12 个月执行一次 • 在任何重要的基础设施或应用程序升级或变更之后执行 • 由合格的内部资源或合格的外部第三方执行。 • 存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。	**规定的方法测试程序** **11.4.3.a** 检查最近一次外部穿透测试的工作范围和结果，以核实穿透测试是否按照本要求中规定的所有元素执行。 **11.4.3.b** 询问相关人员，核实外部穿透测试是否由合格的内部资源或合格的外部第三方执行，并且存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。	• 执行穿透测试的既往经验—例如，经验年限，以及既往工作的类型和范围，可以帮助确认测试人员的经验是否适合工作的需要。 **更多信息** 更多指南，请参考*信息补充：*更多指南，请参见 PCI SSC 网站上的*穿透测试指南*。
定制方法目标 根据实体确定的方法，通过技术测试对外部系统防御进行核实，以应对不断变化的新攻击和威胁，并确保重大变更不会引入未知漏洞。		
规定的方法要求 **11.4.4** 纠正穿透测试期间发现的可利用的漏洞和安全弱点，具体如下： • 根据实体对要求 6.3.1 中规定的安全问题所带来的风险评估纠正。 • 重复进行穿透测试，以核实纠正结果。	**规定的方法测试程序** **11.4.4** 检查穿透测试结果，核实是否根据本要求中规定的所有元素纠正了所指出的可利用漏洞和安全弱点。	**目的** 穿透测试的结果通常是演习中发现的漏洞的优先次序列表。测试人员通常会将一些漏洞串联起来，以威胁系统组件。补救穿透测试发现的漏洞，可显著降低相同漏洞被恶意攻击者利用的概率。

要求和测试程序		指南
定制方法目标 减轻核实系统防御时发现的漏洞和安全弱点。		使用实体自身的漏洞风险评估流程（请参见要求 6.3.1）可确保对实体构成最高风险的漏洞将更快得到补救。 **良好做法** 作为实体风险评估的一部分，实体应考虑漏洞被利用的可能性有多大，以及环境中是否存在其他控制来降低风险。 应该解决任何指向 PCI DSS 要求未得到满足的弱点。
规定的方法要求	**规定的方法测试程序**	**目的**
11.4.5 如果使用分段将 CDE 与其他网络隔离开来，则对分段控制执行穿透测试，具体如下： • 至少每 12 个月执行一次，并在分段控制/方法出现任何变更后执行 • 覆盖所有正在使用的分段控制/方法。 • 根据该实体确定的穿透测试方法。 • 确认分段控制/方法是否可操作及有效，并将 CDE 与所有范围外的系统隔离开来。 • 确认任何使用隔离来分离具有不同安全级别的系统是否有效（请参见要求 2.2.3）。 • 由合格的内部资源或合格的外部第三方执行。 • 存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。	**11.4.5.a** 检查分段控制和审核穿透测试方法，核实是否制定了穿透测试程序，以根据本要求中规定的所有元素测试所有分段方法。 **11.4.5.b** 检查最近一次穿透测试的结果，以核实穿透测试是否涵盖并解决了本要求中规定的所有元素。 **11.4.5.c** 询问相关人员，核实测试是否由合格的内部资源或合格的外部第三方执行，并且存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。	当一个实体使用分段控制将 CDE 与内部不可信的网络隔离开来时，CDE 的安全取决于分段功能。许多攻击涉及到攻击者从实体认为是隔离的网络横向进入 CDE。使用穿透测试工具和技术认证一个不可信的网络确实与 CDE 隔离开来，可以向该实体发出警报，以注意分段控制的故障或错误配置，然后可以予以纠正。 **良好做法** 可以使用主机发现和端口扫描等技术来核实范围外网段是否没有权限访问 CDE。

要求和测试程序		指南
定制方法目标 如果使用分段，通过技术测试定期核实它是否持续有效，包括在任何变更之后，将 CDE 与所有范围外系统隔离开来。		
规定的方法要求 **11.4.6** ***仅针对服务提供商的额外要求：*** 如果使用分段将 CDE 与其他网络隔离开来，则对分段控制执行穿透测试，具体如下： • 至少每六个月执行一次，并在分段控制/方法出现任何变更后执行 • 覆盖所有正在使用的分段控制/方法。 • 根据该实体确定的穿透测试方法。 • 确认分段控制/方法是否可操作及有效，并将 CDE 与所有范围外的系统隔离开来。 • 确认任何使用隔离来分离具有不同安全级别的系统是否有效（请参见要求 2.2.3）。 • 由合格的内部资源或合格的外部第三方执行。 • 存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。	**规定的方法测试程序** **11.4.6.a** ***仅针对服务提供商评估的额外测试程序：*** 检查最近一次穿透测试的结果，以核实穿透测试是否涵盖并解决了本要求中规定的所有元素。 **11.4.6.b** ***仅针对服务提供商评估的额外测试程序：*** 询问相关人员，核实测试是否由合格的内部资源或合格的外部第三方执行，并且存在组织对测试人员的独立性（不要求是 QSA 或 ASV）。	**目的** 服务提供商通常可以访问更大量的持卡人数据，或者可以提供一个输入点，利用该输入点可以威胁其他多个实体。服务提供商通常还拥有更大、更复杂的网络，这些网络会发生更频繁的变化。在服务提供商的环境中，分段控制在复杂和动态网络中失效的概率更大。 更为频繁认证分段控制可能会在攻击者试图从范围外的不可信网络横向转移到 CDE 之前发现分段故障。 **良好做法** 尽管要求规定该范围认证至少每六个月进行一次，并在重大变更后进行，但该工作应尽可能频繁地进行，以确保它能有效地将 CDE 与其他网络隔离开来。
定制方法目标 如果使用分段，通过技术测试核实它是否持续有效，包括在任何变更之后，将 CDE 与所有范围外系统隔离开来。		

要求和测试程序		指南
适用性说明 本要求仅在被评估实体是服务提供商的情况下适用。		
规定的方法要求 **11.4.7** ***仅针对****多租户服务提供商****服务提供商的测试程序：***多租户服务提供商提供商按照要求 11.4.3 和 11.4.4 支持其客户执行外部穿透测试。	**规定的方法测试程序** **11.4.7** ***仅针对多租户服务提供商的测试程序：*** 检查证据，多租户服务提供商是否按照要求 11.4.3 和 11.4.4 支持了其客户执行外部穿透测试。	**目的** 各实体需要根据 PCI DSS 执行穿透测试，以模拟攻击者行为并发现其环境中的漏洞。在共享和云环境中，多租户服务提供商可能会担心穿透测试人员的活动会影响其他客户的系统。 多租户服务提供商不能禁止穿透测试，因为这将导致其客户的系统被利用。因此，多租户服务提供商必须支持客户执行穿透测试或获取穿透测试结果的请求。
定制方法目标 多租户服务提供商支持其客户执行技术测试的需求，方法是提供访问权限，或提供证据证明已进行类似的技术测试。		

要求和测试程序		指南
适用性说明 本要求仅在被评估实体是多租户服务提供商的情况下适用。 为满足这项要求，多租户服务提供商可以选择： • 提供证据，向其客户表明已根据要求 11.4.3 和 11.4.4 对客户订购的基础设施执行了穿透测试，或 • 向其每个客户提供及时访问，以便客户能够执行他们自己的穿透测试。 提供给客户的证据可以包括经编辑的穿透测试结果，但需要包括足够的信息，以证明代表客户满足要求 11.4.3 和 11.4.4 的所有元素。 *另请参考附录 A1：针对多租户服务提供商的额外 PCI DSS 要求。* *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑*		

要求和测试程序		指南
11.5 检测并响应网络入侵和意外文件变更。		
规定的方法要求	**规定的方法测试程序**	**目的**
11.5.1 入侵检测和/或入侵防御技术用于检测和/或防御网络入侵，具体如下： • 在 CDE 周边监控所有流量。 • 在 CDE 关键点上监控所有流量。 • 向有关人员发出警报，以注意可疑威胁。 • 保持所有入侵检测和防御引擎、基线和签名的时效性。	**11.5.1.a** 检查系统配置和网络图，核实是否建立了入侵检测和/或入侵防御技术，以： • 在 CDE 周边监测所有流量。 • 在 CDE 关键点上监测所有流量。	入侵检测和/或入侵防御技术（例如 IDS/IPS）将进入网络的流量与已知的“签名”和/或数以千计的威胁类型（黑客工具、木马和其他恶意软件）的行为进行比较，然后发出警报和/或在发生时停止尝试。如果没有用于检测未经授权的活动的主动方法，对计算机资源的攻击（或滥用）可能会在很长一段时间内被忽视。在许多方面，入侵 CDE 的影响是攻击者在被检测到之前在环境中的一个时间因素。
	11.5.1.b 检查系统配置并询问负责人员，核实入侵检测和/或入侵预防技术是否向有关人员发出了注意可疑威胁的警报。	**良好做法**
定制方法目标	**11.5.1.c** 检查系统配置和供应商文件，以核实入侵检测和/或入侵防御技术的配置是否保持了所有引擎、基线和签名的时效性。	应持续监控这些技术产生的安全警报，以便能够阻止企图或实际的入侵，并限制潜在的损害。
实施各种机制，实时检测可能表明威胁行为者活动的可疑或异常的网络流量。有关人员或自动化方法会响应这些机制产生的警报，以确保系统组件不会因检测到的活动而受到威胁。		**定义** 关键位置可以包括但不限于网段之间的网络安全控制（例如，DMZ 和内部网络之间或范围内网络和范围外网络之间）以及保护较不信任的系统组件和较信任的系统组件之间的连接点。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
11.5.1.1 ***仅针对服务提供商的额外要求：***入侵检测和/或入侵防御技术可以检测、提醒/预防和解决秘密恶意软件通信渠道。	**11.5.1.1.a** ***仅针对服务提供商评估的额外测试程序：***检查文件和配置设置，以核实是否制定了并正在运行检测和警告/防止秘密恶意软件通信渠道的方法。	检测秘密恶意软件通信尝试（例如，DNS 隧道）可以帮助阻止恶意软件在网络内的横向传播和数据渗漏。当决定放置这种控制的位置时，实体应考虑网络中的关键位置，以及秘密通道的可能路线。 当恶意软件在受感染的环境中建立一个立足点时，它往往试图建立一个连接到指挥和控制（C&C）服务器的通信渠道。通过 C&C 服务器，攻击者与被威胁系统上的恶意软件进行沟通并对其进行控制，以提供恶意的有效载荷或指令，或启动数据渗漏。在许多情况下，恶意软件将通过僵尸网络与 C&C 服务器间接通信，绕过监测、阻断控制，并使这些方法无法有效地检测到秘密渠道。
定制方法目标	**11.5.1.1.b** ***仅适用于服务提供商评估的额外测试程序：***检查实体的事件响应计划（要求 12.10.1），以核实其是否要求并确定了在检测到秘密恶意软件通信渠道时的响应。	**良好做法**
建立机制，以检测和提醒/防止与指挥和控制系统的秘密通信。有关人员或通过自动化方法响应这些机制产生的警报，以确保此类通信被阻止。	**11.5.1.1.c** ***仅针对服务提供商评估的额外测试程序：***询问负责人员并观察流程，以核实人员是否保持对秘密恶意软件通信和控制技术的了解，并了解在怀疑有恶意软件时如何应对。	有助于检测和解决恶意软件通信渠道的方法包括实时端点扫描、出口流量过滤、“允许”列表、数据丢失防御工具和网络安全监控工具，例如 IDS/IPS。此外，DNS 查询和响应是网络防御者用来支持事件响应以及入侵侦测的一个关键数据源。当收集这些交易进行处理和分析时，它们可以实现一些有价值的安全分析方案。 组织保持对恶意软件操作模式的最新了解非常重要，因为缓解这些问题有助于检测和限制环境中恶意软件的影响。
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求 **11.5.2** 部署变更检测机制（例如，文件完整性监控工具），具体如下： • 向有关人员发出警报，注意关键文件是否出现未经授权的修改（包括更改、增加和删除）。 • 每周至少执行一次关键文件对比。 **定制方法目标** 未经授权的人员不得在不产生警报的情况下修改关键文件。 **适用性说明** 对于变更检测的目的，关键文件通常是那些不定期变更的文件，但其修改可能表明系统遭到威胁或有遭到威胁的风险。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关键文件。实体（即商户或服务提供商）必须评估和确定其他关键文件，例如定制应用程序的文件。	**规定的方法测试程序** **11.5.2.a** 检查系统设置、受监控的文件和监控活动的结果，以核实是否使用了变更检测机制。 **11.5.2.b** 检查变更检测机制的设置，以核实是否根据本要求中规定的所有元素配置了该配置。	**目的** 对关键系统、配置或内容文件的变更可能表明攻击者已进入组织系统。这种变更可以使攻击者采取更多的恶意行动，访问持卡人数据，和/或在不被检测或记录的情况下执行活动。 变更检测机制将检测和评估对关键文件的此类变更，并产生警报，可以按照规定的程序作出响应，以便工作人员可以采取适当的行动。 如果没有正确的实施和对变更检测解决方案的输出进行监控，恶意者可以添加、删除或改变配置文件内容、操作系统程序或应用程序执行表。未经授权的变更，如果未检测到，可能会使现有的安全控制失效和/或导致持卡人数据被盗，不会对正常处理产生明显影响。 **良好做法** 应被监控的文件类型的示例包括，但不限于： • 系统执行表。 • 应用程序执行表。 • 配置和参数文件。 • 集中存储、记录或存档的检查日志。 • 实体确定的其他关键文件（例如，通过风险评估或其他方法）。 **示例** 变更检测解决方案，例如检查关键文件是否出现变更、增加和删除并在检测到这种变更时发出通知的文件完整性监控（FIM）工具

要求和测试程序		指南
11.6 检测并响应支付页面上未经授权的变更。		
规定的方法要求	**规定的方法测试程序**	**目的**
11.6.1 部署变更和篡改检测机制，具体如下： • 向有关人员发出警报，注意消费者浏览器收到的 HTTP 头和支付页面的内容是否出现未经授权的修改（包括威胁指标、变更、添加和删除）。 • 配置该机制，以评估收到的 HTTP 头和支付页面。 • 执行该机制的功能，具体如下： – 至少每七天执行一次 **或** – 定期执行（按照实体的目标风险分析中定义的频率，即根据要求 12.3.1 中规定的所有元素执行）。	**11.6.1.a** 检查系统设置、受监控的支付页面以及监控活动的结果，以核实是否使用了变更和篡改检测机制。 **11.6.1.b** 检查配置设置，以核实是否根据本要求中规定的所有元素配置了该机制。 **11.6.1.c** 如果根据实体定义的频率执行机制功能，则检查实体确定频率的目标风险分析，以核实是否根据要求 12.3.1 规定的所有元素执行了风险分析。 **11.6.1.d** 检查配置设置并询问相关人员，以核实机制功能的执行情况，包括： • 至少每七天执行一次 **或** • 是否根据实体为该要求执行的目标风险分析中定义的频率。	现在，许多网页都依赖于从多个互联网位置组装对象，包括活动内容（主要是 JavaScript）。此外，使用内容管理和标签管理系统来确定许多网页的内容，而使用传统的变更检测机制可能无法对其进行监控。 因此，检测变更或恶意活动指标的唯一位置是在消费者的浏览器中，因为在这里构建了页面并解释了所有 JavaScript。 通过比较消费者浏览器收到的 HTTP 头的当前版本和支付页面的活动内容与较早或已知版本，有可能检测到可能表明有盗取攻击的未经授权变更。 此外，通过寻找已知的威胁指标和脚本元素或典型的盗取者行为，可以提出可疑警报。
定制方法目标		**示例**
在没有产生及时警报的情况下，不能将电子商务撇账代码或技术添加到消费者浏览器收到的支付页面上。在没有产生及时警报的情况下，不能移除支付页面中的反盗用措施。		检测和报告支付页面的标题和内容变更的机制包括但不限于： • 可以使用 *report-to* 或 *report-uri* CSP 指令向实体报告违反内容安全策略（CSP）的行为。 *（下一页继续）*

要求和测试程序		指南
适用性说明 这项要求的目的并非让实体在其消费者的系统或浏览器中安装软件，而是让实体使用诸如指导栏中的示例所描述的技术来防止和检测意外的脚本活动。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		• 对 CSP 本身的变更可以表明篡改 • 由请求和分析收到的网页的系统进行外部监控（也称为合成用户监控）可以检测到支付页面中 JavaScript 的变更，并向人员发出警报 • 嵌入防篡改、防篡改检测脚本到支付页面中，可以在检测到恶意脚本行为时发出警报并进行阻止。 • 反向代理和内容交付网络可以检测到脚本的变更，并向人员发出警报 通常情况下，这些机制是基于订阅或云的，但也可以基于定制和订制的解决方案。

维护信息安全政策

要求 12:　　使用组织政策和计划支持信息安全

章节
12.1 管理和提供方向以保护实体信息资产的综合信息安全政策是已知的和最新的。
12.2 确定并实施终端用户技术的可接受使用政策。
12.3 正式识别、评估和管理持卡人数据环境面临的风险。
12.4 管理 PCI DSS 遵从性。
12.5 记录和认证 PCI DSS 范围。
12.6 安全意识教育是一项持续的活动。
12.7 筛选相关人员，以减少内部威胁的风险。
12.8 管理与第三方服务供应商（TPSP）关系相关的信息资产的风险。
12.9 第三方服务提供商（TPSP）支持其客户的 PCI DSS 遵从性。
12.10 立即响应可能影响 CDE 的可疑和确认的安全事件。

概述

组织的整体信息安全政策为整个实体定下了基调，并告知人员对他们有何期望。所有人员都应了解持卡人数据的敏感性以及他们保护数据的责任。

在要求 12 中，“人员”是指负有责任保护帐户数据安全或可能影响帐户数据安全的全职和兼职雇员、临时雇员、承包商和顾问。

请参阅附录 G 了解 PCI DSS 术语的定义。

要求和测试程序		指南
12.1 管理和提供方向以保护实体信息资产的综合信息安全政策是已知的和最新的。		
定义的方法要求 **12.1.1** 整体信息安全政策是： • 建立。 • 公布。 • 已维护。 • 向所有相关人员以及相关供应商和业务伙伴传播。 **定制方法目标** 确定、采用并让所有人员知晓信息安全的战略目标和原则。	**规定的方法测试程序** **12.1.1** 检查信息安全政策并询问相关人员，以核实是否根据本要求中规定的所有元素管理了整体信息安全政策。	**目的** 组织的整体信息安全政策与所有其他定义保护持卡人数据安全的政策和程序相联系并受其管理。 信息安全政策传达了管理层关于保护其最宝贵的资产（包括持卡人数据）的目的和目标。 如果没有信息安全政策，个人将对组织内所需的控制做出自己的价值决定，这可能导致组织既不能履行其法律、法规和合同义务，也无法以一致的方式充分保护其资产。 为了确保政策得到实施，组织内所有相关人员以及相关的第三方、供应商和业务伙伴都必须了解组织的信息安全政策以及他们保护信息资产安全的责任。 **良好做法** 组织的安全政策确定了目的、范围、责任和信息，明确界定了组织在信息安全方面的立场。 整体信息安全政策有别于针对特定技术或安全学科的个别安全政策。该政策规定了整个组织的指令，而个别安全政策则是对整体安全政策的调整和支持，并传达技术或安全学科的具体目标。 *(下一页继续)*

要求和测试程序		指南
		组织内所有相关人员以及相关的第三方、供应商和业务伙伴都必须了解组织的信息安全政策以及他们保护信息资产安全的责任。 **定义** 本要求中的"相关"是指将信息安全政策传播给那些在公司内部或由于供应商或第三方提供的服务/功能而适用于政策中部分或全部主题的人。
规定的方法要求 **12.1.2** 信息安全政策： • 每 12 个月至少审核一次。 • 视需要进行更新，以反映业务目标或环境风险的变化。 **定制方法目标** 信息安全政策继续反映组织的战略目标和原则。	**规定的方法测试程序** **12.1.2** 检查信息安全政策并询问负责人员，以核实是否根据本要求中规定的所有元素管理了这项政策。	**目的** 安全威胁和相关保护方法发展迅速。如果不更新信息安全政策以反映相关的变化，就可能无法解决抵御这些威胁的新措施。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.1.3 安全政策明确界定了所有人员的信息安全角色和责任，所有人员都知道并承认其信息安全责任。	**12.1.3.a** 检查信息安全政策，以核实它们是否明确界定了所有人员的信息安全角色和责任。	如果没有明确定义的安全角色和责任分配，可能会出现滥用组织的信息资产或与信息安全人员不一致的互动，导致技术的不安全实施或使用过时或不安全的技术。
	12.1.3.b 询问不同角色的人员，以核实他们是否了解他们的信息安全责任。	
	12.1.3.c 检查书面证据，以核实人员是否承认他们的信息安全责任。	
定制方法目标		
人员了解他们在保护实体的持卡人数据方面的作用。		
规定的方法要求	**规定的方法测试程序**	**目的**
12.1.4 将信息安全的责任正式分配给首席信息安全官或执行管理层中其他具有信息安全知识的成员。	**12.1.4** 检查信息安全政策，以核实是否将信息安全的责任正式分配给首席信息安全官或执行管理层中其他具有信息安全知识的成员。	为了确保具备充分权限和责任的人积极管理和支持组织的信息安全计划，需要在组织内的执行层面上分配信息安全的责任和职责。 该角色的常见执行管理头衔包括首席信息安全官（CISO）和首席安全官（CSO–为了满足该要求，CSO 的角色必须负责信息安全）。这些职位通常处于管理层的最高级别，是首席执行官级别或 C 级的一部分，通常向首席执行官或董事会报告。 **良好做法** 实体还应该考虑这些关键人员的过渡和/或继任计划，以避免关键安全活动的潜在漏洞。
定制方法目标		
执行管理层的一名指定成员负责信息安全。		

要求和测试程序		指南
12.2 确定并实施终端用户技术的可接受使用政策。		
规定的方法要求 **12.2.1** 记录并实施终端用户技术的可接受使用政策，包括： • 由授权方明确批准。 • 可接受使用技术。 • 经公司授权供员工使用的产品清单，包括硬件和软件。 **定制方法目标** 确定并管理终端用户技术的使用，以确保授权使用。 **适用性说明** 预计可接受使用政策的终端用户技术的例子，包括但不限于远程访问和无线技术、笔记本电脑、平板电脑、移动电话和可移动电子媒体、电子邮件使用和互联网使用。	**规定的方法测试程序** **12.2.1** 检查最终用户技术的可接受使用政策，并询问负责人员，以核实是否根据本要求规定的所有元素记录并实施了流程。	**目的** 最终用户技术是一项重要的投资，如果管理不善，可能会给组织带来巨大的风险。可接受使用政策概述了人员在使用组织的信息技术时的预期行为，并反映了组织的风险容忍度。 这些政策指导人员可以和不可以使用公司的设备，指导人员正确使用公司的互联网和电子邮件资源。这些政策可以在法律上保护组织，并允许其在违反政策的情况下采取行动。 **良好做法** 重要的是，技术控制应支持使用政策，以管理政策的执行情况。 以简单的“该做事项”和“不该做事项”要求构建政策，并与目的相联系，有助于消除含糊其词的地方，并为工作人员提供要求的背景信息。

要求和测试程序		指南
12.3 正式识别、评估和管理持卡人数据环境面临的风险。		
规定的方法要求 **12.3.1** 目标风险分析支持那些提供灵活的执行频率（例如，要求定期执行）的每个书面 PCI DSS 要求，包括： • 识别被保护的资产。 • 识别该要求所要保护的威胁。 • 识别导致威胁发生的可能性和/或影响的因素。 • 由此产生的分析，确定必须多频繁地执行该要求以最大限度地减少威胁发生的可能性，并包括这方面的理由。 • 至少每 12 个月对每个目标风险分析进行一次审核，以确定结果是否仍然有效或是否需要更新风险分析。 • 根据年度审核决定，在需要时执行更新的风险分析。 **定制方法目标** 保持对 CDE 面临的风险的最新了解并对其进行评估。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **12.3.1** 检查书面政策和程序，核实是否制定了相应流程，以执行每个 PCI DSS 要求的目标风险分析，从而为执行要求的频率提供灵活性，并且该流程包括本要求中规定的所有元素。	**目的** 一些 PCI DSS 要求允许实体根据环境的风险来确定执行活动的频率。根据一种可确保政策和程序的有效性和一致性的方法执行这种风险分析。 这种目标风险分析（相对于传统的企业风险评估）侧重于那些允许实体灵活执行特定控制的频率的 PCI DSS 要求。对于这种风险分析，实体仔细评估提供这种灵活性的每个 PCI DSS 要求，并确定支持实体充分安全的频率，以及实体愿意接受的风险水平。 风险分析确定了特定资产，例如系统组件和数据—例如，日志文件或凭证—该要求旨在保护，以及该要求保护资产免受的威胁或结果—例如，恶意软件、未被发现的入侵者或凭证的滥用。可能导致可能性或影响的因素的示例包括任何可能增加资产对威胁的脆弱程度的因素—例如，暴露在不信任的网络中，环境的复杂性，或高的人员流动，以及系统组件的关键性，或被保护数据的量和敏感性。 至少每 12 个月审核一次这些目标风险分析的结果，并在发生可能影响环境风险的变更时，组织可以确保风险分析结果与组织变更和不断发展的威胁、趋势和技术保持一致，并确保所选频率仍然能够充分应对实体的风险。 *（下一页继续）*

要求和测试程序		指南
		良好做法 企业风险评估是一种使实体能够识别威胁和相关漏洞的时间点活动，建议但不要求实体确定和理解有可能对其业务产生负面影响的更广泛和新出现的威胁。可以建立这种企业风险评估作为总体风险管理计划的一部分，该计划被用作对组织整体信息安全政策的年度审核的投入（请参见要求 12.1.1）。 用于企业风险评估的风险评估方法的示例包括但不限于 ISO *27005* 和 NIST *SP 800-30*。
规定的方法要求 **12.3.2** 对实体使用定制方法满足的每项 PCI DSS 要求执行了目标风险分析，包括： • 详述附录 D 中规定的每个元素的书面证据：定制方法（至少包括控制矩阵和风险分析）。 • 高级管理层批准书面证据。 • 至少每 12 个月执行一次目标风险分析。	**规定的方法测试程序** **12.3.2** 检查实体使用定制方法满足的每项 PCI DSS 要求的书面目标风险分析，以核实是否有每项要求的文件，并符合本要求中规定的所有元素。	**目的** 遵循可重复和稳健的方法进行的风险分析使实体能够达到定制方法目标。 **定义** 满足 PCI DSS 要求的定制方法允许实体确定用于满足特定要求的定制方法目标的控制措施，其方式并不严格遵循定义的要求。这些控制措施预计至少要达到或超过所定义的要求所提供的安全性，并要求使用定制方法的实体提供大量的文件。 **更多信息** 关于如何记录定制方法所需证据的指示，请参阅附录 D：定制方法。 如需实体可用于记录其定制控制的模板，请参见附录 E 支持定制方法的样本模板。请注意，虽然可以选择是否使用这些模板，但必须记录每个模板中规定的信息并提供给每个实体的评估商。
定制方法目标 这项要求是定制方法的一部分，并且使用定制方法的人员必须满足。		
适用性说明 这项要求只适用于使用定制方法的实体。		

要求和测试程序		指南
规定的方法要求 **12.3.3** 至少每 12 个月记录和审核一次正在使用的加密套件和协议，至少包括以下内容： • 所有正在使用的加密套件和协议的最新清单，包括目的和使用地点。 • 积极监控有关所有正在使用的加密套件和协议的持续维持能力的行业趋势。 • 响应加密漏洞的预期变化的书面战略。 **定制方法目标** 实体能够快速响应加密协议或算法中的任何漏洞，而这些漏洞会影响到对持卡人数据的保护。 **适用性说明** 该要求适用于用于满足 PCI DSS 要求的所有加密套件和协议。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **12.3.3** 检查正在使用的加密套件和协议的文件，并询问相关人员，以核实文件和审核是否符合本要求中规定的所有元素。	**目的** 协议和加密强度可能会迅速变化，或因发现漏洞或设计缺陷而被淘汰。为了支持当前和未来的数据安全需求，实体需要知道使用加密技术的位置，并了解他们如何能够快速响应影响其加密实作强度的变化。 **良好做法** 加密敏捷性对于确保原始加密方法或加密原语的替代方案至关重要，并计划在不对系统基础设施进行重大改变的情况下升级到替代方案。例如，如果该实体知道协议或算法何时会被标准机构淘汰，它就可以在淘汰对业务产生影响之前制定主动的升级计划。 **定义** “加密敏捷性”是指监控和管理部署在组织内的加密和相关验证技术的能力。 **更多信息** *参考 NIST SP 800-131a，过渡使用加密算法和密钥长度。*

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.3.4 至少每 12 个月对所使用的硬件和软件技术审核一次，至少包括以下方面： • 分析这些技术是否能继续及时从供应商那里获得安全修复。 • 分析这些技术是否继续支持（并且不妨碍）实体的 PCI DSS 遵从性。 • 记录与技术相关的任何行业公告或趋势，例如，当供应商已宣布某项技术的“终结”计划的时候。 • 记录经高级管理层批准的计划，以补救过时的技术，包括那些供应商已宣布“终结”计划的技术。	**12.3.4** 检查正在使用的硬件和软件技术的审核文件，并询问相关人员，以核实审核是否符合本要求中规定的所有元素。	硬件和软件技术不断发展，组织需要了解他们所使用技术出现的变化，以及这些技术所面临的不断变化的威胁，以确保他们能够准备并管理硬件和软件中的漏洞，因为供应商或开发商不会补救这些漏洞。 **良好做法** 组织应审核固件版本，以确保它们保持最新并得到供应商的支持。各组织还需要了解技术供应商对其产品或流程所做的改变，以了解这种改变会如何影响到组织对该技术的使用。 对影响 PCI DSS 控制的技术进行定期审核，可以帮助采购、使用和部署策略，并确保依赖这些技术的控制发挥作用。这些审核包括但不限于审核不再受供应商支持的技术和/或不再满足组织的安全需求的技术。
定制方法目标 该实体的硬件和软件技术保持最新，并得到供应商的支持。定期审核删除或替换所有不支持的系统组件的计划。		
适用性说明 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
12.4 管理 PCI DSS 遵从性。		
规定的方法要求	**规定的方法测试程序**	**目的**
12.4.1 ***仅针对服务供应商的额外要求：*** 执行管理层确立了责任，以保护持卡人数据和 PCI DSS 遵从性计划，包括： • 对维护 PCI DSS 遵从性的总体责任。 • 确定 PCI DSS 遵从性计划的章程，并向执行管理层传达。	**12.4.1** ***仅针对服务提供商评估的额外测试程序：*** 检查文件，以核实执行管理层是否按照本要求中规定的所有元素，确立了保护持卡人数据和 PCI DSS 遵从性计划的责任。	执行管理层分配 PCI DSS 遵从性责任，确保行政级别了解 PCI DSS 遵从性计划，并允许有机会提出适当问题，以确定计划的有效性并影响战略重点。
定制方法目标		
执行人员对持卡人数据的安全负责并承担相应责任。		
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。执行管理层可能包括 C 级职位、董事会或同等职位。具体头衔将取决于特定的组织结构。 可能将 PCI DSS 遵从性计划的责任分配给组织内的个人角色和/或业务单位。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.4.2 ***仅针对服务供应商的额外要求：*** 至少每三个月执行一次审核，以确认人员是否按照所有安全政策和操作程序执行任务。审核由非负责执行特定任务的人员执行，包括但不限于以下任务 • 每日日志审核。 • 网络安全控制的配置审核。 • 在新系统中应用配置标准。 • 响应安全警报。 • 变更管理流程。	**12.4.2.a** ***仅适用于服务提供商评估的额外测试程序：*** 检查政策和程序，核实是否制定了用于执行审核的相应程序，以确认相关人员是否按照所有安全政策和所有操作程序执行任务，包括但不限于本要求中规定的任务。	定期确认安全政策和程序是否得到遵守，可以保证预期的控制措施发挥作用，并按预期工作。这项要求与其他指定要执行的任务的要求不同。这些审查的目的不是为了重新执行其他 PCI DSS 要求，而是为了确认安全活动正在持续进行。
定制方法目标	**12.4.2.b** ***仅适用于服务提供商评估的额外测试程序：*** 询问负责人员并检查审核记录，以核实审核的执行情况，包括： • 至少每三个月执行一次。 • 审核是否由非负责执行特定任务的人员执行。	**良好做法**
通过手动检查记录，定期验证关键 PCI DSS 控制的运行有效性。		这些审核也可用于核实适当证据是否得到维护—例如，检查日志、漏洞扫描报告、网络安全控制规则集的审核—协助实体准备下一次 PCI DSS 评估。
适用性说明		**示例**
本要求仅在被评估实体是服务提供商的情况下适用。		以要求 1.2.7 为例，通过至少每三个月确认一次是否以规定的频率审核了网络安全控制配置来满足要求 12.4.2。另一方面，通过审核要求中规定的所述配置来满足要求 1.2.7。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.4.2.1 ***仅适用于服务提供商的额外要求：*** 记录根据要求 12.4.2 执行的审核，以包括： • 审核的结果。 • 任何对被发现未按要求 12.4.2 执行的任务所采取的书面补救措施。 • 由受托负责 PCI DSS 遵从性计划的人员审核和签收结果。	**12.4.2.1** ***仅适用于服务提供商评估的额外测试程序：*** 检查根据 PCI DSS 要求 12.4.2 执行的审核所涉文件，以核实该文件是否包括本要求中规定的所有元素。	这些独立检查旨在确认安全活动是否持续执行。这些审核也可用于核实适当证据是否得到维护—例如，检查日志、漏洞扫描报告、网络安全控制规则集的审核—协助实体准备下一次 PCI DSS 评估。
定制方法目标		
管理层评估运行有效性审核的结果；实施适当的补救活动。		
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。		

要求和测试程序		指南
12.5 记录并认证 PCI DSS 范围。		
规定的方法要求 **12.5.1** 备存和更新 PCI DSS 范围内的系统组件清单，包括功能/用途描述。 **定制方法目标** 确定并了解 PCI DSS 范围内的所有系统组件。	**规定的方法测试程序** **12.5.1.a** 检查清单，以核实它是否包括所有范围内的系统组件，以及每个组件的功能/用途描述。 **12.5.1.b** 询问相关人员，以核实清单是否保持最新状态。	**目的** 备存所有系统组件的最新清单，将使组织能够规定其环境的范围，并准确、有效地实施 PCI DSS 要求。如果没有清单，可能会忽略一些系统组件，并无意中被排除在组织的配置标准之外。 **良好做法** 如果某实体保持所有资产的清单，则应该可以在其他资产中清楚地识别那些在 PCI DSS 范围内的系统组件。 清单应包括可能被实例化的容器或图像。 分配一个所有者给清单，有助于确保清单保持时效性。 **示例** 备存清单的方法包括使用数据库、一系列文件或清单管理工具。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.5.2 实体至少每 12 个月一次并在范围内环境发生重大变动时记录并确认 PCI DSS 范围。范围界定认证至少包括： • 确定各个支付阶段（例如，授权、捕获、结算、拒付和退款）和认可渠道（例如，实体信用卡、虚拟信用卡和电子商务）的所有数据流。 • 根据要求 1.2.4 更新所有数据流程图。 • 确定所有储存、处理和传输帐户数据的位置，包括但不限于：1）当前确定的非 CDE 内的任何位置，2）处理 CHD 的应用程序，3）系统和网络之间的传输，以及 4）文件备份。 • 识别 CDE 中的、连接到 CDE 的或可能影响 CDE 安全的所有系统组件。 • 识别所有正在使用的分段控制和分割 CDE 的所在环境，包括环境不在范围内的理由。 • 识别所有来自第三方实体的、可以访问 CDE 的连接。 • 确认所有已识别的数据流、帐户数据、系统组件、分段控制以及来自第三方实体的、可以访问 CDE 的连接是否包括在范围内。	**12.5.2.a** 检查范围审核的书面结果并询问相关人员，以核实审核的执行情况，包括： • 审核是否至少每 12 月进行一次。 • 审核是否在范围内环境发生重大变动后进行。 **12.5.2.b** 检查由实体执行的范围审核的书面结果，以核实 PCI DSS 范围界定确认活动包括本要求中规定的所有元素。	经常认证 PCI DSS 范围有助于确保 PCI DSS 范围保持最新状态，并与不断变化的业务目标保持一致，从而确保安全控制能够保护所有合适的系统组件。 **良好做法** 准确范围界定包括严格评估 CDE 和所有连接的系统组件，以确定 PCI DSS 要求的必要覆盖范围。范围界定活动，包括仔细分析和持续监控，有助于确保对范围内系统的适当保护。在记录帐户数据位置时，该实体可以考虑创建一个包括以下信息的表格或电子表格： • 数据存储（数据库、文件、云端等），包括数据存储的目的和保留期、 • 存储的 CHD 元素（PAN、到期日、持卡人姓名和/或完成授权前的任何 SAD 元素）、 • 保持数据安全的方法（加密类型和强度、散列算法和强度、截词、令牌化）、 • 记录数据存储访问情况的方式，包括正在使用的记录机制的描述（企业解决方案、应用程序级别、操作系统级别等）。 *（下一页继续）*

要求和测试程序		指南
定制方法目标 通过综合分析和适当的技术措施，定期并在发生重大变动后核实 PCI DSS 的范围。 **适用性说明** PCI DSS 范围年度确认是接受评估的实体预计执行的活动，它与实体的评估商在年度评估期间执行的范围界定确认不同，也不打算被其取代。		除了内部系统和网络之外，还需要识别来自第三方实体的所有连接—例如，商业伙伴、提供远程支持服务的实体以及其他服务提供商—以确定纳入 PCI DSS 范围的情况。确定范围内连接后，便可实施适用的 PCI DSS 控制，以减轻第三方连接被用于威胁实体的 CDE 的风险。 可以使用数据发现工具或方法，以促进对 PAN 所有来源和位置的识别，并寻找留在当前确定的非 CDE 内的系统和网络上或在确定的 CDE 内意外位置的 PAN—例如，在错误日志或内存转储文件中。这种方法可以帮助确保检测到之前未知的 PAN 位置，并确保 PAN 的消除或适当保护。 **更多信息** 有关其他指导，请参阅*信息补充：PCI DSS 范围界定和网络分段指南*。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.5.2.1 ***仅适用于服务提供商的额外要求：***实体至少每六个月一次并在范围内环境发生重大变动时记录并确认 PCI DSS 范围。范围界定认证至少包括要求 12.5.2 中规定的所有元素。	**12.5.2.1.a** ***仅适用于服务提供商评估的额外测试程序：***检查范围审核的书面结果并询问相关人员，以核实审核按照要求 12.5.2 的执行情况，包括： • 审核是否至少每六个月进行一次。 • 审核是否在发生重大变化之后进行。	与商户相比，服务提供商通常可以访问更大量的持卡人数据，或者可以提供一个输入点，利用该输入点可以威胁其他多个实体。服务提供商通常还拥有更大、更复杂的网络，这些网络会发生更频繁的变化。在服务提供商的环境中，范围变更在复杂和动态的网络中被忽略的概率更大。 更频繁地认证 PCI DSS 范围，有可能会在攻击者利用这种被忽略的变化之前发现它们。
定制方法目标	**12.5.2.1.b** ***仅适用于服务提供商评估的额外测试程序：***。检查范围审核的书面结果，以核实范围界定认证包括要求 12.5.2 中规定的所有元素。	
通过综合分析和适当的技术措施，核实 PCI DSS 范围的准确性是否持续准确。		
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。*本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.5.3 ***仅适用于服务供应商的额外要求：***组织结构的重大变动促成对 PCI DSS 范围和控制适用性的影响的书面（内部）审核，审核结果将会通报给执行管理层。	**12.5.3.a** ***仅适用于服务提供商评估的额外测试程序：***检查政策和程序，以核实是否制定了相应流程，使得组织结构的重大变动促成对 PCI DSS 范围和控制适用性的影响的书面审核。	组织的结构和管理确定了有效和安全操作的要求和协议。这种结构的变更可能会对现有的控制和框架产生负面影响，因为必须重新分配或移除曾经支持 PCI DSS 控制的资源，或继承可能没有既定控制的新职责。因此，在对组织的结构和管理进行变更时，必须重新审视 PCI DSS 的范围和控制措施，以确保控制措施到位并发挥作用。
定制方法目标	**12.5.3.b** ***仅适用于服务提供商评估的额外测试程序：***检查文件（例如，会议记录）并询问负责人员，以核实组织结构的重大变动是否促成了包括本要求中规定的所有元素的书面审核，审核结果是否通报给执行管理层。	**示例**
在组织结构发生重大变动后确认 PCI DSS 范围。		组织结构变动包括但不限于公司合并或收购，以及负责安全控制的人员的重大变动或重新分配。
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
12.6 安全意识教育是一项持续的活动。		
规定的方法要求 **12.6.1** 实施正式的安全意识计划，使所有人员了解该实体的信息安全政策和程序，以及他们在保护持卡人数据方面扮演什么角色。 **定制方法目标** 人员了解威胁情况、他们在操作相关安全控制方面的责任，并且在需要时能获得援助和指导。	**规定的方法测试程序** **12.6.1** 检查安全意识计划，以核实它是否向所有人员提供了关于该实体的信息安全政策和程序以及人员在保护持卡人数据方面扮演什么角色的相关信息。	**目的** 如果人员没有接受过有关其公司的信息安全政策和程序以及他们自己的安全责任的培训，已实施的安全保障措施和程序可能会因无意的错误或有意的行动而变得无效。
规定的方法要求 **12.6.2** 安全意识计划： • 每 12 个月至少审核一次，并且 • 视情况进行更新，以解决任何可能影响实体的 CDE 安全的新威胁和漏洞，或提供给相关人员的关于他们在保护持卡人数据方面扮演什么角色的信息。 **定制方法目标** 定期审核和更新安全意识材料的内容。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **12.6.2** 检查安全意识计划的内容、审核的证据，并询问相关人员，以核实安全意识计划是否符合本要求中规定的所有元素。	**目的** 威胁环境和实体的防御措施并非处于静态。因此，必须视情况经常更新安全意识计划材料，以确保人员接受的教育为最新，并代表当前的威胁环境。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.6.3 人员接受安全意识培训，具体情况如下： • 在受雇时进行培训，之后至少每 12 个月进行一次。 • 采用多种沟通方式。 • 人员至少每 12 个月确认一次，他们已阅读并理解信息安全政策和程序。	**12.6.3.a** 检查安全意识计划记录，以核实相关人员是否在受雇时参加安全意识培训，之后至少每 12 个月参加一次。	培训人员确保他们收到有关信息安全重要性的信息，并了解他们在保护组织方面扮演什么角色。 要求相关人员作出确认，有助于确保他们已阅读和理解安全政策和程序，并且他们已做出并将继续承诺遵守这些政策。
	12.6.3.b 检查安全意识计划材料，以核实该计划是否包括传达意识和教育人员的多种方法。	**良好做法** 各实体可将新员工培训纳入到人力资源部门入职流程的一部分。培训应概述与安全有关的“该做事项”和“不该做事项”。 定期的复习培训可加强可能被遗忘或绕过的关键安全流程和程序。 实体应考虑在人员从不影响帐户数据安全的角色转到可能影响帐户数据安全的角色时要求进行安全意识培训。 方法和培训内容可能会有所不同，具体取决于人员角色。
	12.6.3.c 询问相关人员以核实他们是否已完成意识培训，并了解他们在保护持卡人数据方面扮演什么角色。	**示例** 可用于提供安全意识和教育的不同方法包括海报、信件、基于网络的培训、面对面培训、团队会议和激励措施。 可以通过书面或电子方式记录相关人员作出的确认。
定制方法目标	**12.6.3.d** 检查安全意识计划材料和相关人员作出的确认，以核实人员是否至少每 12 个月确认一次，他们已阅读并理解信息安全政策和程序。	
人员持续了解威胁情况、他们在操作相关安全控制方面的责任，并且在需要时能获得援助和指导。		

要求和测试程序		指南
规定的方法要求 **12.6.3.1** 安全意识培训包括对可能影响 CDE 安全的威胁和漏洞的认识，包括但不限于： • 网络钓鱼和相关攻击。 • 社会工程。 **定制方法目标** 相关人员了解他们自己的人性弱点，以及威胁行动者将如何试图利用这些弱点。相关人员在需要时能够获得援助和指导。 **适用性说明** 关于检测和保护用户免受网络钓鱼攻击的技术和自动控制之间的区别，以及为用户提供有关网络钓鱼和社会工程的安全意识培训的要求，请参见要求 5.4.1。这是两个独立的、不同的要求，通过实施另一项要求的相应控制，不能满足其中一项的要求。 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **12.6.3.1** 检查安全意识培训的内容，以核实它是否包括本要求中规定的所有元素。	**目的** 教育相关人员如何检测、应对和报告潜在的网络钓鱼和相关攻击以及社会工程企图，这对于最大限度地减少成功攻击的概率至关重要。 **良好做法** 一个有效的安全意识计划应该包括钓鱼邮件的例子和定期测试，以确定报告此类攻击的人员的普遍性。实体可以考虑为该主题提供的培训材料包括： • 如何识别网络钓鱼和其他社会工程攻击。 • 如何应对可疑的网络钓鱼和社会工程。 • 何地以及如何报告可疑的网络钓鱼和社会工程活动。 重视报告，允许组织能够奖励积极的行为，优化技术防御（请参见要求 5.4.1），并立即采取行动，从收件箱中删除规避技术防御的类似网络钓鱼邮件。

要求和测试程序		指南
规定的方法要求 **12.6.3.2** 安全意识培训包括根据要求 12.2.1 对可接受使用终端用户技术的认识。 **定制方法目标** 人员了解他们在最终用户技术的安全和操作方面的职责，并且在需要时能获得援助和指导。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **12.6.3.2** 检查安全意识培训内容，以核实其是否包括根据要求 12.2.1 对可接受使用终端用户技术的认识。	**目的** 通过将可接受使用政策的要点纳入常规培训和相关背景，人员将了解他们的责任以及这些责任如何影响组织的系统安全。

要求和测试程序		指南
12.7 筛选相关人员，以减少内部威胁的风险。		
规定的方法要求 **12.7.1** 在当地法律的约束下，聘用前对拥有权限访问 CDE 的人员进行筛选，以尽量减少来自内部来源的攻击风险。 **定制方法目标** 了解并管理与允许新员工访问 CDE 有关的风险。 **适用性说明** 对于那些可能被雇用担任商店收银员等职位的人员，他们在促进交易时一次只能访问一个卡号，这项要求只是一项建议。	**规定的方法测试程序** **12.7.1** 询问负责的人力资源部门管理层，以核实是否在当地法律的约束下，聘用前对拥有权限访问 CDE 的人员进行筛选。	**目的** 在雇用预计将被授予权限访问 CDE 的潜在人员之前，执行彻底筛选，提供实体所需信息，以便就他们雇用、将拥有权限访问 CDE 的人员作出明智的风险决策。 筛选潜在人员的其他好处包括帮助确保工作场所的安全并确认潜在雇员在其简历中提供的信息。 **良好做法** 各实体应考虑在现有人员从没有权限访问 CDE 的职位转到拥有权限访问 CDE 的职位时对其进行筛选。 为有效起见，筛选的程度应适合该职位。例如，相对于责任和访问权限较小的职位，需要承担更大责任的职位或拥有管理权限访问关键数据或系统的职位可能需要更详细或更频繁的筛选。 **示例** 筛选选项可包括（视情况而定）实体所在地区、既往就业历史、公共信息/社会媒体资源审核、犯罪记录、信用记录以及推荐人检查。

要求和测试程序		指南
12.8 管理与第三方服务供应商（TPSP）关系相关的信息资产的风险。		
规定的方法要求	**规定的方法测试程序**	**目的**
12.8.1 备存与之共享帐户数据或可能影响帐户数据安全的所有第三方服务提供商（TPSP）的清单，包括对所提供的每项服务的描述。	**12.8.1.a** 检查政策和程序，核实是否制定了相应流程，以为与帐户数据共享或可能影响帐户数据安全的所有 TPSP 备存一份 TPSP 清单，包括对所提供的每项服务的描述。	备存一份所有 TPSP 的清单，以确定潜在风险延伸到组织之外的地方，并确定组织的扩展攻击面。
	12.8.1.b 检查文件，以核实是否保存了一份所有 TPSP 的清单，其中包括对所提供服务的描述。	**示例** 不同类型的 TPSP 包括那些： • 代表实体存储、处理或传输帐户数据（如支付网关、支付处理器、支付服务提供商（PSP）和非现场存储提供商）。 • 管理包含在实体的 PCI DSS 评估中的系统组件（如网络安全控制服务、反恶意软件服务和安全事故与事件管理（SIEM）的提供商；联络和呼叫中心；网络托管公司；以及 IaaS、PaaS、SaaS 和 FaaS 云提供商）。 • 可能影响实体 CDE 的安全（如通过远程访问提供支持的供应商，以及定制的软件开发人员）。
定制方法目标		
备存 TPSP 和所提供服务的记录。		
适用性说明		
使用符合 PCI DSS 的 TPSP 并不能使实体符合 PCI DSS，也不能免除实体对其自身 PCI DSS 遵从性的责任。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.8.2 维护与 TPSP 签订的书面协议，具体如下： • 维护与共享帐户数据或可能影响 CDE 安全的 TPSP 签订的书面协议。 • 书面协议包括 TPSP 的确认，即他们对 TPSP 拥有的或以其他方式代表该实体存储、处理或传输的帐户数据的安全负责，或在可能影响该实体的 CDE 安全的情况下负责。	**12.8.2.a** 检查政策和程序，核实是否制定了相应程序，以根据本要求中规定的所有元素维护了与所有 TPSP 签订的书面协议。	TPSP 的书面确认表明他们致力于确保其从客户处获得的帐户数据得到适当安全，并表明 TPSP 完全了解在提供 TPSP 服务期间可能受到影响的资产。特定 TPSP 对帐户数据安全的负责程度将取决于所提供的服务以及供应商与被评估实体（客户）之间的协议。 结合要求 12.9.1，本要求旨在促进各方对其适用的 PCI DSS 责任的理解达到一致水平。例如，该协议可能包括作为所提供服务的一部分而需要维护的适用 PCI DSS 要求。
定制方法目标	**12.8.2.b** 检查与 TPSP 签订的书面协议，以核实是否根据本要求中规定的所有元素对其进行了维护。	**良好做法** 实体还可能需要考虑在其与 TPSP 签订的书面协议中包括，TPSP 将支持实体根据要求 12.9.2 提出的信息请求。实体还希望了解是否有任何 TPSP 与其他 TPSP 有“嵌套”关系，即主要 TPSP 为提供服务而与其他 TPSP 签订合同。 必须了解主要 TPSP 是否依靠次要 TPSP 来实现服务的整体遵从性，以及主要 TPSP 与次要 TPSP 签订了哪些类型的书面协议。实体可以考虑在他们的书面协议中包括对主要 TPSP 可能使用的任何“嵌套”TPSP。
备存每个 TPSP 确认其保护帐户数据的责任的记录。		**更多信息** 请参考*“信息补充：关于进一步指南，第三方安全保证。*
适用性说明		
确认的确切措辞将取决于双方之间的协议、所提供服务的细节以及分配给每一方的责任。确认不一定要包括本要求中规定的确切措辞。 证明 TPSP 符合 PCI DSS 要求的证据（例如，PCI DSS 遵从性证明（AOC）或公司网站上的声明）与本要求中规定的书面协议不同。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 聘用 TPSP 的全面流程，包括聘用前的选择和审查细节，有助于确保 TPSP 在建立正式关系前得到实体内部的全面审查，并确保了解与聘用 TPSP 有关的持卡人数据风险。 **良好做法** 每个组织的具体尽职调查过程和目标会有所不同。应该考虑的元素包括供应商的报告惯例、违规通知和事件响应程序、PCI DSS 责任在各方之间分配的细节、TPSP 如何认证其 PCI DSS 遵从性以及他们提供的证据。
12.8.3 为聘用 TPSP 实施既定流程，包括在聘用前进行适当的尽职调查。	**12.8.3.a** 检查政策和程序，核实是否制定了聘用 TPSP 的相应流程，包括在聘用前进行适当的尽职调查。	
	12.8.3.b 检查证据并询问负责人员，核实聘用 TPSP 的流程是否包括在聘用前进行适当的尽职调查。	
定制方法目标		
在聘请 TPSP 之前，评估潜在 TPSP 在充分保护帐户数据方面的能力、意图和资源。		

要求和测试程序		指南
规定的方法要求 **12.8.4** 实施一项计划，至少每 12 个月监测一次 TPSP 的 PCI DSS 遵从性状态。 **定制方法目标** 定期核实 TPSP 的 PCI DSS 遵从性状态。 **适用性说明** 如果一个实体与 TPSP 达成协议，代表该实体满足 PCI DSS 要求（例如，通过防火墙服务），该实体必须与 TPSP 合作，确保满足适用的 PCI DSS 要求。如果 TPSP 不满足这些适用的 PCI DSS 要求，那么这些要求对该实体来说也是“未到位”的。	**规定的方法测试程序** **12.8.4.a** 检查政策和程序，核实是否制定了相应流程，以监控（至少每 12 个月一次）TPSP 的 PCI DSS 遵从性状态。 **12.8.4.b** 检查文件并询问负责人员，以核实是否至少每 12 个月一次对每个 TPSP 的 PCI DSS 遵从性状态进行了监控。	**目的** 掌握所有聘用的 TPSP 的 PCI DSS 遵从性状态，保证并了解他们是否符合适用于他们向组织提供的服务的要求。 **良好做法** 如果 TPSP 提供各种服务，实体监控的遵从性状态应该具体，包括交付给实体的那些服务以及实体的 PCI DSS 评估范围内的那些服务。 如果 TPSP 拥有 PCI DSS 遵从性证明书（AOC），则 TPSP 必须能够应客户要求提供，以证明其 PCI DSS 遵从性状态。 如果 TPSP 没有执行 PCI DSS 评估，他们可能能够提供其他足够的证据来证明其已满足适用要求，无需执行正式的遵从性认证。例如，TPSP 能够向实体的评估商提供具体证据，以便评估商可以确认适用要求得到满足。或者，TPSP 能够选择接受每个客户的评估商的多次按需评估，每次评估都是为了确认适用要求是否得到满足。 **更多信息** 关于第三方服务供应商的更多信息，请参考： • PCI DSS 部分：*第三方服务供应商的使用*。 • *信息补充：第三方安全保证*。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 重要的是，实体必须了解其 TPSP 同意满足哪些 PCI DSS 要求和子要求，哪些要求是 TPSP 和实体之间共享的，对于那些共享的要求，具体说明如何共享以及哪个实体负责满足每个子要求。 如果没有这种共识，实体和 TPSP 将不可避免地认为特定的 PCI DSS 子要求是另一方的责任，因此可能根本无法解决该子要求。 某实体维护的具体信息将取决于与其供应商签订的特定协议、服务类型等。TPSP 可以将他们的 PCI DSS 责任定义为对所有客户都是一样的；否则，这种责任应该由实体和 TPSP 共同商定。 **良好做法** 实体可以通过一个矩阵来记录这些责任，该矩阵确定了所有适用的 PCI DSS 要求，并针对每个要求指出实体或 TPSP 是否负责满足该要求，或者它是否为一个共同责任。这种类型的文件通常被称为*责任矩阵*。 各实体还必须了是否有任何 TPSP 与其他 TPSP 有“嵌套”关系，即主要 TPSP 为提供服务而与其他 TPSP 签订合同。必须了解主要 TPSP 是否依靠次要 TPSP 来实现服务的整体遵从性，以及主要 TPSP 如何监控服务绩效和次要 TPSP 的 PCI DSS 遵从性状态。请注意，管理和监控任何次要 TPSP 是主要 TPSP 的责任。 **更多信息** 如需责任矩阵模板样本，请参考*信息补充：第三方安全保障*。
12.8.5 维护哪些 PCI DSS 要求由每个 TPSP 管理，哪些由实体管理，以及是否有 TPSP 和实体之间共享的任何要求的任何信息。	**12.8.5.a** 检查政策和程序，核实是否制定了相应流程，以保留关于哪些 PCI DSS 要求由每个 TPSP 管理，哪些由实体管理，以及是否有 TPSP 和实体之间共享的任何要求的任何信息。	
定制方法目标	**12.8.5.b** 检查文件并询问相关人员，以核实该实体是否保留了关于哪些 PCI DSS 要求由每个 TPSP 管理，哪些由实体管理，以及是否有 TPSP 和实体之间共享的任何要求的任何信息。	
保留并定期审核详细说明 PCI DSS 要求以及每个 TPSP 单独或共同负责的相关系统组件的记录。		

要求和测试程序		指南
12.9 第三方服务提供商（TPSP）支持其客户的 PCI DSS 遵从性。		
规定的方法要求 **12.9.1** ***仅针对服务供应商的额外要求：*** TPSP 以书面形式向客户确认，他们对 TPSP 拥有的或以其他方式代表客户存储、处理或传输的帐户数据的安全负责，或在他们可能影响客户 CDE 安全的范围内负责。 **定制方法目标** TPSP 正式承认他们对客户负有安全责任。 **适用性说明** 本要求仅在被评估实体是服务提供商的情况下适用。确认的确切措辞将取决于双方之间的协议、所提供服务的细节以及分配给每一方的责任。确认不一定要包括本要求中规定的确切措辞。	**规定的方法测试程序** **12.9.1** ***仅适用于服务提供商评估的附加测试程序：*** 检查 TPSP 的政策、程序和用于书面协议的模板，核实是否制定了相应流程，以使 TPSP 按照本要求规定的所有元素向客户提供书面确认。	**目的** 结合要求 12.8.2，本要求旨在促进 TPSP 和其客户之间对其适用的 PCI DSS 责任的理解达到一致的水平。TPSP 的书面确认证明了他们致力于确保其从客户处获得的帐户数据得到适当安全。 TPSP 提供书面确认的方法应该由提供商和其客户商定。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.9.2 ***仅针对服务提供者的额外要求：*** TPSP 支持其客户对信息的要求，以满足要求 12.8.4 和 12.8.5，根据客户要求提供以下内容： • TPSP 代表客户执行的任何服务的 PCI DSS 遵从性状态信息（要求 12.8.4）。 • 关于哪些 PCI DSS 要求是 TPSP 的责任，哪些是客户的责任的信息，包括任何共享责任（要求 12.8.5）。	**12.9.2.** ***仅针对服务提供商评估的额外测试程序：*** 检查政策和程序，核实是否制定了相应流程，使 TPSP 能够支持客户的信息要求，从而根据本要求中规定的所有元素满足要求 12.8.4 和 12.8.5。	如果 TPSP 不提供所需信息，使其客户能够满足他们的安全和合规要求，客户将无法保护持卡人数据，也无法履行他们自身的合同义务。 **良好做法** 如果 TPSP 拥有 PCI DSS 遵从性证明书 (AOC），则 TPSP 必须能够应客户要求提供，以证明其 PCI DSS 遵从性状态。 如果 TPSP 没有执行 PCI DSS 评估，他们可能能够提供其他足够的证据来证明其已满足适用要求，无需执行正式的遵从性认证。例如，TPSP 能够向实体的评估商提供具体证据，以便评估商可以确认适用要求得到满足。或者，TPSP 能够选择接受每个客户的评估商的多次按需评估，每次评估都是为了确认适用要求是否得到满足。 TPSP 应该向其客户提供足够的证据，以核实 TPSP 的 PCI DSS 评估的范围涵盖了适用于客户的服务，并且相关的 PCI DSS 要求已被审查并确定到位。 *（下一页继续）*
定制方法目标		
TPSP 视需要提供信息，以支持其客户的 PCI DSS 合规工作。		
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。		

要求和测试程序		指南
		TPSP 可以将他们的 PCI DSS 责任定义为对所有客户都是一样的；否则，这种责任应该由客户和 TPSP 共同商定。重要的是，客户必须了解其 TPSP 同意满足哪些 PCI DSS 要求和子要求，哪些要求是 TPSP 和客户之间共享的，对于那些共享的要求，具体说明如何共享以及哪个实体负责满足每个子要求。记录这些责任的一个示例是通过一个矩阵，确定所有适用的 PCI DSS 要求，并指出客户或 TPSP 是否负责满足该要求，或者它是否为一个共同责任。 **更多信息** 如需更多指南，请参考： • PCI DSS 部分：使用第三方服务供应商.。 • 信息补充：第三方安全保证（包括责任矩阵模板样本）。

要求和测试程序		指南
12.10 立即响应可能影响 CDE 的可疑和确认的安全事件。		
规定的方法要求	**规定的方法测试程序**	**目的**
12.10.1 制定了事件响应计划，并随时准备在发生可疑或确认的安全事件时启动。该计划包括，但不限于： • 发生可疑或确认的安全事件时的角色、责任以及沟通和联系策略，至少包括通知支付品牌和收单机构。 • 事件响应程序，包括针对不同类型事件的具体遏制和缓解活动。 • 业务恢复和连续性程序。 • 数据备份程序。 • 分析报告数据遭受威胁的法律要求。 • 覆盖和响应所有关键系统组件。 • 参考或纳入支付品牌的事件响应程序。	**12.10.1.a** 检查事件响应计划，以核实该计划是否存在，并至少包括本要求中规定的元素。 **12.10.1.b** 询问相关人员并检查之前报告的事件或警报的文件，以核实是否遵循了书面事件响应计划和程序。	如果没有一个全面的事件响应计划，并被负责的各方适当地传播、阅读和理解，那么混乱和缺乏统一的响应会给企业带来更多的停机时间，不必要的公共媒体曝光，以及财务和/或声誉损失的风险和法律责任。 **良好做法** 事件响应计划应该全面，并包含利益相关者（例如，法律、通信）的所有关键元素，以便在发生可能影响帐户数据的违规事件时，实体能够做出有效响应。重要的是，要及时更新计划中所有被指定为在事件响应中发挥作用的个人的最新联系信息。其他需要通知的相关方可能包括客户、金融机构（收单机构和发卡机构）以及商业伙伴。 各实体应考虑如何在其事件响应计划中处理 CDE 内的所有数据威胁问题，包括对帐户数据、无线加密密钥、用于传输和存储或帐户数据或持卡人数据的加密密钥等。 **示例** 报告威胁事件的法律要求包括美国大多数州、欧盟通用数据保护条例（GDPR）和个人数据保护法（新加坡）的要求。 **更多信息** 欲了解更多信息，请参阅 *NIST SP 800-61 第 2 版，计算机安全事件处理指南。*
定制方法目标		
维护符合支付卡品牌期望的综合事件响应计划。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.10.2 至少每 12 个月对安全事件响应计划进行一次： • 审核并视需要更新内容。 • 测试，包括要求 12.10.1 中列出的所有元素。	**12.10.2** 询问相关人员并审核文件，以核实是否至少每 12 个月对安全事件响应计划进行一次： • 审核并视需要更新内容。 • 测试，包括要求 12.10.1 中列出的所有元素。	适当测试安全事件响应计划，可以识别受损的业务流程，并确保关键步骤不被遗漏，否则可能导致事件发生时的风险增大。对计划的定期测试，可确保流程保持可行，并确保组织中的所有相关人员都熟悉该计划。
定制方法目标		**良好做法**
事件响应计划保持最新，并定期进行测试。		对事件响应计划的测试可以包括模拟事件和以“桌面演习”形式进行的相应响应，相关人员也参与其中。审核事件和响应质量可以为实体提供保证，所有要求的元素都包含在计划中。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.10.3 指定特定人员 24 小时全天候待命，以响应可疑或确认的安全事件。	**12.10.3** 检查文件和询问担任指定角色的负责人员，以核实是否指定了特定人员 24 小时全天候待命，以响应可疑或确认的安全事件。	事件可能随时发生，因此，如果在检测到事件时，并且现场有曾接受过事件响应培训并熟悉实体计划的人员，实体正确响应事件的能力就会有所提高。 **良好做法** 通常，特定人员被指定为安全事件响应团队的一员，该团队全面负责响应事件（可能根据轮流时间表）并根据计划管理这些事件。事件响应团队可以由长期分配的核心成员组成，也可以由“按需”人员组成，可以根据自身的专长和事件的具体情况在必要时召集他们。 拥有可用资源以快速响应事件，可以最大限度地减少对组织造成的干扰。 团队或个人应响应的活动类型的例子包括任何未经授权的活动的证据，检测未经授权的无线接入点，关键的 IDS 警报，以及报告未经授权的关键系统或内容文件变更。
定制方法目标		
适当时立即响应事件。		

要求和测试程序		指南
规定的方法要求 **12.10.4** 负责响应可疑和确认的安全事件的人员应定期接受适当培训，了解他们的事件响应责任。	**规定的方法测试程序** **12.10.4** 检查培训文件并询问事件响应人员，以核实人员是否在其事件响应责任方面接受了适当的和定期的培训。	**目的** 如果没有训练有素且随时可用的事件响应团队，可能会对网络造成长期的损坏，关键数据和系统可能会因不当处理目标系统而遭到“污染”。这可能会阻碍事件后调查的成功。 **良好做法** 所有参与事件响应的人员都必须接受培训，并了解管理取证和调查的证据，这一点非常重要。
定制方法目标 相关人员了解他们在事件响应中的角色和责任，并且在需要时能获得援助和指导。		
规定的方法要求 **12.10.4.1** 实体的目标风险分析确定了事件响应人员的定期培训频率，该分析根据要求 12.3.1 中规定的所有元素执行。	**规定的方法测试程序** **12.10.4.1.a** 检查实体的目标风险分析，了解事件响应人员的培训频率，以核实风险分析是否按照要求 12.3.1 中规定的所有元素执行。 **12.10.4.1.b** 检查事件响应人员定期培训的书面结果并询问相关人员，核实是否根据实体为该要求执行的目标风险分析中规定的频率执行了培训。	**目的** 每个实体的环境和事件响应计划大不相同，其方法将取决于多种因素，包括实体的规模和复杂性、环境的变化程度、事件响应团队的规模以及人员的流动。 执行风险分析将使该实体能够确定向负有事件响应责任的人员提供培训的最佳频率。
定制方法目标 事件响应人员的培训频率与实体的风险相符。		
适用性说明 *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.10.5 安全事件响应计划包括监控和响应来自安全监控系统的警报，包括但不限于： • 入侵检测系统和入侵防御系统。 • 网络安全控制。 • 关键文件的变更检测机制。 • 支付页面的变更和篡改检测机制。*本项内容在其生效日期前是最佳实践；详情请参考下面的适用性说明。* • 检测未经授权的无线接入点。	**12.10.5** 检查文档并观察事件响应流程，以核实监控和响应来自安全监控系统的警报是否包含在安全事件响应计划中，包括但不限于本要求中规定的系统。	响应安全监控系统产生的警报，这些系统专门关注数据的潜在风险，这对防止漏洞至关重要，因此，这必须包括在事件反应流程中。
定制方法目标		
以结构化、可重复的方式响应由监控和检测技术产生的警报。		
适用性说明		
上述内容（监测和响应来自支付页面的变更和篡改检测机制的警报）在 2025 年 3 月 31 日之前是最佳实践，在此日期后将作为要求 12.10.5 的一部分并且必须在 PCI DSS 评估中予以充分考虑。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.10.6 安全事件响应计划根据所吸取的经验教训进行修改和发展并结合行业发展。	**12.10.6.a** 检查政策和程序，以核实是否制定了相应流程，以根据所吸取的经验教训来修改和发展安全事件响应计划并结合行业发展。	在事件发生后将吸取的经验教训纳入事件响应计划，并与行业发展同步，有助于保持计划的时效性，并能够响应新兴的威胁和安全趋势。
	12.10.6.b 检查安全事件响应计划，并与负责人员面谈，以核实事件响应计划是否根据所吸取的经验教训进行修改和发展并结合行业发展	**良好做法** 经验教训活动应包括所有级别的人员。尽管它通常被列为整个事件审核的一部分，但它应侧重于如何改进实体对事件的响应。 重要的是，不仅要考虑响应中没有达到已规划结果的元素，还要了解哪些方面做得不错，以及从这些做得不错的元素中吸取的经验教训是否可以应用到计划中没有达到已规划结果的元素。 优化实体的事件响应计划的另一种方法是了解针对其他组织的攻击，并利用这些信息来微调实体的检测、遏制、缓解或恢复程序。
定制方法目标		
每次调用后，审核并更新事件响应计划的有效性和准确性。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
12.10.7 建立事件响应程序，一旦检测到 PAN 储存在非预期位置立即启动，并包括： • 确定如果在非 CDE 内发现 PAN 应该采取的应对措施，包括恢复、安全删除和/或迁移到当前确定的 CDE 中，如适用。 • 确定敏感验证数据是否与 PAN 一起存储。 • 确定帐户数据的来源，以及它如何出现在非预期的位置。 • 补救导致帐户数据出现在非预期位置的数据泄漏或流程漏洞。	**12.10.7.a** 检查书面事件响应程序，核实是否制定了相应程序，以响应 PAN 储存在非预期位置的情况，准备好启动，并包括本要求中规定的所有元素。	在发现 PAN 储存在非预期位置后遵循书面事件响应程序，有助于确定必要的补救措施并防止未来发生泄漏。
定制方法目标	**12.10.7.b** 询问相关人员并检查响应行动的记录，以核实事件响应程序是否在检测到 PAN 储存在非预期位置时立即执行。	**良好做法**
制定相应流程，以便在检测到 PAN 储存在非预期位置时及时响应、分析和处理情况。		如果在非 CDE 内发现 PAN，则应进行分析，以 1）确定它是否与其他数据分开保存或与敏感验证数据一起保存，2）确定数据的来源，以及 3）确定导致数据在非 CDE 内的控制差距。 各实体应考虑是否有促成因素，如业务流程、用户行为、不当的系统配置等，导致 PAN 存储在一个意外位置。如果存在这种促成因素，应根据本要求进行处理，以防止再次发生。
适用性说明		
本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。		

附录 A　额外 PCI DSS 要求

本附录包含针对不同类型实体的额外 PCI DSS 要求。在本附录中，章节包括：

- 附录 A1：　针对多租户服务提供商的额外 PCI DSS 要求
- 附录 A2：　针对使用 SSL/早期 TLS 进行实体信用卡 POS POI 终端连接的实体的额外 PCI DSS 要求
- 附录 A3：　指定的实体补充认证(DESV)

每一部分都提供了指导和适用性信息。

附录 A1：针对多租户服务提供商的额外 PCI DSS 要求

章节
A1.1 多租户服务提供商保护和隔离所有客户环境和数据。
A1.2 多租户服务供应商促进所有客户的日志记录和事件响应。

概述
所有服务提供商都有责任满足其自身环境的 PCI DSS 要求，因为该环境适用于向其客户提供的服务。此外，多租户服务提供商必须满足本附录中的要求。
多租户服务提供商是一种向商户和其他服务提供商提供各种共享服务的第三方服务提供商，客户共享系统资源（如物理或虚拟服务器）、基础设施、应用程序（包括软件即服务（SaaS））和/或数据库。服务可包括但不限于在单一共享服务器上托管多个实体，提供电子商务和/或"购物车"服务，基于网络的托管服务，支付应用程序，各种云应用程序和服务，以及与支付网关和处理器连接。
就本附录而言，仅提供共享数据中心服务的服务提供商（通常称为主机托管或"主机托管（co-lo）"提供商），其设备、空间和带宽均以租赁方式提供，不被视为多租户服务提供商。
注：即使多租户服务提供商可能满足这些要求，每个客户仍有责任遵守适用于其环境的 PCI DSS 要求，并视情况认证遵从性。一般情况下，提供商和客户共同负责一些 PCI DSS 要求（可能是环境的各个不同方面）。要求 12.8 和 12.9 描述了所有第三方服务提供商（TPSP）与其客户之间关系的具体要求，以及双方的责任。这包括确定客户正在接受的具体服务，以及客户必须满足的 PCI DSS 要求，TPSP 必须满足的 PCI DSS 要求，以及客户和 TPSP 必须共同满足的要求。

要求和测试程序		指南
A1.1 多租户服务提供商保护并分离所有客户环境和数据。		
规定的方法要求 **A1.1.1** 逻辑分离的实施方式如下： • 供应商未经授权不能访问其客户的环境。 • 客户未经授权不能访问提供商的环境。 **定制方法目标** 客户不能访问供应商的环境。供应商未经授权不能访问其客户的环境。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **A1.1.1** 检查文件和系统及网络配置并询问相关人员，以核实是否根据本要求中规定的所有元素实施了逻辑分离。	**目的** 如果没有在提供商的环境和客户的环境之间制定相应控制，提供商环境中的恶意行为者可能会威胁客户的环境，同样，客户环境中的恶意行为者也可能会威胁提供商和提供商的其他客户。 多租户环境应该相互隔离，并与提供商的基础设施隔离，以便它们可以成为单独管理的实体。也就是说，它们之间没有连接。 **良好做法** 供应商应确保在专为客户访问而设计的环境（例如配置和计费门户）与供应商的私有环境之间进行强有力的分离，后者只应由授权供应商人员访问。 服务提供商按照要求 8.2.3 访问客户环境。 **更多信息** 更多指南，请参考*信息补充：PCI SSC 云计算指南*。

要求和测试程序		指南
规定的方法要求 **A1.1.2** 实施相应控制，以便每个客户只有权限访问自己的持卡人数据和 CDE。 **定制方法目标** 客户不能访问其他客户的环境。	**规定的方法测试程序** **A1.1.2.a** 检查文件，以核实是否制定了相应控制，以便每个客户只有权限访问自己的持卡人数据和 CDE。 **A1.1.2.b** 检查系统配置，以核实每个客户只有权限访问自己的帐户数据和 CDE。	**目的** 多租户服务提供商必须制定相应控制，以便每个客户只能访问他们自己的环境和 CDE，以防止客户从他们自己的环境未经授权地访问另一个环境。 **示例** 在基于云的基础设施中，例如基础设施即服务（IaaS）产品，客户的 CDE 可能包括由客户配置和管理的虚拟网络设备和虚拟服务器，包括操作系统、文件、内存等。
规定的方法要求 **A1.1.3** 实施相应控制，以便每个客户只能访问分配给他们的资源。 **定制方法目标** 客户不能影响分配给其他客户的资源。	**规定的方法测试程序** **A1.1.3** 检查客户的权限，以核实每个客户是否只能访问分配给他们的资源。	**目的** 为了防止对其他客户的环境或帐户数据产生任何无意或有意的影响，重要的是每个客户只能访问分配给该客户的资源。

要求和测试程序		指南
规定的方法要求 **A1.1.4** 至少每六个月通过穿透测试确认一次用于分离客户环境的逻辑分离控制的有效性。 **定制方法目标** 定期认证客户环境与其他环境的分离是否有效。 **适用性说明** 除了要求 11.4.6 中规定的穿透测试，还对多租户服务提供商环境中客户之间的适当分离进行了测试。 ***本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。***	**规定的方法测试程序** **A1.1.4** 检查最近一次穿透测试，以核实测试是否确认了用于分离客户环境的逻辑分离控制的有效性。	**目的** 多租户服务供应商负责管理其客户之间的分段。 如果使用的技术无法保证分段控制的有效性，服务提供商的技术变更就有可能无意中产生漏洞，而这个漏洞可以在服务提供商的所有客户中加以利用。 **良好做法** 通过使用服务提供者创建的代表客户环境的临时（模拟）环境，并尝试 1）从另一个环境访问一个临时环境，以及 2）从互联网访问一个临时环境，可以确认分离技术的有效性。

要求和测试程序		指南
A1.2 多租户服务提供商促进所有客户的记录和事件响应。		
规定的方法要求 **A1.2.1** 检查日志功能在每个客户的环境中启用，与 PCI DSS 要求 10 一致，包括： • 日志在常见的第三方应用程序中启用。 • 默认情况下，日志处于激活状态。 • 日志只供自有客户查看。 • 日志的位置清楚地传达给自有客户。 • 日志数据和可用性与 PCI DSS 要求 10 一致。 **定制方法目标** 在不影响其他客户的保密性的情况下，日志功能供所有客户使用。	**规定的方法测试程序** **A1.2.1** 检查文件和系统配置设置，以核实供应商是否按照本要求中规定的所有元素为每个客户环境启用了检查日志功能。	**目的** 日志信息非常适用于检测和排除安全事件，也适用于取证调查。因此，客户必须拥有这些日志的访问权限。 然而，攻击者也可以使用日志信息进行侦察，因此，客户的日志信息必须只由日志相关的客户所访问。
规定的方法要求 **A1.2.2** 实施相应流程或机制，以在任何客户发生可疑或确认的安全事件时，支持和/或促进对相关服务器的及时取证调查。 **定制方法目标** 在发生可疑或确认的安全事件时，客户可随时要求取证调查。	**规定的方法测试程序** **A1.2.2** 检查书面程序，以核实供应商是否有相应流程或机制，以在任何客户发生可疑或确认的安全事件时，支持和/或促进对相关服务器的及时取证调查。	**目的** 在怀疑或确认持卡人数据的保密性遭到违反的情况下，客户的取证调查员旨在找到违反的原因，将攻击者排除在环境之外，并确保移除所有未经授权的访问。 迅速及有效响应取证调查员的要求，可以缩短调查员在保护客户环境方面所需的时间。

要求和测试程序		指南
规定的方法要求 **A1.2.3** 实施相应流程或机制，以报告和处理可疑或确认的安全事件和漏洞，包括： • 客户可以安全地向提供商报告安全事件和漏洞。 • 提供商根据要求 6.3.1 处理和补救可疑或确认的安全事件和漏洞。 **定制方法目标** 发现并处理可疑或确认的安全事件或漏洞。适当时通知客户。 **适用性说明** *本要求在 2025 年 3 月 31 日之前是最佳实践，在此日期后规定并且必须在 PCI DSS 评估中予以充分考虑。*	**规定的方法测试程序** **A1.2.3** 检查书面程序并询问相关人员，以核实该提供商是否拥有一个报告和处理可疑或确认的安全事件和漏洞的机制，并符合本要求规定的所有元素。	**目的** 所提供服务中的安全漏洞会影响到服务提供商所有客户的安全，因此必须按照服务提供商的既定流程进行管理，并优先解决具有最高威胁概率的漏洞。 客户在使用服务时有可能注意到漏洞和安全错误配置。 实施客户报告安全事件和漏洞的安全方法，鼓励客户报告潜在的问题，并使供应商能够快速了解和解决其环境中的潜在问题。

附录 A2：针对使用 SSL/早期 TLS 进行实体信用卡 POS POI 终端连接的实体的额外 PCI DSS 要求

章节
A2.1 使用 SSL 和/或 早期 TLS 的 POI 终端被确认为不易受到已知 SSL/TLS 利用的影响。

概述

本附录仅适用于使用 SSL/早期 TLS 作为安全控制来保护 POS POI 终端的实体，包括提供 POS POI 终端连接的服务提供商。

使用 SSL 和早期 TLS 进行 POS POI 终端连接的实体必须努力尽快升级到强大的加密协议。此外，不得将 SSL 和/或早期 TLS 引入到尚未存在这些协议的环境中。在发布之时，很难在 POS POI 支付终端中利用已知漏洞。然而，随时可能会出现新的漏洞，组织有责任及时了解漏洞趋势，并确定其是否易受任何已知漏洞的影响。

直接受影响的 PCI DSS 要求包括：

- **要求 2.2.5**：在存在任何不安全的服务、协议或守护程序的情况下；记录业务理由，并记录和实施额外的安全功能，以减轻在使用不安全的服务、协议或守护程序时的风险。
- **要求 2.2.7**：使用强效加密法对所有非控制台的管理访问进行加密。
- **要求 4.2.1**：在开放的公共网络进行传输时，实施强效加密法和安全协议以保护 PAN。

不得使用 SSL 和早期 TLS 作为安全控制来满足这些要求，除非是在 POS POI 终端连接的情况下，如本附录所详述。为了支持实体在 POS POI 终端上从 SSL/早期 TLS 的迁移工作，将包括以下规定：

- 新的 POS POI 终端实施不得使用 SSL 或早期 TLS 作为安全控制。
- 所有 POS POI 终端服务提供商必须提供安全的服务项目。
- 支持使用 SSL 和/或早期 TLS 的现有 POS POI 终端实施的服务提供商必须制定一个正式的风险缓解和迁移计划。
- 在实体信用卡环境中的 POS POI 终端，如果可以核实其不易受任何已知的 SSL 和早期 TLS 以及**其连接的 SSL/TLS 终端点**的影响，可以继续使用 SSL/早期 TLS 作为安全控制。

本附录中的要求不适用于定制方法。

要求和测试程序		指南
A2.1 使用 SSL 和/或早期 TLS 的 POI 终端被确认为不易受到已知 SSL/TLS 利用的影响。		
规定的方法要求 **A2.1.1** 如果商户或支付认可地点的 POS POI 终端使用 SSL 和/或早期 TLS，该实体确认这些设备不易受到这些协议的任何已知漏洞的影响。 **定制方法目标** 这项要求不适用于定制方法。 **适用性说明** 本要求旨在针对拥有 POS POI 终端的实体，如商户。本要求并非针对作为所述 POS POI 终端的终端或连接点的服务提供商。要求 A2.1.2 和 A2.1.3 适用于 POS POI 服务提供者。 对目前不易被利用的 POS POI 终端的允许是基于目前已知的风险。如果出现了 POS POI 终端易受影响的新漏洞，则将需要立即更新 POS POI 终端。	**规定的方法测试程序** **A2.1.1** 对于使用 SSL 和/或早期 TLS 的 POS POI 终端，确认该实体拥有相应文件（例如，供应商文件、系统/网络配置细节），以核实该设备不易受到任何已知的 SSL /早期 TLS 的影响。	**目的** 在实体信用卡环境中使用的 POS POI 终端可以继续使用 SSL/早期 TLS，如果可以证明该 POS POI 终端不易受到当前已知漏洞的影响。 **良好做法** 然而，SSL 是过时的技术，将来可能易受到更多安全漏洞的影响；因此强烈建议 POS POI 终端尽快升级到安全协议。如果环境中不需要 SSL/早期 TLS，应禁止这些版本的使用和回退。 **更多信息** 更多指南，请参考当前 PCI SSC 关于 SSL/早期 TLS 的信息补充。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A2.1.2 ***仅针对服务提供者的额外要求：*** 对于拥有与使用 A2.1 中确定的 SSL 和/或早期 TLS 的 POS POI 终端的现有连接点的所有服务提供商，制定了正式的风险缓解和迁移计划，包括： • 使用情况说明，包括正在传输的数据、使用和/或支持 SSL/早期 TLS 的系统类型和数量，以及环境类型。 • 风险评估结果和已实施的风险降低控制。 • 描述监测与 SSL/早期 TLS 相关的新漏洞的流程。 • 描述为确保 SSL/早期 TLS 不会在新环境应用而实施的变更控制流程。 • 概述在未来取代 SSL/早期 TLS 的迁移项目计划。	**A2.1.2** ***仅针对服务提供商评估的额外测试程序：*** 审核书面风险缓解和迁移计划，以核实其是否包括本要求中规定的所有元素。	POS POI 终端，包括但不限于服务提供商，例如收单机构或收单机构处理商，在能够证明服务提供商具备控制来降低支持服务提供商环境的这些连接的风险时，可以继续使用 SSL/早期 TLS。 **良好做法** 服务提供商应向所有使用 SSL/早期 TLS 的客户传达与使用该协议相关的风险以及迁移到安全协议的必要性。 **定义** 风险缓解和迁移计划是一份由实体编制的文件，详细说明了其迁移到安全协议的计划，并描述了实体为减少与 SSL/早期 TLS （直到迁移完成）相关的风险的控制措施。 **更多信息** 关于风险缓解和迁移计划的更多指南，请参考当前 PCI SSC 关于 SSL/早期 TLS 的信息补充。
定制方法目标		
这项要求不适用于定制方法。		
适用性说明		
本要求仅在被评估实体是服务提供商的情况下适用。		

要求和测试程序		指南
规定的方法要求 **A2.1.3** ***仅针对服务提供商的额外要求***：所有服务提供商提供安全服务项目。 **定制方法目标** 这项要求不适用于定制方法。 **适用性说明** 本要求仅在被评估实体是服务提供商的情况下适用。	**规定的方法测试程序** **A2.1.3** ***仅针对服务提供商评估的额外测试程序：***检查系统配置和支持文件，以核实服务提供商是否为其服务提供安全协议选项。	**目的** 客户必须能够选择升级其 POI 以消除使用 SSL 和早期 TLS 的漏洞。在许多情况下，客户需要采取分阶段或渐进的方式将其 POS POI 从不安全协议迁移到安全协议，因此需要的是服务提供商支持安全服务项目。 **更多信息** 更多指南，请参考当前 PCI SSC 关于 SSL/早期 TLS 的信息补充。

附录 A3：指定的实体补充认证(DESV)

章节
A3.1 实施 PCI DSS 遵从性计划。
A3.2 记录和认证 PCI DSS 范围。
A3.3 将 PCI DSS 纳入到业务正常（BAU）活动中。
A3.4 控制和管理持卡人数据环境的逻辑访问情况。
A3.5 识别并应对可疑事件。

概述

本附录仅适用于由支付品牌或收单机构指定的需要额外认证现有 PCI DSS 要求的实体。只有在收单机构或支付品牌的指示下，实体才需要根据本附录执行评估。本附录可能适用的实体的例子包括：

- 那些存储、处理和/或传输大量帐户数据的实体。
- 那些为帐户数据提供汇总点的实体，或
- 那些曾遭受过重大或反复的帐户数据漏洞的实体。

此外，其他 PCI 标准可以参考本附录的完成情况。

这些补充认证步骤旨在通过认证业务正常（BAU）流程以及加强认证和范围界定考虑，更好地保证 PCI DSS 控制的有效和持续维护。

注：*部分要求具有规定的时间范围（例如，至少每三个月一次或至少每六个月一次），某些活动必须在此范围内执行。对于本文件的初次评估，不要求在前一年每个此类时间范围内都执行某项活动，如果评估商核实：*

- *该活动是在最近的时间范围内（例如，最近的三个月或六个月）按照适用的要求执行的，并且*
- *该实体制定了书面政策和程序，以便在规定的时间范围内继续执行该活动。*

对于初次评估后的随后几年，必须在每个规定的时间范围内执行一项活动（例如，要求每三个月执行一次的活动必须在前一年至少执行四次，间隔时间不超过 90 天）。

并非 PCI DSS 中的所有要求都适用于可能执行 PCI DSS 评估的所有实体。正是由于这个原因，一些 PCI DSS 要求在本附录中重复出现。有关本附录的任何问题都应向收单机构或支付品牌提出。

要求和测试程序		指南
A3.1 实施 PCI DSS 遵从性计划。		
规定的方法要求	**规定的方法测试程序**	**目的**
A3.1.1 执行管理层确立了责任，以保护帐户数据和 PCI DSS 遵从性计划，其中包括： • 对维护 PCI DSS 遵从性的总体责任。 • 确定 PCI DSS 遵从性计划的章程。 • 至少每 12 个月向执行管理层和董事会提供一次关于 PCI DSS 遵从性计划和问题的最新信息，包括补救活动。 **PCI DSS 参考**：*要求 12*	**A3.1.1.a** 检查文件，以核实执行管理层是否已分配维护实体的 PCI DSS 遵从性的总体责任。 **A3.1.1.b** 检查公司的 PCI DSS 章程，以核实其是否概述了组织 PCI DSS 遵从性计划的条件。 **A3.1.1.c** 检查执行管理层和董事会的会议记录和/或演示，以确保至少每 12 个月沟通一次 PCI DSS 遵从性计划和补救活动。	执行管理层分配 PCI DSS 遵从性责任，确保行政级别了解 PCI DSS 遵从性计划，并允许有机会提出适当问题，以确定计划的有效性并影响战略重点。 **良好做法** 执行管理层可能包括 C 级职位、董事会或同等职位。具体头衔将取决于特定的组织结构。 可能将 PCI DSS 遵从性计划的责任分配给组织内的个人角色和/或业务单位。
定制方法目标		
这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.1.2 制定正式的 PCI DSS 遵从性计划，其中包括： • 定义维护和监控整体 PCI DSS 遵从性的活动，包括业务正常活动。 • 年度 PCI DSS 评估流程。 • 持续认证 PCI DSS 要求的流程（例如，每天、每周、每三个月，根据要求适用）。 • 执行业务影响分析的流程，以确定 PCI DSS 对战略业务决策的潜在影响。 **PCI DSS 参考**：*要求 1-12*	**A3.1.2.a** 检查信息安全政策和程序，以核实是否制定了相应流程，以执行正式的 PCI DSS 遵从性计划，其中包括本要求中规定的所有元素。	正式的遵从性计划使组织能够监控其安全控制的健康状况，在控制发生故障时采取主动，并在整个组织内有效地沟通活动和遵从性状态。 **良好做法** PCI DSS 遵从性计划可以是一个专项计划，也可以是主要遵从性和/或治理计划的一部分，并且应该包括一个定义明确的方法，以展示一致和有效的评估。 应对战略业务决策是否受到 PCI DSS 的潜在影响进行分析，这些决策可能包括兼并和收购、新技术采购或新的支付认可渠道。 **定义** 维护和监控组织的整体 PCI DSS 遵从性包括确定每天、每周、每月、每三个月或每年需要执行的活动，并确保这些活动的相应执行（例如，使用安全自我评估或 PDCA 方法）。 **示例** 支持遵从性计划管理的方法包括计划-执行-检查-处理（PDCA）、ISO 27001、COBIT、DMAIC 和六西格玛。
定制方法目标	**A3.1.2.b** 询问相关人员并观察遵从性活动，以核实是否按照本要求中规定的所有元素实施了正式的 PCI DSS 遵从性计划。	
这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.1.3 具体定义 PCI DSS 的遵从性角色和责任并正式分配给一个或多个人员，包括： • 管理 PCI DSS 的业务正常活动。 • 管理年度 PCI DSS 评估。 • 管理 PCI DSS 要求的持续认证（例如，每天、每周、每三个月，根据要求适用）。 • 管理业务影响分析，以确定 PCI DSS 对战略业务决策的潜在影响。 **PCI DSS 参考**：*要求 12*	**A3.1.3.a** 检查信息安全政策和程序并询问相关人员，以核实 PCI DSS 遵从性角色和职责是否按照本要求的所有元素具体定义并正式分配给一名或多名人员。 **A3.1.3.b** 询问负责人员，核实他们是否熟悉并履行其指定的 PCI DSS 遵从性职责。	正式定义具体的 PCI DSS 遵从性角色和责任，有助于确保问责和监测正在进行的 PCI DSS 遵从性工作。 **良好做法** 应将所有权分配给有权做出基于风险的决策的个人，并由其对特定功能问责。应该正式定义职责，所有者应该能够证明对其职责和问责的理解。 可以将遵从性角色分配给一个所有者，也可以分配给不同需求元素的多个所有者。
定制方法目标		
这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.1.4 至少每 12 个月向承担 PCI DSS 遵从性职责的人员（如 A3.1.3 中确定的）提供一次最新的 PCI DSS 和/或信息安全培训。 **PCI DSS 参考**：*要求 12*	**A3.1.4.a** 检查信息安全政策和程序，以核实每个承担 PCI DSS 遵从性职责的角色是否需要至少每 12 个月进行一次 PCI DSS 和/或信息安全培训。	负责 PCI DSS 遵从性的相关人员拥有超出一般安全意识培训所提供的具体培训需求，以使他们能够履行其职责。 **良好做法** 承担 PCI DSS 遵从性职责的人员应该接受专门培训，除了一般的信息安全意识之外，还应该关注特定的安全主题、技能、流程或方法，这些是所述人员为能有效履行遵从性职责必须遵循的培训。 培训可以由第三方提供，例如 PCI SSC（例如，PCI Awareness、PCIP 和 ISA）、支付品牌和收单机构，也可以由内部人员提供培训。培训内容应适用于个人的工作职能，确保其时效性，包括最新的安全威胁和/或 PCI DSS 的版本。 **更多信息** 有关其他指导，请参阅*信息补充：实施安全意识计划的最佳做法*
定制方法目标	**A3.1.4.b** 询问相关人员，并检查培训结业证书或其他记录，以核实承担 PCI DSS 遵从性职责的人员是否至少每 12 个月接受一次最新的 PCI DSS 和/或类似信息安全培训。	
这项要求不适用于定制方法。		

要求和测试程序		指南
A3.2 记录和认证 PCI DSS 范围。		
规定的方法要求	**规定的方法测试程序**	**目的** 经常认证 PCI DSS 范围有助于确保 PCI DSS 范围保持时效性，并与不断变化的业务目标保持一致，从而确保安全控制能够保护所有合适的系统组件。 **良好做法** 准确范围界定包括严格评估 CDE 和所有连接的系统组件，以确定 PCI DSS 要求的必要覆盖范围。范围界定活动，包括仔细分析和持续监控，有助于确保对范围内系统的适当保护。在记录帐户数据位置时，该实体可以考虑创建一个包括以下信息的表格或电子表格： • 数据存储（数据库、文件、云端等），包括数据存储的目的和保留期、 • 存储的 CHD 元素（PAN、到期日、持卡人姓名和/或完成授权前的任何 SAD 元素）、 • 保持数据安全的方法（加密类型和强度、散列算法和强度、截词、令牌化）、 • 记录数据存储访问情况的方式，包括正在使用的记录机制的描述（企业解决方案、应用程序级别、操作系统级别等）。 *（下一页继续）*
A3.2.1 至少每三个月一次并在范围内环境发生重大变动时记录并确认 PCI DSS 范围的准确性。范围界定认证至少包括： • 确定各个支付阶段（例如，授权、捕获、结算、拒付和退款）和认可渠道（例如，实体信用卡、虚拟信用卡和电子商务）的所有数据流。 • 根据要求 1.2.4 更新所有数据流程图。 • 确定所有储存、处理和传输帐户数据的位置，包括但不限于：1）当前定义的非 CDE 内的任何位置；2）处理 CHD 的应用程序；3）系统和网络之间的传输；以及 4）文件备份。 • 对于在当前定义的非 CDE 内发现的任何帐户数据，1）安全删除，2）迁移到当前定义的 CDE，3）扩展当前定义的 CDE 以使之包括在内。 • 识别 CDE 中的、连接到 CDE 的或可能影响 CDE 安全的所有系统组件。 • 识别所有正在使用的分段控制和分割 CDE 的所在环境，包括环境不在范围内的理由。 • 识别所有与可访问 CDE 的第三方实体的连接。 *（下一页继续）*	**A3.2.1.a** 检查范围审核的书面结果并询问相关人员，以核实审核的执行情况，包括： • 至少每三个月执行一次。 • 审核是否在范围内环境发生重大变动后进行。 **A3.2.1.b** 检查范围审核（至少每三个月执行一次）的书面结果，以核实范围界定认证包括本要求规定的所有元素。	

要求和测试程序		指南
• 确认所有已识别的数据流、帐户数据、系统组件、分段控制以及来自第三方实体的、可以访问 CDE 的连接是否包括在范围内。 **PCI DSS 参考**：*PCI DSS 要求的范围，要求 12。*		除了内部系统和网络之外，还需要识别来自第三方实体的所有连接—例如，商业伙伴、提供远程支持服务的实体以及其他服务提供商—以确定纳入 PCI DSS 范围的情况。确定范围内连接后，便可实施适用的 PCI DSS 控制，以减轻第三方连接被用于威胁实体的 CDE 的风险。 可以使用数据发现工具或方法，以促进对 PAN 所有来源和位置的识别，并寻找留在当前确定的非 CDE 内的系统和网络上或在确定的 CDE 内意外位置的 PAN—例如，在错误日志或内存转储文件中。这种方法可以帮助确保检测到之前未知的 PAN 位置，并确保 PAN 的消除或适当保护。 **更多信息** 如需责任矩阵模板样本，请参考*信息补充：PCI DSS 范围界定和网络分段指南*。
定制方法目标 这项要求不适用于定制方法。		
规定的方法要求	**规定的方法测试程序**	**目的**
A3.2.2 确定 PCI DSS 范围对系统或网络的所有变更的影响，包括增加新系统和新网络连接。流程包括： • 执行正式的 PCI DSS 影响评估。 • 识别系统或网络的适用 PCI DSS 要求。 • 适当地更新 PCI DSS 范围。 • 负责人员（如 A3.1.3 定义的）记录并签收影响评估的结果。 **PCI DSS 参考**：*PCI DSS 要求的范围；要求 1-12*	**A3.2.2** 检查变更文件询问相关人员，以核实对于系统或网络的每项变更，是否已确定 PCI DSS 范围的影响，并包括本要求中规定的所有元素。	系统或网络变动会对 PCI DSS 范围产生重大影响。例如，网络安全控制规则集的变更可能会使整个网段进入范围，或者新的系统可能会被添加到必须受到适当保护的 CDE 中。 在变更前执行正式的影响评估，可以向实体保证该变更不会对 CDE 的安全产生不利影响。 **良好做法** 确定系统和网络的变更可能对实体的 PCI DSS 范围产生的潜在影响的流程可以作为专门 PCI DSS 遵从性计划的一部分予以执行，也可以在实体的主要遵从性和/或治理计划下予以执行。
定制方法目标 这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.2.2.1 在完成变更后，确认所有相关的 PCI DSS 要求是否在所有新的或变更后的系统和网络上实施，文件是否视情况进行更新。 **PCI DSS 参考**：*PCI DSS 要求的范围；要求 1-12*	**A3.2.2.1** 检查变更记录和受影响的系统/网络，询问相关人员，以核实是否实施了所有相关的 PCI DSS 要求，以及是否根据变更规定更新了文件。	拥有分析对系统或网络所做的所有变更的流程非常重要，以确保所有适当的 PCI DSS 控制适用于由于变更而添加到范围内环境的任何系统或网络。 将这种认证纳入到变更管理流程中，有助于确保设备清单和配置标准保持最新，并在需要时应用安全控制。 **良好做法** 变更管理流程应包括支持证据，证明 PCI DSS 要求通过迭代流程得到实施或保留。 **示例** 应核实的 PCI DSS 要求包括但不限于： • 更新网络图以反映变更。 • 根据配置标准对系统进行配置，更改所有默认密码并禁用多余的服务。 • 系统通过所需的控制受到保护—例如，文件完整性监控、反恶意软件、补丁和检查日志。 • 不存储敏感验证数据，记录所有帐户数据存储并将其纳入数据保留政策和程序。 • 新系统包括在每季度的漏洞扫描过程中。
定制方法目标		
这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.2.3 组织结构变动促成对 PCI DSS 范围和控制适用性的影响的正式（内部）审核。 **PCI DSS 参考**：*要求 12*	**A3.2.3** 检查政策和程序，以核实组织结构变动是否促成对 PCI DSS 范围和控制适用性的影响的正式审核。	组织的结构和管理确定了有效和安全操作的要求和协议。这种结构的变更可能会对现有的控制和框架产生负面影响，因为必须重新分配或移除曾经支持 PCI DSS 控制的资源，或继承可能没有既定控制的新职责。因此，在对组织的结构和管理进行变更时，必须重新审视 PCI DSS 的范围和控制措施，以确保控制措施到位并发挥作用。
定制方法目标		**示例**
这项要求不适用于定制方法。		组织结构变动包括但不限于公司合并或收购，以及负责安全控制的人员的重大变动或重新分配。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 根据 PCI DSS 规定，必须每 12 个月通过穿透测试来对分段控制进行核实。 更为频繁认证分段控制可能会在攻击者试图从范围外的不可信网络横向转移到 CDE 之前发现分段故障。 **良好做法** 尽管要求规定该范围认证至少每六个月进行一次，并在重大变更后进行，但该工作应尽可能频繁地进行，以确保它能有效地将 CDE 与其他网络隔离开来。 **更多信息** 如需责任矩阵模板样本，请参考*信息补充：穿透测试指南*。
A3.2.4 如果使用分段，PCI DSS 范围确认如下： • 根据要求 11.4.1 中定义的实体方法。 • 至少每六个月对分段控制进行一次穿透测试，并在分段控制/方法发生任何变更后进行。 • 穿透测试涵盖所有正在使用的分段控制/方法。 • 穿透测试核实分段控制/方法是否可操作及有效，并将 CDE 与所有范围外的系统隔离开来。 **PCI DSS 参考**：*要求 11*	**A3.2.4** 检查最近一次穿透测试的结果，以核实该测试按照本要求中规定的所有元素执行。	
定制方法目标 这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求 **A3.2.5** 实施一种数据发现方法，以： • 确认 PCI DSS 范围。 • 至少每三个月一次，并在 CDE 或流程发生重大变化时，确定明文 PAN 的所有来源和位置。 • 解决明文 PAN 存在于当前定义的非 CDE 内的系统和网络中的可能性。 **PCI DSS 参考**：*PCI DSS 要求的范围* **定制方法目标** 该要求不适用于定制方法	**规定的方法测试程序** **A3.2.5.a** 检查书面数据发现方法，以核实它包括本要求中规定的所有元素。 **A3.2.5.b** 检查近期数据发现工作的结果，并询问负责人员，以核实数据发现是否至少每三个月进行一次，并在 CDE 或流程发生重大变化时进行。	**目的** PCI DSS 规定，作为范围界定工作的一部分，接受评估的实体必须确定并记录存在于其环境中的所有明文 PAN。实施数据发现方法，确定明文 PAN 的所有来源和位置，并检查当前定义的非 CDE 内的系统和网络上或在定义的 CDE 内的意外位置（例如，在错误日志或内存转储文件中）是否有明文 PAN，有助于确保检测到明文 PAN 的既往未知位置并得到适当保护。 **示例** 数据发现过程可以通过各种方法进行，包括但不限于：1) 商业上可用的数据发现软件，2) 内部开发的数据发现程序，或 3）人工搜索。也可以根据需要使用各种方法的组合。 无论使用何种方法，这项工作的目标是找到明文 PAN 的所有来源和位置（不仅仅是在定义的 CDE 中）。

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 测试数据发现方法的有效性以确保帐户数据检测的完整性和准确性的流程。 **良好做法** 为了保证完整性，范围内网络的系统组件和范围外网络的系统都应包括在数据发现过程中。 数据发现过程应该在所有正在使用的操作系统和平台上运作。将测试 PAN 置于正在使用的系统组件和文件格式上，并确认数据发现方法是否检测到测试 PAN，即可测试准确性。
A3.2.5.1 数据发现方法确认如下： • 测试了这些方法的有效性。 • 这些方法能够发现所有类型的系统组件上和正在使用的文件格式的明文 PAN。 • 数据发现方法的有效性至少每 12 个月确认一次。 **PCI DSS 参考**：*PCI DSS 要求的范围*	**A3.2.5.1.a** 询问相关人员并审核文件，以核实： • 该实体是否设有测试数据发现方法的有效性的流程。 • 该流程是否包括核实这些方法能否发现所有类型的系统组件和正在使用的文件格式上的明文 PAN。	
定制方法目标	**A3.2.5.1.b** 检查有效性测试的结果，以核实数据发现方法的有效性是否至少每 12 个月确认一次。	
这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的** 在非 CDE 内发现明文 PAN 后遵循书面响应程序，有助于确定必要的补救措施并防止未来发生泄漏。 **良好做法** 如果在非 CDE 内发现 PAN，则应进行分析，以 1）确定它是否与其他数据分开保存或与敏感验证数据一起保存，2）确定数据的来源，以及 3）确定导致数据在非 CDE 内的控制差距。 各实体应考虑是否有促成因素，如业务流程、用户行为、不当的系统配置等，导致 PAN 存储在一个意外位置。如果存在这种促成因素，应根据本要求进行处理，以防止再次发生。
A3.2.5.2 实施响应程序，一旦检测到非 CDE 内的明文 PAN 立即启动，包括： • 确定如果在非 CDE 内发现明文 PAN 应该采取的应对措施，包括恢复、安全删除和/或迁移到当前定义的 CDE 中，如适用。 • 确定数据在非 CDE 内的最终结果。 • 补救导致数据在非 CDE 内的数据泄漏或流程漏洞。 • 识别数据的来源。 • 识别磁道数据是否与 PAN 一并存储。	**A3.2.5.2.a** 检查书面响应程序，以核实是否制定了相应流程，以便在检测到非 CDE 内的明文 PAN 作出响应，并包括本要求中规定的所有元素。	
	A3.2.5.2.b 询问相关人员并检查响应行动的记录，以核实在非 CDE 内检测到明文 PAN 时是否执行了补救活动。	
定制方法目标		
这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.2.6 实施各种用于检测和防止明文 PAN 通过未经授权的渠道、方法或程序离开 CDE 的机制，包括以下类型的机制： • 主动运行的机制。 • 被配置为检测和防止明文 PAN 通过未经授权的渠道、方法或程序离开 CDE 的机制。 • 一旦检测到明文 PAN 通过未经授权的渠道、方法或程序离开 CDE 便生成检查日志和警报的机制。 **PCI DSS 参考**：*PCI DSS 要求 12 的范围*	**A3.2.6.a** 检查文件并观察已经实施的机制，以核实这些机制是否符合本要求中规定的所有元素。	使用相应机制，检测和防止未经授权地让 PAN 离开 CDE，有助于组织能够检测和防止可能导致数据丢失的情况。 **良好做法** 这些机制的覆盖范围应包括但不限于，电子邮件、下载到可移动媒体和输出到打印机等。 **示例** 检测和防止明文 PAN 的未经授权丢失的机制可能包括使用适当工具，如数据丢失预防（DLP）解决方案，以及手动过程和程序。
定制方法目标	**A3.2.6.b** 检查检查日志和警报，询问负责人员，以核实是否调查了警报。	
这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.2.6.1 实施响应程序，一旦检测到有人试图通过未经授权的渠道、方法或程序将明文 PAN 移出 CDE 立即启动：响应程序包括： • 负责人员迅速调查警报的程序。 • 补救数据泄漏或流程漏洞（必要时）以防止任何数据损失的程序。 **PCI DSS 参考**：*要求 12*	**A3.2.6.1.a** 检查书面响应程序，以核实响应程序（针对有人试图通过未经授权的渠道、方法或程序将明文 PAN 移出 CDE）包括本要求中规定的所有元素： • 负责人员迅速调查警报的程序。 • 补救数据泄漏或流程漏洞（必要时）以防止任何数据损失的程序。	通过未经授权的渠道、方法或程序来删除明文 PAN 的意图，可能表明存在窃取数据的恶意意图，也可能是不知道或完全没有遵循正确方法的授权员工的行为。及时调查这些情况，可以确定哪些方面需要进行补救并提供宝贵信息，以帮助了解威胁的来源。
定制方法目标	**A3.2.6.1.b** 当检测到明文 PAN 通过未经授权的渠道、方法或流程离开 CDE 时，询问相关人员并检查所采取的行动记录，并核实是否执行了补救活动。	
这项要求不适用于定制方法。		

要求和测试程序		指南
A3.3 将 PCI DSS 纳入到业务正常（BAU）活动中。		
规定的方法要求	**规定的方法测试程序**	**目的**
A3.3.1 及时检测、警报和处理关键安全控制系统故障，包括但不限于以下故障： • 网络安全控制 • IDS/IPS • FIM • 反恶意软件解决方案 • 实体访问控制 • 逻辑访问控制 • 检查日志机制 • 分段控制（如果使用） • 自动的检查日志审核机制。*本项内容在其生效日期前是最佳实践；详情请参考下面的适用性说明。* • 自动代码审核工具（如果使用）。 *本项内容在其生效日期前是最佳实践；详情请参考下面的适用性说明。* **PCI DSS 参考**：*要求 1-12*	**A3.3.1.a** 检查书面政策和程序，核实是否制定了相应程序，以根据本要求规定的所有元素及时检测、警报和处理关键安全控制故障。 **A3.3.1.b** 检查检测和警报程序，询问相关人员，以核实是否实施了本要求中规定的所有关键安全控制的程序，并且关键安全控制每次发生故障时是否都会产生警报。	如果没有及时（尽快）检测、警报和处理关键安全控制故障的正式程序，则可能不会检测到故障，或者在很长一段时间内不会得到解决。此外，如果没有正式的具有时间限制的流程，攻击者将有充足的时间来破坏系统并从 CDE 中窃取帐户数据。 **良好做法** 故障的具体类型可能有所不同，取决于设备系统组件的功能和使用的技术。典型的故障包括系统停止执行其安全功能或不按预期方式运行，如防火墙删除其所有规则或离线。
定制方法目标		
这项要求不适用于定制方法。		

要求和测试程序		指南
适用性说明 *上述内容（自动的检查日志审核机制和自动的代码审查工具（如果使用））在 2025 年 3 月 31 日之前是最佳实践，之后它们将成为 A3.3.1 要求的一部分，并且必须在 PCI DSS 评估中得到充分考虑。*		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.3.1.2 任何关键安全控制系统会在每次故障发生时作出及时响应。响应安全控制系统故障的过程包括： • 恢复安全功能。 • 识别并记录安全故障的持续时间（从开始到结束的日期和时间）。 • 识别并记录故障的原因，包括根本原因，并记录解决根本原因所需的补救措施。 • 识别并解决故障期间出现的任何安全问题。 • 确定是否由于安全故障而需要采取进一步行动。 • 实施控制以防止故障原因再次发生。 • 恢复安全控制监控。 **PCI DSS 参考**：*要求 1-12*	**A3.3.1.2.a** 检查记录的政策和程序并询问相关人员，核实是否制定并实施了相应程序，以根据本要求规定的所有元素及时响应安全控制故障。 **A3.3.1.2.b** 检查记录，核实是否记录了安全控制故障，其中包括： • 识别故障的原因，包括根本原因。 • 安全故障的持续时间（开始和结束的日期和时间）。 • 解决根本原因所需的补救措施的细节。	如果没有快速、有效响应关键安全控制系统的故障警报，攻击者可能会利用这段时间插入恶意软件，获得系统控制权，或窃取实体环境中的数据。 **良好做法** 书面证据（例如，问题管理系统内的记录）应支持应对安全故障的现有流程和程序。此外，工作人员应了解他们在发生故障时的责任。应在书面证据中记录对故障采取的相应行动和应对措施。
定制方法目标		
这项要求不适用于定制方法。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.3.2 至少每 12 个月审核一次硬件和软件技术，以确认它们是否继续满足组织的 PCI DSS 要求。 **PCI DSS 参考**：*要求 2、6、12。*	**A3.3.2.a** 检查记录的政策和程序并询问相关人员，核实是否制定并实施了相应程序，以审核硬件和软件技术，确认它们是否继续满足组织的 PCI DSS 要求。	硬件和软件技术正在不断发展，组织需要了解他们所使用的技术的变化，以及这些技术不断变化所涉及的威胁。对这些技术进行适当审核，确保他们能够准备好应对并管理硬件和软件中的漏洞，而供应商或开发商不会修复这些漏洞。
	A3.3.2.b 审核最近对硬件和软件技术的审核结果，以核实是否至少每 12 个月进行了一次审查。	**良好做法** 组织还应该考虑审核固件版本，以确保它们保持最新并得到供应商的支持。
定制方法目标 这项要求不适用于定制方法。	**A3.3.2.c** 审核文件，以核实对于任何被确定为不再符合组织的 PCI DSS 要求的技术，是否制定了计划来对该技术进行补救。	各组织还需要了解技术供应商对其产品或流程所做的改变，以了解这种改变会如何影响到组织对该技术的使用。 对影响 PCI DSS 控制的技术进行定期审核，可以帮助采购、使用和部署策略，并确保依赖这些技术的控制发挥作用。这些审核包括但不限于审核不再受供应商支持的技术和/或不再满足组织的安全需求的技术。
适用性说明 该过程包括补救不再符合组织的 PCI DSS 要求的技术的计划，酌情包括更换技术。		

要求和测试程序		指南
规定的方法要求	**规定的方法测试程序**	**目的**
A3.3.3 至少每三个月进行一次审核，以核实是否遵循了 BAU 活动。审核由受托负责 PCI DSS 遵从性计划（如 A3.1.3 中确定的）的人员执行，包括： • 确认所有 BAU 活动（包括 A3.2.2、A3.2.6 和 A3.3.1）正在执行。 • 确认相关人员正在遵循安全政策和操作程序（例如，每日日志审核、网络安全控制的规则集审核、新系统的配置标准）。 • 记录审核的完成方式，包括如何核实所有 BAU 活动是否已经到位。 • 按照年度 PCI DSS 评估的要求，收集记录的证据。 • 由 A3.1.3 中确定的受托负责 PCI DSS 遵从性计划的人员审核和签收结果。 • 记录和文件至少保留 12 个月，涵盖所有 BAU 活动。 **PCI DSS 参考**：*要求 1-12*	**A3.3.3.a** 检查政策和程序，核实是否制定了相应程序，以根据本要求中规定的所有元素审核并验证 BAU 活动。 **A3.3.3.b** 询问负责人员，检查审核记录，以核实： • 审核由受托负责 PCI DSS 遵从性计划的人员执行。 • 至少每三个月进行一次审核。	定期确认安全政策和程序是否得到遵守，可以保证预期的控制措施发挥作用，并按预期工作。这些审查的目的不是为了重新执行其他 PCI DSS 要求，而是为了确认安全活动正在持续进行。 **良好做法** 这些审核也可用于核实适当证据是否得到维护—例如，检查日志、漏洞扫描报告、网络安全控制规则集的审核—协助实体准备下一次 PCI DSS 评估。 **示例** 以要求 1.2.7 为例，通过至少每三个月确认一次是否以规定的频率审核了网络安全控制配置来满足要求 A3.3.3。另一方面，通过审核要求中规定的所述配置来满足要求 1.2.7。
定制方法目标		
这项要求不适用于定制方法。		

要求和测试程序		指南
A3.4 控制和管理持卡人数据环境的逻辑访问权限。		
规定的方法要求 **A3.4.1** 至少每六个月审核一次用户帐户和范围内系统组件的访问权限，以确保根据工作职能授权的用户帐户和访问权限依然适当，并授权了所有访问权限。 **PCI DSS 参考**：*要求 7* **定制方法目标** 这项要求不适用于定制方法。	**规定的方法测试程序** **A3.4.1** 询问负责人员并检查支持性文件，以核实： • 是否至少每六个月审核了一次用户帐户和访问权限。 • 根据工作职能指定的访问权限是否适当，是否授权了所有访问权限。	**目的** 定期审核访问权限，有助于发现在用户工作职责变更、系统功能变更或其他修改后剩余的过度访问权限。如果没有适时撤销过度用户权限，恶意用户可能会将其用于未经授权的访问。 这种审核提供了另一个机会，以确保所有离职用户的帐户已被删除（如果在离职时遗漏了任何帐户），以及确保任何不再需要访问的第三方的访问权限已被终止。

要求和测试程序		指南
A3.5 识别并应对可疑事件。		
规定的方法要求	**规定的方法测试程序**	**目的**
A3.5.1 实施一种方法，以迅速识别整个系统的攻击模式和不良行为，包括： • 当异常或可疑活动发生时，对其进行识别。 • 在发现可疑活动或异常情况时，及时向负责人员发出警报。 • 根据记录的响应程序对警报做出响应。 **PCI DSS 参考**：*要求 10、12*	**A3.5.1.a** 检查文件并询问相关人员，核实是否制定并实施了一种方法，以迅速识别整个系统的攻击模式和不良行为，并包括本要求中规定的所有元素。	识别整个系统的攻击模式和不良行为的能力—例如，使用集中管理的或自动的日志相关工具—对于防止、检测或最大限度地减少数据泄露的影响至关重要。所有环境中的日志都允许在出错时进行彻底的跟踪、警报和分析。如果没有相应流程来证实源于关键系统组件和执行安全功能的系统（如网络安全控制、IDS/IPS 和文件完整性监控（FIM）系统）的信息，那么确定泄露的原因就非常困难，甚至是不可能。因此，需要收集、关联和维护所有执行安全功能的关键系统组件和系统的日志。这可能包括使用软件产品和服务方法来提供实时分析、警报和报告，如安全信息和事件管理（SIEM）、FIM 或变化检测。
定制方法目标	**A3.5.1.b** 检查事件响应程序并询问负责人员，以核实： • 值班人员及时收到警报。 • 根据记录的响应程序，对警报做出响应。	
这项要求不适用于定制方法。		

附录 B　补偿性控制

当实体由于合理的书面技术或业务制约因素而无法明确满足一项 PCI DSS 要求，但通过实施其他控制或补偿性控制，充分降低了与该要求相关的风险时，可考虑采取补偿性控制。

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. 提供与原始 PCI DSS 要求类似的防御水平，从而使补偿性控制充分抵消了原始 PCI DSS 要求旨在防御的风险。要了解要求的目的，请参见大部分 PCI DSS 要求的*定制方法目标*。如果一项要求不适用于定制方法，因此没有定制方法目标，请参考该要求指导栏中的**目的**部分。
3. 要“超越”其他 PCI DSS 要求。（仅仅符合其他 PCI DSS 要求并不是补偿性控制。）
4. 在评估补偿性控制的“超越”时，请考虑以下几点：

注： *执行 PCI DSS 评估的评估商必须审核和认证所有补偿性控制是否充分。补偿性控制的有效性取决于实施该控制的环境的具体情况、周围的安全控制以及控制的配置。各实体应了解，并不是每个特定的补偿性控制在所有环境中都有效。*

a. 如果现有的 PCI DSS 要求已被规定用于审核的项目，则不能被视为补偿性控制。例如，非控制台管理访问权限的密码必须加密发送，以减少拦截明文管理密码的风险。实体不能使用其他 PCI DSS 密码要求（入侵者锁定、复杂密码等）来补偿缺乏加密密码的问题，因为这些其他密码要求不能减轻拦截明文密码的风险。此外，其他密码控制已经是审核（密码）项目的 PCI DSS 要求。

b. 如果现有的 PCI DSS 要求是其他领域的要求，但不是审查项目的要求，则可能被视为补偿性控制。

c. 现有的 PCI DSS 要求可以与新的控制措施相结合，成为一种补偿性控制措施。例如，如果一家公司由于供应商尚未提供安全更新而无法解决可通过网络接口利用的漏洞，则补偿性控制可以由包括以下所有的控制措施组成：1）内部网络分段，2）限制对脆弱接口的网络访问权限，只允许必要的设备访问（IP 地址或 MAC 地址过滤），以及 3）IDS/IPS 对通往脆弱接口的所有流量进行监控。

5. 解决不遵守 PCI DSS 要求所带来的额外风险。

6. 解决当前和未来的要求。补偿性控制不能解决过去遗漏的要求（例如，两个季度前要求执行一项任务，但该任务没有执行）。

评估商需要在每个年度 PCI DSS 评估中彻底评估补偿性控制，以确认每个补偿性控制都能充分解决最初 PCI DSS 要求所要解决的风险，见上述第 1-6 项。

为了保持合规性，必须制定流程和控制措施，以确保补偿性控制在评估完成后仍然有效。此外，补偿性控制结果必须记录在评估的适用报告（例如，遵从性报告或自我评估调查问卷）中相应的 PCI DSS 要求部分，并在向请求组织提交适用报告时包括在内。

附录 C　补偿性控制工作表

该实体必须使用此工作表，定义任何要求的补偿性控制，以使用补偿性控制来满足 PCI DSS 要求。请注意，补偿性控制也应根据相应的 PCI DSS 要求部分的遵从性报告中的指示进行记录。

注： *只有那些具备合理的、记录的技术或业务制约因素的实体才能考虑使用补偿性控制来实现合规。*

要求编号和定义：

	所需信息	**解释**
1.　限制	记录妨碍遵从原始要求的合理技术或业务限制。	
2.　补偿性控制的定义	定义补偿性控制：解释它们如何解决原始控制的目标和增大的风险（如有）。	
3.　目标	定义原始控制的目标（例如，定制方法目标）。	
	确定补偿性控制所达到的目标 *（注意：这可以是，但不需要是 PCI DSS 要求的既定"定制方法目标"）*。	
4.　确定的风险	确定因缺乏原始控制而带来的任何额外风险。	
5.　认证补偿性控制	定义认证和测试补偿性控制的方法。	
6.　维护	定义维护补偿性控制的过程和控制措施。	

附录 D　定制方法

这种方法适用于那些决定以不严格遵循所定义的要求的方式来满足 PCI DSS 要求的既定定制方法目标的实体。定制方法允许实体采取战略方法来满足要求的定制方法目标，因此它可以确定和设计所需的安全控制，以满足该组织的独特目标。

实施定制方法的**实体**必须满足以下标准：

- 记录并保存有关每个定制控制的证据，包括附录 E1 中控制矩阵模板中规定的所有信息。
- 对每个定制控制进行并记录目标风险分析（PCI DSS 要求 12.3.2），包括附录 E2 中的目标风险分析模板中规定的所有信息。
- 对每个自定义控制进行测试，以证明其有效性，并在控制矩阵中记录所进行的测试、使用的方法、测试的内容、测试的时间以及测试的结果。
- 监测并保持有关每个自定义控制的有效性的证据。
- 向其评估商提供完整的控制矩阵、目标风险分析、测试证据和定制控制有效性的证据。

对定制控制执行评估的**评估商**必须满足以下标准：

- 审核实体的控制矩阵、目标风险分析和控制有效性的证据，以充分了解定制控制，并核实实体是否符合所有定制方法文件和证据要求。
- 衍生并记录所需的适当测试程序，以便对每个定制控制进行彻底的测试。
- 测试每个定制控制，以确定实体的实施情况是否：1）符合要求的定制方法目标；2）导致要求的“到位”结果。
- 在任何时候，QSA 都保持《QSA 资格要求》中规定的独立性要求。这意味着如果一名 QSA 参与设计或实施定制控制，该名 QSA 不会为该定制控制衍生测试程序、评估或协助评估。

实体和其评估商应共同合作，以确保：1）他们同意定制控制完全满足定制方法目标；2）评估商完全理解定制控制；以及 3）实体理解评估商将执行的衍生测试。

定制方法的使用必须由 QSA 或 ISA 完成，并按照遵从性报告（ROC）模板中的指示和 PCI SSC 网站上提供的 *PCI DSS v4.0 ROC 模板的常见问题*中的指示进行记录。

完成自我评估调查问卷的实体没有资格使用定制方法；但是，这些实体可以选择由 QSA 或 ISA 执行评估，并将其记录在 ROC 模板中。

定制方法的使用可能受到管理遵从性计划的组织（例如，支付品牌和收单机构）的监管。因此，有关使用定制方法的问题必须提交给这些组织，包括，例如，一个实体是否被要求使用 QSA，或可以使用 ISA 来完成通过定制方法的评估。

注：*补偿性控制不是定制方法的一个选项。因为定制方法允许实体确定和设计满足某项要求的定制方法目标所需的控制，实体应有效地实施它为该要求设计的控制，而无需同时实施替代的的补偿性控制。*

附录 E　支持定制方法的样本模板

本附录包含控制矩阵和目标风险分析的示例模板。根据定制方法规定，实体会对示例模板进行记录。这些模板是可以使用的格式范例。*虽然并不要求实体遵循本附录中提供的具体格式，但实体的控制矩阵和目标风险分析必须包括这些模板中定义的所有信息。*

E1 控制矩阵模板样本

以下是一个控制矩阵模板样本，实体可以用它来记录他们的定制实施。

如*附录 D 中*所述：*自定方法*，使用自定方法的实体必须完成控制矩阵，为每个实施的控制提供详细信息，解释实施的内容、实体如何确定控制满足 PCI DSS 要求的既定目标、控制如何提供至少与满足定义的要求同等的保护水平，以及实体如何持续保证控制的有效性。

评估商使用每个控制矩阵中的信息来计划和准备评估。

该控制矩阵模板样本包括实体需要记录并提供给评估商进行定制验证的最低限度信息。虽然并不要求使用这个特定模板，但要求实体的定制方法文件包括本模板中定义的所有信息，实体也需要向其评估商提供这些确切的信息。

控制矩阵并不能取代评估商独立开发适当的测试程序以验证已实施的控制的需要。 评估商仍然必须执行所需的测试，以验证控制是否符合要求的目标，是否有效，以及是否得到适当维护。控制矩阵也不能取代 ROC 模板中规定的自定认证的报告要求。

控制矩阵必须至少包括下表信息。

通过定制方法满足的 PCI DSS 要求的控制矩阵模板样本 由接收评估的实体完成		
定制控制的名称/标识符	<实体定义他们希望如何提及此控制>	
PCI DSS 要求的编号和通过此控制实现的目标	要求#： 要求#：	目标： 目标：

通过定制方法满足的 PCI DSS 要求的控制矩阵模板样本 由接收评估的实体完成	
控制的细节	
什么是已实现的控制？	<实体描述该控制是什么以及它的作用>
何地实施控制？	<实体确定实施和管理控制的设施和系统组件的位置>
何时执行控制？	<实体详细说明了控制的执行频率 – 例如，实时连续运行或计划在 NN 时间和 XX 间隔内运行>
谁对该控制负有全面责任和义务？	<实体包括对该控制负有责任和义务的个别人员/角色的详细信息>
谁参与管理、维护和监控该控制？	<实体包括管理、维护和监控该控制的个别人员/角色和/或团队（如适用）的详细信息>
对于用于控制的*每个*PCI DSS 要求，实体提供以下细节：	
实体描述已实施的控制如何满足 PCI DSS 要求的既定***定制方法目标。***	<实体描述了控制如何满足 PCI DSS 要求的既定定制方法目标，并总结了相关结果>
实体描述了**它所执行**的测试和测试结果，证明该（些）控制符合适用要求的目标。	<实体描述了其为证明控制符合 PCI DSS 要求的既定目标而执行的测试，并总结了相关结果>

通过定制方法满足的 PCI DSS 要求的控制矩阵模板样本 由接收评估的实体完成	
实体简要说明了**它所执行**的单独目标风险分析的结果，该分析解释了所实施的控制，并说明结果如何核实该控制是否至少提供了与适用 PCI DSS 要求中定义的方法同等的保护水平。*关于如何记录该风险分析的详细信息，请参见单独目标风险分析模板。*	<实体简要描述了该控制风险分析的结果，该结果另在目标风险分析中详细说明>
实体描述了**它所实施**的措施，以确保该（些）控制得到维持，其有效性得到持续保证。*例如，实体如何监测控制的有效性，如何检测和应对控制故障，以及所采取的行动。*	<实体描述了如何确保控制得到维护以及如何保证控制的有效性。>

E2 目标风险分析模板样本

以下是某实体可用于其定制实施的目标风险分析模板样本。*虽然并不要求实体遵循这一特定格式，但其定制方法文件必须包括该模板中定义的所有信息。*

如*附录 D 中*所述：*自定方法*，根据 PCI DSS 要求 12.3.2，使用自定方法的实体必须为该实体通过自定义方法满足的每项要求提供详细的目标风险分析。风险分析定义了风险，评估了如果未满足定义要求对安全的影响，并描述了该实体如何确定控制至少提供了与定义的 PCI DSS 要求同等的保护水平。

评估商使用目标风险分析中的信息来计划和准备评估。

完成定制方法的目标风险分析后，务必记住：

- 被保护资产是由该实体存储、处理或传输的持卡人数据。
- 威胁行为者具有高度的动机和能力。威胁行动者的动机和能力往往会随着成功攻击的持卡人数据量而增加。
- 当某实体存储、处理或传输更多的持卡人数据时，该实体成为威胁行动者目标的可能性就会增加。
- 伤害与目标直接相关。例如，如果目标是“恶意软件不能执行”，那么伤害就是恶意软件执行；如果目标是“分配执行所有活动的日常责任”，那么伤害就是没有分配责任。

注：本目标风险分析中使用的术语“伤害”（例如，下表中的1.3）是指对实体的安全状况产生负面影响的事情或事件。例子包括：没有制定政策，没有执行漏洞扫描，或者恶意软件在实体的环境中执行。

该目标风险分析模板样本包括实体需要记录并提供给评估商进行定制验证的最低限度信息。虽然并不要求使用这个特定模板，但要求实体的定制方法文件包括本模板中定义的所有信息，实体也需要向其评估商提供这些确切的信息。

目标风险分析必须至少包括下表信息。

通过定制方法满足 PCI DSS 要求的目标风险分析样本 由接收评估的实体完成	
项目	**细节**
1.识别该要求	
1.1 确定 PCI DSS 的书面要求。	<实体识别了要求>
1.2 确定 PCI DSS 书面要求的目标。	<实体确定了要求的目标>

通过定制方法满足 PCI DSS 要求的目标风险分析样本 由接收评估的实体完成	
项目	**细节**
1.3 描述该要求旨在防止的伤害	<实体描述了伤害> <实体描述了如果实体没有成功达到目标，对安全产生的影响> <实体描述了如果实体没有成功达到目标，不会存在哪些安全基本元素，或者威胁行为者可能会采取什么行动。
2.描述拟议的解决方案	
2.1 自定控制的名称/标识符	<实体识别了定制控制，就像记录于控制矩阵中的那样。>
2.2 在拟议的解决方案中，哪些书面要求部分会发生变化？	<实体确定定义的方法不会满足哪些要求的元素，因此将被定制方法所覆盖。这些元素可能很小，但足以改变某个要求的周期，或实施一个完全不同的控制集合来满足目标。>
2.3 拟议的解决方案将如何防止伤害的发生？	<实体描述了控制矩阵中详述的控制将如何防止 1.3 中确定的伤害。>

通过定制方法满足 PCI DSS 要求的目标风险分析样本 由接收评估的实体完成						
项目	**细节**					
3.分析发生伤害的可能性而导致持卡人数据的机密性遭到破坏的任何变化。						
3.1 描述控制矩阵中详述的影响伤害发生的可能性的因素。	实体描述： • 控制如何成功地防止伤害的发生 • 控制矩阵中详述的控制如何降低伤害发生的可能性					
3.2 描述在应用定制控制后伤害仍可能发生的原因。	实体描述： • 控制失败的典型原因，发生的可能性，以及如何能够防止这种情况的发生 • 实体的流程和系统在检测控制未正常运行方面的弹性如何？ • 威胁行动者如何绕过该控制 – 他们需要采取什么步骤，困难程度，威胁行动者是否会在控制失效前被发现？如何确定这一点？					
3.3 与定义的方法要求相比，定制方法中详述的控制在多大程度上代表了伤害发生的可能性的变化？	发生伤害 的可能性更高	☐	没有变更	☐	发生伤害 的可能性更低	☐
3.4 提供理由，说明为何必须对定制控制到位后发生伤害的可能性的变化进行评估。	实体提供： • 记录在 3.3 中的评估理由。 • 记录在 3.3 中的评估标准和价值。					

通过定制方法满足 PCI DSS 要求的目标风险分析样本 由接收评估的实体完成				
项目	**细节**			
4.分析对未经授权访问帐户数据的影响的任何变化				
4.1 对于本解决方案所涵盖的系统组件范围，如果解决方案失败，有多少数量的帐户数据会面临未经授权访问的风险？	**4.1.1** 已存储 PAN 的数量	*任何时候的最大值*	**4.1.2** 在 12 个月内已处理或已传输 PAN 的数量	*总数*
4.2 描述定制控制将如何直接： • 如果威胁行动者成功，减少遭到威胁的个人 PAN 的数量，和/或 • 允许在更快时间内向支付卡品牌通知 PAN 遭到威胁的情况。	对支付生态系统的影响直接关系到遭到威胁的帐户数量以及发卡机构如何快速阻止任何遭到威胁的 PAN。 如果有任何定制控制，实体描述定制控制如何实现以下目标： • 减少存储、处理或传输的持卡人数据量，从而减少落在成功威胁行动者的数据，和/或 • 减少检测、通知受损帐户和遏制威胁行为者的时间。			
5.风险批准和审核				
5.1 我已经审核了上述风险分析，我同意使用所述的拟议定制方法，至少可以提供与适用的 PCI DSS 要求中定义的方法同等的保护水平。	行政管理部门的一名成员必须审核并同意拟议的定制方法。 <实体的执行管理部门成员签署其审核并同意此处记录的定制方法。>			
5.2 该风险分析必须在不晚于以下时间进行审核和更新：	风险分析应至少每十二个月审核一次，如果定制方法本身设有时间限制（例如，因为对技术的计划性变更），或者其他因素决定了需要变更，则应更频繁地审核。如果发生不定期的风险审核，详细说明审核发生的原因。 <实体说出审查和更新目标风险分析的日期。>			

附录 F　利用 PCI 软件安全框架以支持要求 6

PCI DSS 要求 6 定义了开发和维护安全系统和软件的要求。由于 PCI SSC 安全软件标准和安全 SLC 标准（统称为软件安全框架）包括严格的软件安全要求，使用按照这两个标准开发和维护的订制和定制软件可以帮助实体满足 PCI DSS 要求 6 中的若干要求，而无需执行所述的额外测试，并且还可以支持使用其他要求的自定义方法。详情请见表 7。

***注：**这种满足要求 6 的支持仅适用于根据安全软件标准或安全 SLC 标准专门开发和维护的软件；它不扩展到要求 6 范围内的其他软件或系统组件。*

表 7。利用 PCI 软件安全框架以支持要求 6

PCI DSS 要求	PCI DSS 要求如何适用于按照安全软件标准开发和维护的软件	PCI DSS 要求如何适用于按照安全 SLC 标准开发和维护的软件
6.1 定义并理解执行要求 6 中活动的流程和机制。	PCI DSS 要求/目标照常适用。	
6.2 安全开发订制和定制软件。	对于按照安全软件标准开发和维护的软件，可视为 PCI DSS 要求 6.2.4 已经到位。	对于按照安全 SLC 标准开发和维护的软件，可视为 PCI DSS 要求 6.2 已经到位。
6.3 识别并及时解决安全漏洞。	PCI DSS 要求/目标照常适用。 按照安全 SLC 标准开发和维护的软件可以支持要求 6.3 目标的定制方法。 虽然使用按照安全 SLC 标准开发和维护的软件可以保证供应商及时提供安全补丁和软件更新，但**实体仍有责任**确保按照 PCI DSS 要求安装补丁和更新。	
6.4 保护面向公众的 Web 应用程序免于攻击。	PCI DSS 要求/目标照常适用。	

PCI DSS 要求	PCI DSS 要求如何适用于按照安全软件标准开发和维护的软件	PCI DSS 要求如何适用于按照安全 SLC 标准开发和维护的软件
6.5 安全管理所有系统组件变更。	PCI DSS 要求/目标照常适用。 按照安全 SLC 标准开发和维护的软件可能支持要求 6.5 目标的定制方法。 虽然使用按照安全 SLC 标准开发和维护的软件可以保证供应商在开发软件和相关更新期间遵循变更管理程序，**但实体仍有责任**确保按照 PCI DSS 要求将软件和系统组件的其他变更实施到其生产环境中。	

*使用由合格的 **SLC** 安全性供应商开发和维护的定制和定制软件*

认证使用由合格的 SLC 安全性供应商开发和维护的软件以满足 PCI DSS 要求 6.2 支持要求 6.3 和 6.5 的定制方法时，评估商必须确认满足以下条件：

- 该软件供应商在 PCI SSC 合格的 SLC 安全性供应商名单上有一个最新的列表，也就是说，认证没有过期。
- 该软件的开发和维护采用了作为软件供应商认证的一部分而评估的软件寿命周期管理做法。
- 该实体正在遵循合格的 SLC 安全性供应商提供的实施指南。

*使用按照 **SLC** 安全性标准开发的订制和定制软件*

内部开发仅用于自身的软件或开发供单一实体使用的软件的实体可选择聘请 SLC 安全性评估商，根据 SLC 标准评估其软件生命周期管理做法。SLC 安全性评估商将在安全 SLC 遵从性报告（ROC）和 SLC 安全性合规证明书（AOC）中记录评估结果。

按照软件寿命周期管理方法开发和维护的软件与由合格的 SLC 安全性供应商开发和维护的软件一样，为 PCI DSS 要求 6 提供相同程度的支持，如果这些方法由 SLC 安全性评估商评估并确认符合 SLC 安全性标准要求，并将结果记录在 SLC 安全性 ROC 和 安全 AOC 中。

认证 SLC 安全性标准的使用

当认证使用按照 SLC 安全性标准开发和维护的软件以满足 PCI DSS 要求 6.2 并支持要求 6.3 和 6.5 的定制方法时，评估商必须确认满足以下条件：

- 软件寿命周期管理实践由 SLC 安全性评估商评估，并确认符合所有 SLC 安全性标准要求，评估结果记录在 SLC 安全性遵从性报告（ROC）和 SLC 安全性合规证明书（AOC）中。
- 该软件的开发和维护采用了 SLC 安全性评估所涵盖的软件寿命周期管理实践。
- 针对软件寿命周期管理实践的全面 SLC 安全性评估是在过去 36 个月内完成的。此外，如果最近一次全面 SLC 安全性评估是在 12 个月前进行的，则开发商/供应商在过去 12 个月内提供了一份年度证明书，确认在使用的软件寿命周期管理实践中继续遵守 SLC 安全性标准。

认证安全软件标准的使用

当认证使用按照安全软件标准开发和维护的软件以满足 PCI DSS 要求 6.2.4 并支持要求 6.3 和 6.5 的定制方法时，评估商必须确认满足以下条件：

- 安全软件评估由安全软件评估商进行，并确认符合安全软件标准的所有要求，其结果记录在安全软件认证报告（ROV）和安全软件认证证明（AOV）中。
- 该软件的开发和维护采用了安全软件评估中所涵盖的软件寿命周期管理方法。
- 全面的安全软件评估是在过去 36 个月内完成的。此外，如果近期的全面安全软件评估是在 12 个月之前进行的，则开发商/供应商在过去 12 个月内提供了一份年度证明书，确认继续遵守安全软件标准。

附录 G　PCI DSS 术语、缩略语和缩写词汇表

术语	定义
帐户	也被称为“用户 ID”、“帐户 ID”或“应用 ID”。 用于识别计算机系统中的个人或进程。参见*验证凭证*和*验证因素*。
帐户数据	帐户数据由持卡人数据和/或敏感验证数据组成。参见*持卡人数据*和*敏感验证数据*。
收单机构	也被称为“商户银行”、“收单银行”或“收单金融机构”。 收单机构是为商户处理支付卡交易的实体，通常为金融机构，由支付品牌定义。收单机构须遵从有关商户遵从性的支付品牌规则和程序。参见*支付处理商*。
管理权限	为使某帐户能够管理系统、网络和/或应用程序而赋予的升级或更高权限。 管理权限可以分配给个人的帐户或内置系统帐户。拥有管理访问权限的帐户通常被称为“超级用户”、“根用户”、“管理员”、“系统管理员”或“主管状态”，根据具体的操作系统和组织结构而定。
AES	“高级加密标准”的缩写。 参见*强效加密法*。
ANSI	“美国国家标准协会”的缩写。
反恶意软件	旨在检测、删除、阻止或遏制各种形式的恶意软件的软件。
AOC	“遵从性证明书”的缩写。 AOC 是商户和服务提供商用于证明 PCI DSS 评估结果的表格，记录于自我评估调查问卷或遵从性报告。
应用程序	包括所有购买和定制和订制的软件程序或程序组，包括内部和外部（例如 web）应用程序。
应用程序和系统帐户	也被称为“服务帐户”。 在计算机系统或应用程序中执行进程或执行任务的帐户。这些帐户通常具有执行专门任务或功能所需的更高权限，通常不是个人使用的帐户。
ASV	“授权扫描供应商”的缩写。 由 PCI SSC 授权可执行外部漏洞扫描服务的公司。
检查日志	也称为“检查记录” 系统活动的序时记录。提供独立可核实的记录，可用于重建、审核和检查从交易启动到获得最终结果过程中的一系列围绕或导致操作、程序或事件的环境和活动。

术语	定义
验证	核实个人、设备或程序的身份的过程。验证通常会有一个或多个验证因素。参见*帐户*、*验证凭证*、和*验证因素*。
验证凭证	用户 ID 或帐户 ID 以及用于验证个人、设备或流程身份的验证因素相结合。参见*帐户*和*验证因素*。
验证因素	用于证明或核实计算机系统中的个人或进程身份的元素。通常通过使用一个或多个验证因素进行验证。 • 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。 ID（或帐户）和验证因素合称为验证凭证。”参见*帐户*和*验证凭证*。
授权	就访问控制而言，授权是将访问权限或其他权限授予用户、程序或流程。授权定义了个人或程序在成功验证后可进行的操作。 就支付卡交易而言，授权是指授权过程，当商家收到交易响应（例如，授权或拒绝）时，授权过程即完成。
BAU	“常规业务”的缩写。
订制和定制软件	*订制软件*是由第三方代表实体并按照该实体的规格为其开发。 *定制软件*由实体开发供其自己使用。
读卡器	一种物理设备，通常连接到合法的读卡设备，用于非法捕获和/或存储支付卡中的信息。
卡验证代码	也称为卡认证代码或值，或者卡安全代码。就 PCI DSS 而言，它是印在支付卡正面或背面的三位或四位数的数值。根据各个参与的支付品牌，可能称为 CAV2、CVC2、CVN2、CVV2 或 CID。更多信息，请联系参与的支付品牌。
持卡人	支付卡发给的客户或者任何被授权使用支付卡的个人。
持卡人数据（CHD）	持卡人数据至少包含完整 PAN。持卡人数据还可能以完整 PAN 加上以下任何信息的形式显示：持卡人姓名、失效日和/或业务码 关于可能在支付交易中传输或处理（但不存储）的其他数据元素，请参见*敏感验证数据*。

术语	定义
CDE	“持卡人数据环境”的缩写。 CDE 由以下部分组成： • 存储、处理或传输持卡人数据或敏感验证数据的系统组件、人员和流程，和/或 • 可能不存储、处理或传输 CHD/SAD 的系统组件，但它们可以不受限制地连接到那些存储、处理或传输 CHD/SAD 的系统组件。
CERT	“计算机应急响应小组”的缩写。
变更控制	审核、测试和批准系统和软件变更以便在实施前施加影响的流程和程序。
CIS	“互联网安全中心”的缩写。
明文数据	未加密的数据。
列级 数据库加密	用于加密的技巧或技术（软件或硬件），加密内容为数据库中的特定列内容，而不是整个数据库的全部内容。或者，请参见*磁盘加密*和*文件级加密*。
商用现成品或技术（COTS）	描述非专门为特定客户或用户定制或设计的库存物品，并可随时使用的产品。
补偿性控制	参见 *PCI DSS* 中的附录 B 和 C。
威胁	也称为“数据威胁”或“数据漏洞” 对计算机系统的入侵，其中涉嫌持卡人数据的非授权披露/盗窃、修改或销毁。
控制台	允许访问和控制服务器、大型机或其他系统类型的直接连接的屏幕和键盘。参见*非控制台访问*。
消费者	购买商品、服务或商品和服务的个别持卡人。
关键系统	实被实体视为特别重要的系统或技术。例如，关键系统可能对于企业经营的业绩或安全功能的维护至关紧要。关键系统往往包括安全系统、面向公众的设备和系统、数据库以及存储、处理或传输持卡人数据的系统。
加密算法	也称为“加密的算法”。 用于将明文数据转换为加密数据并复原的明确规定的可逆数学过程。参见*强效加密法*。

术语	定义
密钥	与加密算法一起使用的参数。该参数用于诸如以下操作： • 将明文数据转换为密文数据、 • 将密文数据转化为明文数据、 • 根据数据计算出来的数字签名、 • 核实根据数据计算出来的数字签名、 • 根据数据计算出来的验证代码，或 • 一个共享秘密的交换协议。 参见*强效加密法*。
密钥生成	密钥生成是密钥管理中的职能之一。下列文件提供了关于适当密钥生成的公认指导： • *NIST 特别出版物 800-133：密钥生成建议* • *ISO 11568-2 金融服务 — 密钥管理（零售） — 第 2 部分：对称密文，其密钥管理和生命周期* – 4.3 密钥生成 • *ISO 11568-4 金融服务 — 密钥管理（零售） — 第 4 部分：非对称密码系统 — 密钥管理和生命周期* – 6.2 密钥寿命周期阶段 — 生成 • *欧洲支付委员会 EPC 342-08 关于算法使用和密钥管理的指导* – 4.1.1 密钥生成 [对称算法] – 4.2.1 密钥生成 [非对称算法]。
密钥管理	支持密钥建立和维护（包括在必要时使用新密钥替换旧密钥）的流程和机制集合。
密钥周期	密钥可用于指定目的的时间段。通常基于密钥的有效期限和/或密钥产生的密文量并且符合行业最佳实践和指南（例如，*NIST 特别出版物 800-57*）进行定义。
定制方法	参见 PCI DSS 章节：8 实施和认证 PCI DSS 的方法。
CVSS	“通用漏洞评分系统”的缩写。 更多信息，请参见*《ASV 计划指南》*。

术语	定义
数据流程图	显示数据在应用程序、系统或网络间的流动方式的图表。
默认帐户	系统、应用程序或设备中预定义的登录帐户，允许系统首次交付使用后的初次访问。系统也可能在安装流程中生成其他默认帐户。
默认密码	系统、应用程序或设备中预定义的关于系统管理员、用户或服务帐户的密码；通常与默认帐户相关。默认帐户和密码会对外发布，因此很容易猜出。
规定的方法	参见 PCI DSS 章节：8 实施和认证 PCI DSS 的方法。
磁盘加密	用于加密所有存储在设备（例如硬盘或闪存驱动器）上的数据的技巧或技术。或者，使用文件级加密或列级数据库加密特定文件或列的内容。
DMZ	“非军事区”的缩写。 为组织的内部专用网络提供其他安全层的物理或逻辑子网络。
DNS	“域名系统”的缩写。
双重控制	需要两个或更多的单独实体（通常是个人）共同操作以便保护敏感功能或信息的流程。两个实体共同负责存在漏洞的交易中相关材料的物理保护。不允许单独的个人访问或使用材料（例如密钥）。对于手动密钥生成、转易、加载、存储和恢复，双重控制需要在实体之间分割密钥知识。另请参见*分割知识*。
ECC	“椭圆曲线加密法”的缩写 请参见*强效加密法*。
电子商务（网络）重定向服务器	在电子商务交易期间将客户浏览器从商户的网站重定向到不同位置以进行支付处理的服务器。
加密	通过加密算法以产生密文（即隐藏数据的信息内容）的数据（可逆）转换流程。请参见*强效加密法*。
加密算法	请参见*加密算法*。
实体	用于表示正在接受 PCI DSS 审查的公司、组织或企业的术语。
文件完整性监控(FIM)	检查关键文件是否出现变更、增加和删除并在检测到这种变更时发出通知的变更检测解决方案。

术语	定义
文件级加密	用于加密特定文件的全部内容的技巧或技术（软件或硬件）。或者，请参见*磁盘加密*和*列级数据库加密*。
防火墙	阻止非授权访问网络资源的硬件和/或软件技术。防火墙会根据规则和其他标准的集合允许或阻止不同安全级别的网络间的计算机流量。
取证	也称为“计算机取证”。 它涉及信息安全，包括应用调查工具和分析技术从计算机资源中收集证据以确定数据遭受威胁的原因。 支付数据泄露事件通常由 PCI 取证调查员（PFI）调查。
FTP	“文件传输协议”的缩写。 用于将数据通过公共网络（例如互联网）从一台计算机传输到另一台计算机的网络协议。一般认为 FTP 是非安全协议，因为密码和文件内容是在无保护的情况下以明文形式发送的。FTP 可通过 SSH 或其他技术安全实施。
散列	一种通过将数据转换为固定长度的消息摘要的数据保护方法。散列是单向（数学）函数，其中非秘密算法会将任一任意长度的消息作为输入，生成固定长度的输出（通常称为“散列代码”或“消息摘要”）。散列函数应具备以下特性： • 只知道散列代码，通过计算不可能确定原始输入， • 通过计算不可能找到散列代码相同的两个输入。
HSM	“硬件安全模块”或“主机安全模块”的缩写。 物理和逻辑上受保护的硬件设备，会提供加密服务的安全集合以用于密钥管理函数和/或帐户数据的解密。
IDS	“入侵检测系统”的缩写。
索引令牌	对应于给定 PAN 的随机值表中的随机值。
交互式登录	个人提供验证凭证以直接登录到一个应用程序或系统帐户的流程。
IPS	“入侵防御系统”的缩写。
ISO	“国际标准化组织”的缩写。
发卡机构	也被称为“发卡银行”或“发卡金融机构”。 发行支付卡或者提供、促进或支持发卡服务的实体，包括但不限于发卡银行和发卡处理机构。
发卡服务	发卡服务包括但不限于授权和卡片个性化等。

术语	定义
加密散列	结合随机生成的秘密密钥以提供抗蛮力攻击和秘密验证完整性的散列函数。 适当的加密散列算法包括但不限于：HMAC、CMAC 和 GMAC，其有效加密强度至少为 128 位（*NIST SP 800-131Ar2*）。 关于 HMAC、CMAC 和 GMAC 的更多信息，请参考以下内容：*NIST SP 800-107r1*、*NIST SP 800-38B* 和 *NIST SP 800-38D*）。 *请参见 NIST SP 800-107（修订版 1）：对使用授权散列算法的应用程序的建议§5.3。*
密钥保管人	受委并负责代表某个实体履行涉及秘密和/或私人密钥、密钥份额或密钥组件的密钥管理职责的角色。
密钥管理系统	提供一种综合方法以生成、分发和/或管理设备和应用程序加密密钥的硬件和软件组合。
LAN	“局域网”的缩写。
LDAP	“轻量级目录访问协议”的缩写。
最小权限	执行工作职能的角色和责任所需的最低权限水平。
日志	见*检查日志*。
逻辑访问控制	限制信息或信息处理资源只提供给授权人或应用程序的机制。请参见*物理访问控制*。
MAC	在加密法中，是“信息验证代码”的缩写。请参见*强效加密法*。
磁条数据	请参见*磁道数据*。
掩盖	显示或打印时隐藏 PAN 分段的方法。查看完整的 PAN 没有业务要求时使用掩盖。掩盖与显示在屏幕、纸质收据、打印件等时的 PAN 保护有关。 关于以电子方式存储、处理或传输时 PAN 的保护，请参见*截词*。
媒体	物理材料，包括但不限于电子存储设备、可移动电子媒体和纸质报告。

术语	定义
商户	在 PCI DSS 中，商户被定义为接受带有任何 PCI SSC 参与支付品牌徽标的支付卡作为商品和/或服务付款的任何实体。 接受支付卡作为商品和/或服务付款的商户也可以是一个服务提供商，如果出售的服务导致代表其他商户或服务提供商存储、处理或传输持卡人数据。例如，ISP 是一个接受支付卡按月计费的商户，但如果它把商户作为客户托管，它也是一个服务提供商。
MO/TO	“邮件订单/电话订单”的缩写。
多因素验证	通过认证至少两个因素验证用户身份的方法。这些因素包括用户所有（例如智能卡或加密狗），用户所知（例如密码、口令或 PIN）或者用户特征或用户所为（例如指纹或其他类型的生物特征）。
多租户服务提供商	一种提供各种共享服务给商户和其他服务提供商，以便客户共享系统资源（如物理或虚拟服务器）、基础设施、应用程序（包括软件即服务（SaaS））和/或数据库的第三方服务提供商。服务可能包括但不限于在一个共享服务器上托管多个实体，提供电子商务和/或"购物车"服务，基于网络的托管服务，支付应用程序，各种云应用程序和服务，以及与支付网关和处理器的连接。请参见*服务提供商*和*第三方服务提供商*。
NAC	“网络访问控制”的缩写。
NAT	“网络地址转换”的缩写。
网络连接	设备之间的一个逻辑、物理或虚拟通信路径，允许传输和接收网络层数据包。
网络图	显示联网环境内系统组件和连接的图表。
网络安全控制 (NSC)	作为网络政策执行点的防火墙和其他网络安全技术。NSC 通常根据预先定义的策略或规则，控制两个或多个逻辑或物理网段（或子网）之间的网络流量。
NIST	“国家标准与技术研究所”的缩写。 美国商务部技术管理内部的无管理联邦机构。
非控制台访问	指的是对系统组件的逻辑访问，通过网络接口（而不是通过直接的物理连接）连接到系统组件上。非控制台访问包括通过本地/内部网络进行的访问，也包括通过外部或远程网络进行的访问。
NTP	“网络时间协议”的缩写。

术语	定义
组织独立性	确保执行活动的个人或部门与评估活动的个人或部门之间没有利益冲突的组织结构。例如，执行评估的个人有组织地与正在评估环境的管理工作分离。
OWASP	“开放式网络应用程序安全项目”的缩写。
PAN	“主帐户号”的缩写。 识别发卡机构和持卡人帐户的唯一支付卡号（信用卡、借记卡或预付卡等）。
密码/口令	作为用户或帐户的验证因素的一串字符。
补丁	更新为现有软件以添加功能或修正缺陷。
参与的支付品牌	也称为“支付品牌”。 截至相关时间，根据 PCI SSC 的管理文件当时被正式接纳为（或附属于）PCI SSC 成员的支付卡品牌。在撰写本文时，参与支付品牌包括 PCI SSC 的创始成员和战略成员。
支付品牌	拥有品牌支付卡或其他支付卡形式因素的组织。支付品牌对带有其品牌或徽标的支付卡或其他形式因素的使用地点和方式进行监管。支付品牌可以是 PCI SSC 的参与支付品牌或其他全球或区域支付品牌、计划或网络。
支付卡形式因素	包括实体支付卡以及具有模拟支付卡功能以启动支付交易的设备。这类设备包括但不限于智能手机、智能手表、健身手环、密钥标签和可穿戴设备（如珠宝）等。
支付卡	就 PCI DSS 而言，任何带有任何 PCI SSC 参与支付品牌徽标的支付卡形式。
支付渠道	商户用于接受客户付款的方法。常见支付渠道包括实体信用卡（实体）和虚拟信用卡（电子商务和 MO/TO）。
支付页面	包含一个或多个表单元素以从消费者获取帐户数据或提交所获取帐户数据的网络用户界面。支付页面可以以下任何一种方式呈现： • 单一文件或实例， • 显示在非支付页面内内联框架中的文件或组件。 • 多个文档或组件，每个包含一个或多个表单元素，包含在一个非支付页面内的多个内联框架中。
支付页面脚本	支付页面上由消费者的浏览器处理和/或解释的任何编程语言命令或指令，包括与页面的文档对象模型互动的命令或指令。编程语言包括 JavaScript 和 VB 脚本等；标记语言（例如，HTML）或样式规则（例如，CSS）均不属于编程语言。

术语	定义
支付处理商	也称为“支付网关”或“支付服务提供商（PSP）”。 由商户或其他实体聘请以代表他们处理支付卡交易的实体。请参见*收单机构*。
PCI DSS	“支付卡行业数据安全标准”的缩写
人员	负有责任保护帐户数据安全或可能影响帐户数据安全的全职和兼职雇员、临时雇员、承包商和顾问。
物理访问控制	限制只有授权人员才能进入物理空间或环境的机制。请参见见*逻辑访问控制*。
PIN	“个人识别码”的缩写
PIN 数据块	处理过程中用于压缩 PIN 的数据块。PIN 数据块格式定义了 PIN 数据块的内容以及用于恢复 PIN 的处理方式。PIN 数据块包括 PIN 和 PIN 长度，还可能包含 PAN （或其截词），这取决于所使用的 ISO PIN 数据块格式的批准情况。
POI	“交互点”的缩写，从卡中读取数据的起点。
销售点系统 (POS)	商户用于接受客户付款的硬件和软件。可能包括 POI 设备、PIN 输入器、电子收银机等。
特权用户	拥有的权限超出基本访问权限的所有用户帐户。一般而言，这些帐户享有较高和较多的特权，比标准用户帐户拥有更多权利。但是不同特权帐户的特权范围差异很大，具体取决于组织、工作职能或角色以及使用的技术。
QIR	“合格的集成商或经销商”的缩写 更多信息，请参见 PCI SSC 网站上的*《QIR 计划指南》*。
QSA	“合格安全性评估商”缩写。 QSA 经由 PCI SSC 授予执行 PCI DSS 现场评估的资格。关于 QSA 公司和员工要求的详情，请参见*《QSA 资格要求》*。
远程访问	从实体的网络外部位置访问电脑网络。VPN 就是一种远程访问技术。
可移动电子媒介	存储数字化数据的媒介，可轻松从一个计算机系统移动和/或传输到另一个。可移动电子媒介包括 CD-ROM、DVD-ROM、USB 闪存驱动器和外部/便携式硬盘等。因此，可移动电子媒介不包括热插拔驱动器、用于批量备份的磁带驱动器，或其他通常不用于将数据从一个位置传输到另一个位置使用的媒介。
风险评估	识别有价值的系统资源和威胁的企业流程。根据估算的频率和产生的成本量化损失暴露风险（即可能导致的损失）；以及（可选）建议如何分配用于应对的资源以最大限度地降低总暴露风险。请参见*目标风险分析*。

术语	定义
风险等级	分类风险以识别、优先考虑并按重要性顺序处理项目的流程。
ROC	“遵从性报告”的缩写。 用于记录实体的 PCI DSS 评估的详细结果的报告工具。
RSA	用于公钥加密的算法。请参见*强效加密法*。
SAQ	“自我评估调查问卷”的首字母缩写。 用于记录某实体的 PCI DSS 评估中自我评估结果的报告工具。
范围界定	要包含在 PCI DSS 评估中的所有系统组件、人员和流程的识别流程。请参阅 PCI DSS 章节：4 PCI DSS 要求的范围。
安全编码	创建和实施应用程序以防止被篡改和/或遭受威胁的流程。
安全事件	组织认为对于系统或其环境而言存在潜在安全隐患的事件。就 PCI DSS 而言，安全事件会识别可疑或异常活动。
安全人员	负责实体安全的主要人员。
分段	也称为“网络分段”或“隔离”。 网络分段可将存储、处理或传输持卡人数据的系统组件与其他无法执行此类操作的系统隔离开来。请参见 *PCI DSS 章节：4 PCI DSS 要求的范围*中的“网络分段”部分。
敏感区域	敏感区域通常是 CDE 的一个子集，是任何对 CDE 至关重要的系统所在区域。这包括数据中心、服务器室、零售地点的后台机房，以及任何集中或聚集了持卡人数据存储、处理或传输的区域。敏感区域还包括管理或维护 CDE 安全的系统所在区域（例如，那些提供网络安全控制或管理物理或逻辑安全的系统）。 这不包括仅有销售点终端的区域，例如零售店的收银区或代理接受付款的呼叫中心。
敏感验证数据（SAD）	用于验证持卡人身份和/或授权支付卡交易的安全相关信息这些信息包括但不限于卡认证代码/值、全磁道数据（磁条数据或芯片上的等效数据）、PIN 和 PIN 数据块。
职责分离	为不同的个人划分职能，以确保单独的个人无法破坏流程的方法。
业务码	磁条中的三位或四位值，位于磁道数据上的支付卡失效日之后。业务码用途多样，可用于定义服务属性、区分国际和国内交换或识别使用限制等。

术语	定义
服务提供商	并非支付品牌的企业实体，代表其他实体直接参与持卡人数据的处理、存储或传输。这包括支付网关、支付服务提供商（PSP）和独立销售组织（ISO）。服务提供商也提供控制或可能影响持卡人数据安全的公司。示例包括提供托管防火墙、IDS 和其他服务的托管服务提供商，以及托管提供商和其他实体。 如果某实体提供*仅*涉及公共网络访问提供的服务（例如仅提供通信链接的电信公司），则不认为该实体是相关服务的服务提供商（不过可认为该实体是其他服务的服务提供商）。请参见*多租户服务提供商*和*第三方服务提供商*。
SNMP	“简单网络管理协议”的缩写。
分割知识	两个或更多的实体分别掌握部分密钥且根据密钥的单个部分无法得知整个密钥的方法。
SQL	“结构化查询语言”的缩写
SSH	“安全外壳”的缩写。
SSL	“安全套接层 "的缩写。
强效加密法	加密法是一种通过可逆转加密过程保护数据的方法，该基本原理被许多安全协议和服务使用。强效加密法基于经过行业测试和认可的算法，以及提供至少 112 位的有效密钥长度及合适的密钥管理方法的密钥长度。 有效密钥强度可能短于密钥的实际“比特”长度，这可能导致具有较大密钥的算法比具有较小实际但较大有效密钥大小的算法提供较少保护。*我们建议所有新实施的内容使用至少 128 位的有效密码长度。* 关于加密算法和密钥长度的行业参考文献的例子包括： • NIST 特别出版物 *800-57 第 1 部分，* • *BSI TR-02102-1，* • *ECRYPT-CSA D5.4 算法、密钥大小和协议报告（2018），以及* • *ISO/IEC 18033 加密算法，以及* • *ISO/IEC 14888-3:2-81 信息技术安全技术 - 数字签名与附录 - 第 3 部分：基于离散对数的机制*
系统组件	包含在或连接到 CDE 或可能影响 CDE 安全的任何网络设备、服务器、计算设备或应用程序。

术语	定义
系统级对象	系统组件上所需的任何对象，包括但不限于应用程序执行表和配置文件、系统配置文件、静态和共享库和 DLL、系统执行表、设备驱动程序和设备配置文件以及第三方组件。
有针对性风险分析	就 PCI DSS 而言，风险分析侧重于特定的 PCI DSS 要求，因为该要求允许灵活性（例如，频率），或者对于定制方法，解释实体如何评估风险并确定定制控制符合 PCI DSS 要求的目标。
TDES	“三重数据加密标准”的缩写 也称为“3DES”或“三重 DES”。
Telnet	“电话网络协议”的缩写。
第三方服务提供商（TPSP）	代表某实体充当服务提供商的任何第三方。请参见*多租户服务提供商*和*服务提供商*。
第三方软件	由某实体获得但并非为其专门开发的软件。它可能是开放源代码、免费软件、共享软件或所购软件。
TLS	“传输层安全”的缩写。
令牌	就验证和访问控制而言，令牌是由硬件或软件提供的值，可与验证服务器或 VPN 一起执行动态或多因素验证。
磁道数据	也被称为“全磁道数据”或“磁条数据”。 编译在磁条或芯片中的数据，用于支付交易中的验证和/或授权。可以是芯片上的磁条图像也可以是磁条上的磁道数据。
截词	通过移除 PAN 数据的某分段，使完整 PAN 不可读的方法。截词存储在以电子方式存储、处理或传输时，与 PAN 的保护相关。 请参见*掩盖*，了解显示在屏幕、纸质收据等时的 PAN 保护。
可信网络	实体能够控制或管理并且符合适用的 PCI DSS 要求的实体网络。
不可信网络	任何不符合“可信网络”定义的网络。
虚拟支付终端	就自我评估调查问卷（SAQ）C-VT 而言，虚拟支付终端会通过网络浏览器访问收单机构、处理机构或第三方服务提供商网站以授权支付卡交易，其中商户通过网络浏览器手动输入支付卡数据与物理终端不同，虚拟支付终端不会直接从支付卡中读取数据。由于支付卡交易信息是手动输入的，因此虚拟支付终端一般用于替代商户环境中交易量较小的物理终端。

术语	定义
虚拟化	将计算资源从物理和/或逻辑约束中进行逻辑抽象。常见的一种抽象为虚拟机或 VM，VM 会获取物理机的内容，允许这些内容在不同的物理硬件上和/或与相同物理硬件上的其他虚拟机一起进行操作。其他常见的抽象包括但不限于容器、无服务器计算或微服务。
VPN	“虚拟专用网络”的缩写。
漏洞	一旦被利用可能有意或无意对系统构成威胁的缺陷或弱点。
网络应用程序	通常通过网络浏览器或通过网络服务访问的应用程序。网络应用程序可通过互联网或专用内部网络提供。