支付卡行业（PCI）
数据安全标准

要求和安全评估程序

3.2.1版本

2018五月

由 **前沿信安资讯阵地** 翻译整理

文档更改

日期	版	描述	网页
2008年10月	1.2	为了引入PCI DSS 1.2版为“PCI DSS要求和安全评估程序，”消除文档之间的冗余，并从PCI DSS安全审计程序V1.1一般和具体的变化。有关完整的信息，请参阅PCI DSS 1.1版的变化的PCI数据安全标准汇总至1.2。	
2009年7月	1.2.1	添加句子不正确PCI DSS 1.1版和1.2版之间删除。	五
		正确的“然后”到“比”中的测试程序6.3.7.a和6.3.7.b.	32
		在测试过程6.5.b.“不到位”删除变灰的标记为“到位”和列	33
		对于补偿性控制工作表 - 完成的示例，在页面顶部正确的写法说“使用此工作的任何要求，通过补偿控制为‘到位’指出定义补偿性控制。”	64
2010年10月	2.0	**修订和执行从V1.2.1变化。看到 *PCI DSS - 变更摘要从PCI DSS最新版本1.2.1至2.0。***	
2013年11月	3.0	**从2.0版更新。看到 *PCI DSS - 变更摘要从PCI DSS 2.0版到3.0。***	
2015年4月	3.1	**更新从PCI DSS 3.0版。看到 *PCI DSS - 变更摘要从PCI DSS 3.0版到 3.1* 更改的细节。**	
2016年4月	3.2	**更新从PCI DSS V3.1。看到 *PCI DSS - 变更摘要从PCI DSS 3.1版到 3.2* 更改的细节。**	
2018五月	3.2.1	**更新从PCI DSS V3.2。看到 *PCI DSS - 变更摘要从PCI DSS 3.2版到 3.2.1* 更改的细节。**	

目录

引言和PCI数据安全标准概述

支付卡行业数据安全标准（PCI DSS）的开发是为了鼓励和加强持卡人数据的安全性和全球促进广泛采用一致的数据安全措施。PCI DSS提供的旨在保护帐户数据的技术和业务需求的基线。PCI DSS适用于***所有*涉及支付卡处理，包括商人，加工，收购，发行商和服务提供商的实体。PCI DSS也适用于*所有*储存，处理或传输持卡人数据（CHD）和/或敏感的认证数据（SAD）的其他实体。下面是12所PCI DSS**要求的高级概述。

PCI数据安全标准 - 高层次概述

建立和维护一个安全的网络和系统	1。 安装和维护防火墙配置，以保护持卡人数据 **2。 不要使用系统密码和其他供应商提供的默认值** 安全参数
保护持卡人数据	**3。 保护存储的持卡人数据** **4。 整个开放的公共网络持卡人数据的加密传输**
维护漏洞管理计划	**5。 防范恶意软件的所有系统，并定期更新杀毒** 软件或程序 **6。 开发并维护安全系统和应用程序**
实施强访问控制措施	**7。 按业务需要知道限制访问持卡人数据** 8。 识别和验证访问系统部件 **9。 限制对持卡人数据的物理访问**
定期监控和测试网络	**10。 跟踪和监控所有访问网络资源和持卡人数据** **11。 定期测试安全系统和流程**
维护信息安全策略	**12。 坚持认为，所有人员解决信息安全的策略**

这个文件，*PCI数据安全标准要求和安全评估程序*，结合了12项PCI DSS要求和相应的测试程序到安全评估工具。它是专为在PCI DSS合规性评估，作为一个实体的验证过程的一部分。以下部分提供了详细的指导方针和最佳做法，以协助实体，进行准备，并报告PCI DSS评估的结果。在PCI DSS要求和测试程序开始15 PCI DSS包括最低限度的保护账户数据要求页，并且可以通过额外的控制和做法得到加强，以进一步降低风险，以及本地，地区和部门的法律法规。此外，立法或监管要求可能需要的个人信息或其他数据元素（例如，持卡人姓名），具体的保护。

PCI DSS资源

PCI安全标准委员会（PCI SSC）网站（www.pcisecuritystandards.org）包含了一些额外资源，以帮助企业与他们的PCI DSS评估和验证，包括：

- 文档库，其中包括：
  - *Ø PCI DSS - 更改摘要从PCI DSS 2.0版到3.0*
  - *Ø PCI DSS快速参考指南*
  - *Ø PCI DSS和条款的PA-DSS术语，缩写词和缩略词*
  - *Ø 信息补充和指南*
  - *Ø 对于PCI DSS优先方法*
  - *Ø 合规（ROC）的报告报告模板和报告说明*
  - *Ø 自我评估问卷（SAQs）和SAQ说明和指导*
  - *Ø 合规性的上作证（AOC的）*
- 常见问题（FAQ）
- PCI小型招商网站
- PCI培训课程和研讨会信息
- 合格安全性评估（QSA的）和授权扫描供应商（ASVS）
- **PTS的名单经批准的设备和PA-DSS认证的支付应用程序请参阅 *www.pcisecuritystandards.org* 关于这些和其他资源的信息。**

***注意：** 信息补充补充PCI DSS并确定额外的考虑和建议，以满足PCI DSS要求，他们不取代，取代或扩展的PCI DSS或它的任何要求。*

PCI DSS适用性信息

PCI DSS适用于 *所有* 涉及支付卡处理，包括商人，加工，收购，发行商和服务提供商的实体。PCI DSS也适用于 *所有* 储存，处理，或传输持卡人数据和/或敏感的验证数据的其他实体。持卡人数据和敏感的验证数据被定义如下：

帐户数据	
持卡人的数据包括：	**敏感验证数据包括：**
• 主账号（PAN） • 持卡人姓名 • 截止日期 • 服务代码	• 全磁道数据（磁条数据或等效的芯片上） • CAV2 / CVC2 / CVV2 / CID • PIN码/ PIN块

主账户号码是持卡人数据的决定性因素。 **如果持卡人姓名，服务代码，和/或到期日期被存储，处理或与PAN发送，或者以其它方式存在于持卡人数据环境（CDE），它们必须根据适用PCI DSS要求进**行保护。

PCI DSS要求适用于其中的帐户数据（持卡人数据和/或敏感的验证数据）被存储，处理或传送的组织。有些PCI DSS要求，也可以适用于已经外包其支付操作或CDE他们的管理机构。[1] 此外，该外包CDE或支付操作的第三方组织有责任确保该帐户数据是由按照适用的PCI DSS要求第三方保护。

下页中的表格示出通常使用的持卡人和敏感认证数据元素，每个数据元素的存储是否被允许或禁止，并且每个数据元素是否必须受到保护。这个表不是穷举的，而是被提供来示出了不同类型的适用于每一个数据元素的要求。

[1] **按照个人支付品牌的合规计划**

		数据元素	存储允许	渲染存储的数据无法读取每 3.4要求
帐户数据	持卡人 数据	主账号（PAN）	是	是
		持卡人姓名	是	没有
		服务代码	是	没有
		截止日期	是	没有
	敏感的认证 数据[2]	全跟踪数据[3]	没有	不能按要求3.2存储
		CAV2 / CVC2 / CVV2 / CID[4]	没有	不能按要求3.2存储
		PIN / PIN块[五]	没有	不能按要求3.2存储

PCI DSS要求3.3和3.4仅适用于PAN。如果PAN存储有持卡人数据的其他元件，仅PAN必须根据PCI DSS要求3.4呈现不可读。

敏感的验证数据不能保存授权之后，即使加密。这适用即使没有在环境中没有PAN。组织应该与他们的收单机构或个人支付品牌，直接了解SAD是否允许多长时间在授权之前被存储，以及任何相关的使用和保护要求。

[2] 敏感的验证数据不得批准后存放（即使加密）。
[3] 从磁条充分轨迹数据，在芯片上等效的数据，或其他地方
[4] 打印在正面或支付卡的背面的三或四数字值
[五] 一个卡交易期间由持卡人输入个人识别号码，和/或加密的交易信息中的PIN块

PCI DSS和PA-DSS的关系

PCI DSS的适用性PA-DSS应用

支付应用数据安全标准（PA-DSS）本身兼容的应用程序不会使实体PCI DSS合规，因为该应用程序必须落实到符合PCI DSS的环境，并根据PA-DSS实施指南通过提供使用支付应用程序供应商。

存储，处理或传输持卡人数据的所有应用程序都在范围为一个实体的PCI DSS评估，包括已经被验证，PA-DSS的应用程序。 在PCI DSS评估应确认PA-DSS认证的支付应用程序的配置是否正确并符合PCI DSS安全地执行。如果应用程序发生任何的定制，更深入的审查将在PCI DSS评估过程中是必须的，因为应用程序可能不再代表的是被验证，以PA-DSS版本。在PA-DSS要求从派生 *PCI DSS要求和安全评估程序*（ 本文档中所定义的）。在PA-DSS详细信息，以便于客户的PCI DSS合规的支付应用程序必须满足的要求。随着安全威胁在不断地发展，即由供应商不再支持的应用程序（例如，被鉴定由供应商为"生命的终结"）可能无法提供相同的安全水平受支持版本。

安全支付应用程序，在符合PCI DSS的环境中实施时，将最大限度地减少安全隐患，导致PAN的妥协，全程跟踪数据，卡验证码和值（CAV2，CID，CVC2，CVV2）和PIN与PIN的潜力块，从这些漏洞所造成的严重欺诈一起。

为了确定PA-DSS是否适用于某个指定的支付应用程序，请参阅PA-DSS计划指南，它可以在www.pcisecuritystandards.org找到。

PCI DSS的适用性支付应用程序供应商

PCI DSS可以适用于支付应用程序的供应商，如果存储，处理，或发送持卡人数据，或能访问其客户的持卡人数据（例如，在服务提供者的角色）。

PCI DSS要求的范围

在PCI DSS安全要求适用于所有系统组件中包含或连接到持卡人数据环境。持卡人数据环境（CDE）由储存，处理，或传输持卡人数据或敏感认证数据的人，工艺和技术。“系统组成部分”包括网络设备，服务器，计算装置，和应用程序。系统组件的实例包括但不限于以下内容：

- 提供安全服务系统（例如，认证服务器），便于分割（如内部防火墙），或可能影响安全（例如，名称解析或Web重定向服务器）的CDE。
- 虚拟化组件诸如虚拟机，虚拟交换机/路由器，虚拟设备，虚拟应用程序/桌面，和管理程序。
- 网络部件，包括但不限于防火墙，交换机，路由器，无线接入点，网络家电等安全设备。
- 服务器类型，包括但不限于网络，应用程序，数据库，认证，邮件，代理，网络时间协议（NTP）和域名系统（DNS）。
- 应用包括所有购买和自定义应用程序，包括内部和外部（例如互联网）应用。
- 任何其他部件或装置位于内或连接到CDE。

一个PCI DSS评估的第一步骤是精确地确定审查的范围。至少每年和之前的年度评估，评估的实体应当通过识别所有位置和持卡人的数据流确认其PCI DSS范围的精确度，以及识别连接到或，如果受损所有系统中，可能会影响在CDE（例如，认证服务器），以确保它们被包括在PCI DSS范围。所有类型的系统和位置应被视为范围界定过程的一部分，包括备份/恢复点和故障切换系统。

为了确认所定义的CDE的准确性，执行以下步骤：

- 所评估的实体识别并记录在他们的环境中的所有持卡人数据的存在，以验证当前定义CDE的外部不存在的持卡人数据。
- 一旦持卡人数据的所有位置被识别和记录，该实体使用的结果来验证PCI DSS范围是适当的（例如，结果可以是图或者持卡人数据位置的清单）。
- 该单位认为发现在CDE的PCI DSS评估和部分范围的任何持卡人数据。如果实体识别当前未包括在CDE数据，这样的数据应该被牢固地删除，迁移到当前定义的CDE或CDE重新定义以包括此数据。

实体保留相关文件，证明PCI DSS范围是如何确定的。下一年度PCI DSS范围确认活动期间的文档被保留用于评价员审查和/或参考。

对于每个PCI DSS评估，评估需要验证该评估的范围被精确地定义和记录。

网络分段

的网络分段，或分离（分段）中，从一个实体的网络的其余部分持卡人数据环境不是PCI DSS要求。然而，强烈建议为可减少的方法：

- PCI DSS的评估范围
- PCI DSS的评估费用
- 成本和实施和维护PCI DSS控制的难度
- 到组织的风险如果没有足够的网络分段（通过合并持卡人数据到更少，更可控的位置降低）（有时被称为“扁平网络”）整个网络是在PCI DSS评估的范围。网络分段可以通过多种物理或逻辑方式来实现，如正确配置内部网络防火墙，具有很强的访问控制列表，或其他技术，限制访问一个网络的特定段的路由器。被认为是超出范围的PCI DSS，系统组件必须正确地从CDE隔离（分段），这样，即使超出范围的系统组件被攻破它无法影响CDE的安全性。

减少持卡人数据环境的范围的一个重要前提是涉及到存储，处理或持卡人数据的传输业务需求和流程清醒的认识。限制持卡人数据通过消除不必要的数据，和必要的数据整合为少数几个位置越好，可能需要长期的业务实践再造。记录持卡人数据经由数据流图示流动有助于完全理解所有持卡人的数据流，并确保任何网络分段是在隔离持卡人数据环境有效。

如果网络分段到位和使用，以减少PCI DSS评估范围，评估必须验证分割是足够的，以减少评估的范围。在高级别上，适当的网络分段隔离储存，处理，或传输持卡人数据从那些不系统。然而，具体实施方式中的网络分割的充分性是高度可变的并且取决于许多因素，如给定的网络的配置，部署的技术，并且可以被实现其他控件。

附录d：分割和商务设施的取样/系统组件 **提供了关于网络分段和采样的上的PCI DSS评估的范围的影响的更多信息。**

无线

如果无线技术被用于存储，处理或传输持卡人数据（例如，点销售交易，“行无效化”），或者如果一个无线局域网（WLAN）是的一部分，或连接到持卡人数据环境中，应用为无线环境的PCI DSS要求和测试程序，并且必须执行（例如，要求1.2.3，2.1.1和4.1.1）。无线技术在实施之前，企业应仔细评估为防范风险技术的需求。仅考虑非敏感数据传输部署无线技术。

第三方服务供应商/外包的应用

服务提供商或商家可以使用第三方服务提供商存储，处理或传输持卡人数据代表他们，或者管理组件，如路由器，防火墙，数据库，物理安全和/或服务器。如果是的话，有可能是对持卡人数据环境的安全性产生影响。

缔约方应明确识别包括在服务提供商的PCI DSS评估范围的服务和系统组件，由服务提供商所涉及的特定的PCI DSS要求，任何要求，这是服务供应商的客户的责任，在包括其自己的PCI DSS审查。例如，主机托管服务提供商应明确规定其自己的IP地址进行扫描作为其季度漏洞扫描过程，其中部分IP地址是其客户的责任在自己的季度扫描包括。

服务提供者有责任证明其PCI DSS合规性，并可能被要求通过支付品牌这样做。服务提供者应联系其收购和/或支付品牌，以确定合适的符合性验证。有两种选择第三方服务提供商验证其是否遵守：

1）**年度考核：服务提供商可以对自己每年进行PCI DSS评估（S）和提供证据的**
客户展示他们的合规性; 要么

2）**多，按需评估：如果他们不接受自己的年度PCI DSS评估，服务提供商必须经历**
在他们的客户和/或要求评估参与他们的每一个客户的PCI DSS审查，以提供给各自的客户的每一个审查的结果（S）

如果第三方进行自己的PCI DSS评估，他们应该提供充分的证据，他们的客户验证服务提供商的PCI DSS评估范围涵盖适用于客户服务和检查，并确定相关的PCI DSS要求到位。由服务提供商提供给他们的客户的证据的具体类型将取决于这些当事方之间发生的协议/合同。例如，提供服务供应商的ROC的AOC和/或相关的部分（节录保护任何机密信息）可以帮助提供全部或部分的信息。

另外，商家和服务提供商必须管理并能够访问持卡人数据监控所有相关的第三方服务提供商的PCI DSS合规性。 ***请参阅要求12.8本文档的细节英寸***

最佳实践实现PCI DSS到业务照常进程

为了确保安全控制继续实施得当，PCI DSS应该落实到业务照常（BAU）活动，作为一个实体的整体安全策略的一部分。这使得监控其安全控制的一个持续的基础上的有效性，并在PCI DSS评估之间维持其符合PCI DSS的环境中的实体。如何整合PCI DSS成BAU活动的例子包括但不限于：

1.监测安全控制-如防火墙，入侵检测系统/入侵预防系统（IDS / IPS），文件完整性监控（FIM），抗病毒，访问控制的等-以确保它们被有效地操作并如预期。

2.确保在安全控制所有故障检测和及时响应。流程安全控制故障响应应包括：

- 恢复安全控制
- 识别失败的原因
- 识别和安全控制的故障期间解决出现的任何安全问题
- 实施缓解（诸如过程或技术控制），以防止故障的重复的原因
- 恢复安全控制的监控，或许与在一段时间内加强监测，以验证控制有效运行

3.回顾（在系统或网络配置，例如，新添加的系统，变化）的变化完成之前于环境的变化，并执行以下步骤：

- 确定PCI DSS范围的潜在影响（例如，一个新的防火墙规则，允许在CDE的系统和其他系统可能带来额外的系统或网络进入范围为PCI DSS之间的连接）。
- 确定适用于系统和受影响的变化的网络PCI DSS的要求（例如，如果一个新的系统是在范围为PCI DSS，那就需要每系统配置标准，包括FIM，AV，贴剂，审核日志记录等，以被配置，并需要被添加到季度漏洞扫描计划）。
- 更新PCI DSS范围和实施安全控制适当。

4.更改造成的影响，以PCI DSS范围和要求正式评审组织结构（例如，一个公司合并或收购）。

5.进行定期审查和通讯，以确认PCI DSS要求的不断到位和人员安全之后的过程。这些定期审查范围应涵盖所有设施和场所，包括零售商店，数据中心等，以及包括审查系统组件（或系统部件的样品），以验证PCI DSS要求的不断到位，例如，配置标准已应用，补丁和AV是最新的，审计日志进行审查，等等。进行定期审查的频率应为适合他们环境的规模和复杂性的实体来确定。这些评论也可以用于验证适当的证据被保持，例如，审计日志，漏洞扫描报告，防火墙评论等

6.每年至少查看硬件和软件技术，以确认他们继续由供应商的支持，能满足实体的安全要求，包括PCI DSS。如果发现技术不再受供应商支持或不能满足实体的安全需求，实体应制定修复计划，直至并包括更换技术的，是必要的。

除了上述做法，组织也不妨考虑执行职责分离为它们的安全功能，使安全性和/或审计功能从操作功能分离。在一个单独的执行多个角色（例如，管理和安全操作）的环境中，任务可以被分配使得没有单个个体具有没有独立的检查点的过程的端至端的控制。例如，对于配置和变更审批职责的责任可以分配给不同的个体。

***注意：** 对于一些实体，这些最佳做法还要求，以确保持续的PCI DSS合规性。*

例如，PCI DSS包括在一些要求这些原理，并且在指定的单位补充验证（PCI DSS附录A3）需要指定实体以验证这些原则。 所有的组织都应该考虑实施最佳做法纳入他们的环境，即使在

组织不需要验证他们。

对审核员：商务设施/系统组件抽样

抽样是对审核员，以方便评估的过程，其中有大量的商业设施和/或系统组件的选项。

虽然这是可以接受的评估者品尝商业设施/系统组件作为他们的一个实体的PCI DSS合规性审查的一部分，这是不能接受的实体应用PCI DSS要求，只有他们的环境样本（例如，要求季报漏洞扫描适用于所有系统组件）。类似地，它是不能接受的一个评估仅审查是否符合PCI DSS要求的样品。

考虑到环境的整体范围和复杂性正在评估后，评估可以独立，以评估实体与PCI DSS要求的符合选择商业设施/系统组件代表性的样本。这些样品必须首先为商业设施，然后确定每个选定的商业设施内的系统组件。样品必须是所有的类型和业务设施位置的选择有代表性，以及为所有选定的商业设施内的各类系统组件。样品必须足够大，以提供保证评估人员按照预期的控制措施。商业设施的例子包括但不限于：公司办公室，商店，特许经营地点，处理设施，数据中心，和其他设施类型在不同的位置。取样应当包括每个选定业务设施内的系统组件。例如，对于每个选定的营业设施，包括各种操作系统，功能和应用程序适用于正在审查的区域。作为一个例子，评估可以定义在商业设施的样本，包括运行Apache的Sun服务器，运行Oracle的Windows服务器，大型机系统上运行的传统卡处理应用程序，运行HP-UX的数据传输服务器和Linux服务器运行MySQL。如果所有的应用程序从OS的单个版本上运行（例如，Windows 7或Solaris 10），该样品仍然应该包括各种应用程序（例如，数据库服务器，web服务器，数据传递服务器）。取样应当包括每个选定业务设施内的系统组件。例如，对于每个选定的营业设施，包括各种操作系统，功能和应用程序适用于正在审查的区域。作为一个例子，评估可以定义在商业设施的样本，包括运行Apache的Sun服务器，运行Oracle的Windows服务器，大型机系统上运行的传统卡处理应用程序，运行HP-UX的数据传输服务器和Linux服务器运行MySQL。如果所有的应用程序从OS的单个版本上运行（例如，Windows 7或Solaris 10），该样品仍然应该包括各种应用程序（例如，数据库服务器，web服务器，数据传递服务器）。取样应当包括每个选定业务设施内的系统组件。例如，对于每个选定的营业设施，包括各种操作系统，功能和应用程序适用于正在审查的区域。作为一个例子，评估可以定义在商业设施的样本，包括运行Apache的Sun服务器，运行Oracle的Windows服务器，大型机系统上运行的传统卡处理应用程序，运行HP-UX的数据传输服务器和Linux服务器运行MySQL。如果所有的应用程序从OS的单个版本上运行（例如，Windows 7或Solaris 10），该样品仍然应该包括各种应用程序（例如，数据库服务器，web服务器，数据传递服务器）。包括各种操作系统，功能和应用程序适用于正在审查的区域。作为一个例子，评估可以定义在商业设施的样本，包括运行Apache的Sun服务器，运行Oracle的Windows服务器，大型机系统上运行的传统卡处理应用程序，运行HP-UX的数据传输服务器和Linux服务器运行MySQL。如果所有的应用程序从OS的单个版本上运行（例如，Windows 7或Solaris 10），该样品仍然应该包括各种应用程序（例如，数据库服务器，web服务器，数据传递服务器）。包括各种操作系统，功能和应用程序适用于正在审查的区域。作为一个例子，评估可以定义在商业设施的样本，包括运行Apache的Sun服务器，运行Oracle的Windows服务器，大型机系统上运行的传统卡处理应用程序，运行HP-UX的数据传输服务器和Linux服务器运行MySQL。如果所有的应用程序从OS的单个版本上运行（例如，Windows 7或Solaris 10），该样品仍然应该包括各种应用程序（例如，数据库服务器，web服务器，数据传递服务器）。大型机系统上运行的传统卡处理应用程序，运行HP-UX的数据传输服务器和Linux服务器运行MySQL。如果所有的应用程序从OS的单个版本上运行（例如，Windows 7或Solaris 10），该样品仍然应该包括各种应用程序（例如，数据库服务器，web服务器，数据传递服务器）。大型机系统上运行的传统卡处理应用程序，运行

当独立选择的商业设施/系统组件样本，评估应考虑以下几点：

- 如果有标准化的，即确保一致性和每个业务设施/系统部件必须遵循集中PCI DSS安全性和操作的流程和控制在适当位置，所述样品可以比如果有没有适当的标准方法/控制小。样品必须足够大，以提供与所有的商业设施/系统组件按照标准流程配置合理保证的评审员。评估员必须验证标准化，集中化的控制措施，有效地工作。

- 如果有代替多于一种类型的标准的安全性和/或操作过程（例如，对于不同类型的业务设施/系统组件），样品必须足够大以包括业务设施/固定与每个类型的系统组件处理。

- 如果没有标准PCI DSS处理/控制在适当位置，并且每个业务设施/系统部件通过非标准过程管理，样品必须更大为放心评价者每个业务设施/系统组件已经实施PCI DSS要求适当。

- 系统部件的样品必须包括所有类型和组合在使用中。例如，当应用程序被采样，样品必须包括对于每种类型的应用程序的所有版本和平台。

对于其中采样被使用时，评估者必须每个实例：

- 记录的基本原理的采样技术和样本大小的后面，
- 文件和验证用于确定样本大小标准化PCI DSS处理和控制，并且
- 解释怎么样是合适的，并代表总人口的。

评估员必须重新验证每个评估采样理由。如果抽样是被使用，商业设施和系统组件不同的样品必须选择为每个评估。

也请参考：
附录d：分割和商务设施的取样/系统组件。

补偿性控制

在年度基础上，任何补偿性控制必须记录，审查和评估者验证，并包含在报告提交合规，每 *附录B：补偿性控制* 和 *附录C：补偿性控制工作表。*

对于每一个补偿控制，该补偿控制工作表（ *附录C* ）必须 完成。此外，补偿控制结果应在ROC在相应的PCI DSS要求部分中记录。见上述 *附件B* 和 *C* 有关详细信息，“补偿性控制。”

说明与内容上的合规报告

在提供了对符合性（ROC）的报告的说明和内容 *PCI DSS ROC报告模板。*

该 *PCI DSS ROC报告模板* 必须作为模板创建的 *报告合规情况。* 被评估的实体应遵循各支付品牌相应的报告要求，确保每个支付品牌确认实体的合规状态。联系每个支付品牌或收购，以确定报告要求和说明
。

PCI DSS评估程序

PCI DSS的评估过程包括如下步骤完成：

1.确认PCI DSS评估范围。

2.执行环境的PCI DSS评估，以下测试程序为每一个需求。

3.完成的评估报告应用（即自我 *评估问卷（* SAQ）或报告合规性（ROC）），
包括所有补偿性控制的文件，根据适用的PCI指导和说明。

4.完成符合服务提供商或商家，如适用的认证，其全文。合规性上作证可在PCI SSC网站上。

5.提交SAQ或ROC，与合规证明，连同任何其他要求的文件，如ASV报告 - 扫描到购买方（商家），或在支付品牌或其他请求者（服务提供商）。

6。 如果需要，进行整治，以解决不到位的要求，并提供最新报告。

PCI DSS版本

如该文件的发布日期，PCI DSS V3.2通过2018年12月31日，在这之后退役是有效的。在此日期之后的所有PCI DSS验证必须是PCI DSS V3.2.1或更高版本。

下表提供了PCI DSS版本及其相关日期的摘要。 [6]

版	发布时间	退休
PCI DSS V3.2.1（本文档）	2018五月	待定
PCI DSS V3.2	2016年4月	2018年12月31日

[6] **在主题的PCI DSS新版本的发布而改变。**

详细的PCI DSS要求和安全评估程序

下面定义了PCI DSS要求和安全评估程序中的列标题：

- **PCI DSS要求** - 此列定义了数据安全标准的要求; PCI DSS合规性进行验证，这些要求。
- **测试程序** 应遵循此列显示过程由评估来验证PCI DSS要求已得到满足，是 - “到位”。
- **指导** - 此列描述了各自的PCI DSS要求背后的意图或安全目标。此列仅包含指导，旨在协助每个需求的意图的理解。在此列中的指导不会取代或扩展的PCI DSS要求和测试程序。

***注意：** PCI DSS要求不被认为是在地方，如果控制尚未实施或正在计划在未来某个日期完成。经过任何公开或不到位的项目是由实体处理，评估，然后将重新评估，以验证修复完成，所有要求得到满足。*

请参考以下资源（PCI SSC网站上提供）来记录PCI DSS评估：

- *有关完成合规（ROC）的报告的说明，请参阅* PCI DSS ROC报告模板。
- *有关完成自我评估问卷指令（SAQ），指的是* PCI DSS SAQ说明和指导。
- *关于提交PCI DSS合规性验证报告的说明，请参阅* 合规的PCI DSS上作证。

建立和维护一个安全的网络和系统

要求1：安装并维护防火墙配置，以保护持卡人数据

防火墙是控制允许一个实体的网络（内部）和不受信任的网络（外部）之间计算机通信，以及车辆进出实体的内部受信任网络内更敏感区域的装置。持卡人数据环境是一个实体的信任网络中的更敏感区域的一个例子。

防火墙检查所有网络流量并阻止那些不符合规定的安全标准传输。所有系统必须受到保护，免受来自不受信任的网络未经授权的访问，无论是通过互联网为电子商务，通过桌面浏览器的员工上网，员工电子邮件访问，如企业对企业连接专用连接进入系统，通过无线网络，或经由其他来源。通常情况下，看起来微不足道的路径和从不受信任网络可以提供未受保护的途径进入关键系统。防火墙是所有计算机网络的关键保护机制。

其它系统组件可以提供防火墙功能，只要它们满足在要求1.当其他系统部件持卡人数据环境中使用，以提供防火墙功能定义防火墙的最低要求，这些装置必须被包含的范围和评估内的要求：1。

PCI DSS要求	测试程序	指导
1.1 建立和实施防火墙和路由器配置标准，包括以下内容：	**1.1 检查以下指定的防火墙和路由器配置标准和其他文档，并验证标准是完整和实施如下：**	防火墙和路由器是用于控制从网络进入和退出该体系结构的关键组件。这些设备是阻止不需要的访问和管理授权访问进出网络的软件或硬件设备。配置标准和程序，将有助于确保其数据保护组织的第一道防线依然强劲。
1.1.1 批准和测试所有网络连接以及更改防火墙和路由器配置的正式流程	**1.1.1.A 检查文件化的程序以核实不存在用于测试和所有批准的正式流程：** • 网络连接和 • 更改防火墙和路由器配置	批准和测试所有连接和更改防火墙和路由器将有助于防止由于网络，路由器或防火墙的配置错误的安全性问题的记载和执行过程。无正式批准和变化检测，变化的记录可能不会被更新，这可能导致网络文件和实际配置之间的不一致性。
	1.1.1.B 对于网络连接的样本，采访负责人员，并检查记录，验证网络连接获得批准并进行测试。	

PCI DSS要求	测试程序	指导
	1.1.1.c 确定的防火墙和路由器配置做出实际变化的样本，比较变更记录，采访负责人员是否要修改批准和测试。	
1.1.2 识别持卡人数据环境和其它网络之间的所有连接当前网络图，包括任何无线网络	**1.1.2.A 检查图（一个或多个），并观察网络配置，以验证当前网络图是否存在以及它记录了持卡人的数据，包括任何无线网络的所有连接。**	网络图描述网络的配置方式，并确定所有网络设备的位置。 如果没有当前网络图，设备可能会被忽略，并在不知不觉中离开出来PCI DSS实施的安全控制，因此很容易受到损害。
	1.1.2.B 采访负责人员确认该图是最新的。	
1.1.3 显示所有持卡人数据电流图跨系统和网络流	**1.1.3 检查数据流图和面试人员核实图表：** • 显示所有持卡人数据流跨系统和网络。 • 在需要时对环境的更改保持当前和更新。	持卡人数据流图识别被存储，处理或在网络内传送的所有持卡人数据的位置。网络和持卡人数据流图帮助企业了解和保持环境的范围的曲目后，显示持卡人的数据通过网络和各个系统和设备之间的流动。
1.1.4 在每个互联网连接的防火墙和任何非军事区（DMZ）和内部网络区之间要求	**1.1.4.a 检查 防火墙配置标准，并验证它们包括用于在每个互联网连接和任何DMZ和内部网络区之间的防火墙要求。**	使用在每一个互联网连接的防火墙进入（以及退出）网络，以及任何DMZ和内部网络之间，允许组织在监视和控制接入和恶意个人通过获得访问内部网络的可能性最小化未受保护的连接。
	1.1.4.b 验证当前网络图是与防火墙配置标准相一致。	
	1.1.4.c 观察的网络配置，以验证防火墙是在每个因特网连接的地方，任何非军事区（DMZ）和内部网络区，每记录配置标准和网络图之间。	

PCI DSS要求	测试程序	指导
1.1.5 组，角色和职责的描述网络组件的管理	**1.1.5.a** 确认防火墙和路由器配置标准包括组，角色和职责的网络组件的管理进行说明。	角色和职责分配的描述确保人员都知道谁是负责所有网络组件的安全性，而且这些分配管理组件是意识到自己的责任。如果角色和职责没有正式分配，设备可以无人管理。
	1.1.5.b 负责网络组件的管理人员接受采访时确认，作用和责任的记录被分配。	
1.1.6 商业论证和批准使用的所有服务，协议和端口的文档允许的，其中包括对被认为是不安全的协议来实现安全功能的文档。	**1.1.6.a** 确认防火墙和路由器配置标准包括的所有服务，协议和端口，包括商业论证和批准的每一个文件列表。	妥协经常发生由于未使用的或不安全的服务和端口，因为这些往往都已知的漏洞和许多组织没有修补系统漏洞的服务，协议和端口不使用（尽管漏洞仍然存在）。通过明确界定和记录服务，协议和端口所必需的业务，企业可以确保所有其他服务，协议和端口禁用或删除。认证应该由独立的人员的人事管理配置的授予。如果不安全的服务，协议或端口所必需的业务，通过使用这些协议所带来的风险，应明确由组织理解和接受，使用该协议的应是合理的，和安全功能，使这些协议被安全地使用，应记录并实施。如果这些不安全的服务，协议或端口是没有必要的业务，他们应该被禁用或删除。有关被认为是不安全的服务，协议或端口的指导，参考行业标准和指导（如NIST，ENISA，OWASP等）。
	1.1.6.b 确定允许不安全的服务，协议和端口; 并确认安全保护功能可记录每个服务。	
	1.1.6.c 检查防火墙和路由器配置以验证该记录的安全特征为每个不安全服务，协议和端口来实现。	

PCI DSS要求	测试程序	指导
1.1.7 要求审查防火墙和路由器的规则集，每半年至少	**1.1.7.a** 确认防火墙和路由器配置标准要求防火墙的审查和路由器规则至少将每半年一次。	本文综述了该组织的机会，至少每半年要清理所有不需要的，过时的，或不正确的规则，并确保所有规则集只允许授权的服务和匹配记录业务理由是港口。高音量的变化防火墙和路由器规则集的组织可能希望考虑更频繁地进行审查，以确保规则集继续满足业务的需求。
	1.1.7.b 审查有关规则集审查和面试负责人员来验证规则集进行审查，至少每半年文档。	
1.2 构建限制不受信任的网络，并在持卡人数据环境中的任何系统组件之间的连接的防火墙和路由器配置。 ***注意：** 一个"不受信任网络"是任何网络外部于审查属于实体网络和/或超出实体的控制或管理能力。*	**1.2** 检查防火墙和路由器配置，并执行以下步骤来验证连接在持卡人数据环境不受信任的网络和系统组件之间的限制：	安装内部，可信网络以及任何不信任的网络，这是外部和/或出实体的控制或管理能力之间的网络保护是至关重要的。不执行这一措施正确导致易受恶意个人或软件的未授权访问的实体。对于防火墙功能是有效的，它必须被正确配置来控制和/或限制车辆进出实体的网络。
1.2.1 限制入站和出站流量到这是必要的持卡人数据环境，特别否认所有其他流量。	**1.2.1.a** 检查防火墙和路由器配置标准，以验证他们确定必要的持卡人数据环境的入站和出站流量。	所有入站和出站连接的检查允许检查和基于所述源和/或目的地地址的通信量的限制，从而防止不可信和可信的环境之间的未过滤的访问。这可以防止恶意个人从通过未经授权的IP地址来访问单位的网络或以未授权方式使用服务，协议或端口（例如，送他们已经从实体的网络出中获得的数据不可信服务器）。是落实否认没有特别需要的所有入站和出站流量有助于防止无意的漏洞，将允许或出意外的和潜在的有害流量的规则。
	1.2.1.b 检查防火墙和路由器配置以验证入站和出站通信被限制为所必需的持卡人数据环境。	
	1.2.1.c 检查防火墙和路由器配置，以验证使用显式"拒绝所有"或隐式拒绝允许语句后，所有其他的入站和出站流量被明确拒绝，例如。	

PCI DSS要求	测试程序	指导
1.2.2 安全和使路由器的配置文件。	**1.2.2.a** 检查路由器的配置文件，以确认他们是从未经授权的访问安全。 **1.2.2.b** 检查路由器配置以验证它们是同步的，例如，正在运行的（或活性的）构型的启动配置（当机器启动使用）相匹配。	虽然运行（或活动）路由器的配置文件包括当前，安全设置，投入运行文件（当路由器重新启动或引导其使用）必须使用相同的安全设置，以确保这些设置应用时更新启动时的配置运行。因为他们只是偶尔运行，启动配置文件常常被遗忘，并且不更新。当路由器重新启动并加载尚未更新，使用相同的安全设置，那些在运行配置一个启动配置，它可能会导致较弱的规则，允许恶意用户进入网络。
1.2.3 安装外围防火墙的所有无线网络和持卡人数据环境之间，并配置这些防火墙拒绝，或者，如果交通是必要的经营宗旨，只允许授权的无线环境和持卡人数据环境之间的流量。	**1.2.3.a** 检查防火墙和路由器配置，以验证是否有周边所有无线网络和持卡人数据环境之间安装防火墙。 **1.2.3.b** 验证防火墙拒绝，或者，如果交通是必要的经营宗旨，只允许授权的无线环境和持卡人数据环境之间的流量。	网络中的已知（或未知）的实施和无线技术的开发是恶意个人访问网络和持卡人数据的共同路径。如果无线设备或网络没有实体的知识安装，恶意个人可以很容易地与“无形”进入网络。如果防火墙不限制从无线网络接入到CDE，即获得对无线网络的非法访问恶意个人可以方便地连接到CDE和妥协的帐户信息。防火墙必须所有无线网络和CDE之间安装，而不管环境的目的，该无线网络连接。这可能包括，但不限于，企业网络，零售商店，客人网络，仓储环境等

PCI DSS要求	测试程序	指导
1.3 禁止在互联网和持卡人数据环境的任何系统组件之间的直接公共访问。	**1.3** 检查防火墙和路由器配置，包括但在互联网中，DMZ路由器和防火墙，所述DMZ持卡人段，周界路由器，和内部持卡人网络不限于扼流路由器段并执行以下，以确定不存在在内部持卡人网段的网络和系统组件之间的直接访问：	虽然有可能是不可信的连接正当的理由被允许DMZ系统（例如，允许Web服务器的公共访问），这种连接不应该在内部网络中授予系统。防火墙的目的是为了管理和控制公共系统和内部系统，尤其是那些存储，处理或传输持卡人数据之间的所有连接。如果直接访问被允许公共系统和CDE之间，由防火墙提供的保护被旁路，和存储持卡人数据的系统组件可能暴露妥协。
1.3.1 实现一个DMZ，以入站流量限制到提供公共授权访问的服务，协议和端口唯一的系统组件。	**1.3.1** 检查防火墙和路由器配置，以验证一个DMZ被实现为入站流量限制到提供公共授权访问的服务，协议和端口唯一的系统组件。	非军事区是管理互联网（或其他不受信任的网络）之间的连接，一个组织需要有提供给公众（如Web服务器），网络和服务的一部分。此功能是为了防止恶意的人访问该组织的内部网络从互联网，或以未授权方式使用服务，协议或端口。
1.3.2 限制入站网络流量DMZ内部IP地址。	**1.3.2** 检查防火墙和路由器配置，以验证入站网络流量被限制在DMZ内的IP地址。	
1.3.3 实施反欺骗措施，以检测和阻止进入网络伪造源IP地址。 （例如，块的流量从因特网与内部源地址始发。）	**1.3.3** 检查防火墙和路由器配置，以验证防伪措施的落实，例如内部地址不能从互联网到DMZ通过。	正常情况下，数据包包含最初发送它使其他计算机网络中知道包来自的计算机的IP地址。使目标系统认为该数据包是来自可靠来源的恶意个人会常常想欺骗（或模仿）发送IP地址。 进入网络过滤数据包帮助，除其他外，确保数据包不“欺骗”的样子，他们是从机构自身的内部网络的到来。

PCI DSS要求	测试程序	指导
1.3.4 不要让从持卡人数据环境至Internet的未授权出站流量。	**1.3.4 检查防火墙和路由器配置，以验证从持卡人数据环境到互联网的明确授权**出站流量。	从持卡人数据环境中的所有出站通信进行评估，以确保其符合既定的授权规则。的连接应被检查（通过限制源/目的地址/端口，和/或内容的阻挡例如），以限制流量，只有经过授权的通信。
1.3.5 只允许"建立的"连接到网络。	**1.3.5 检查防火墙和路由器配置，以验证防火墙只允许已建立的连接到内部网络**，并否认不与先前建立的会话相关联的所有入站连接。	对于通过防火墙的每个连接保持"状态"（或状态）防火墙知道到以前的连接的明显响应是否确实是有效的，授权响应（因为它保留了每一个连接的状态），或者是恶意流量企图欺骗防火墙进入允许连接。
1.3.6 持卡人数据（例如数据库）存储在内部网络区域的地方的系统组件，从所述DMZ和其他不受信任的网络隔离。	**1.3.6 检查防火墙和路由器配置，以验证存储持卡人数据的使用的是内部网络区**域系统组件，从所述DMZ和其他不受信任的网络隔离。	如果持卡人数据位于DMZ中，它对于外部攻击者访问此信息更容易，因为存在更少的层渗透。保护持卡人数据存储在从所述DMZ和其他不受信任的网络由防火墙隔离可以防止到达系统部件未经授权的网络流量的内部网络区域的系统组件。 ***注意：* *该要求不旨在适用于易失性存储器持卡人数据的临时存储。***

PCI DSS要求	测试程序	指导
1.3.7 不要公开其私人IP地址和路由信息未经授权的第三方。 ***注意：*** *方法掩盖IP地址可能包括，但不限于：* • *网络地址转换（NAT）* • *将含有后面代理服务器/防火墙持卡人数据服务器，* • *去除或路由广告所采用的注册地址私有网络的过滤，* • *内部采用RFC1918地址空间，而不是注册地址。*	**1.3.7.a 检查防火墙和路由器配置，以验证方法，以防止私有IP地址的内部网络到互联网的信息披露和路由信息。** **1.3.7.b 面试人员，并检查文件，验证私有IP地址的任何披露和路由信息到外部实体授权。**	限制内部或私有IP地址的披露是必要的，以防止黑客“学习”的内部网络的IP地址，并使用该信息来访问网络。用来满足此要求的意图可以根据具体的网络技术而不同的方法被使用。例如，用于满足这种要求的控制可以是用于IPv4网络比IPv6网络不同。

PCI DSS要求	测试程序	指导
1.4 在任何便携式计算设备（包括公司和/或员工自备）连接到Internet的网络之外时（例如，员工使用的笔记本电脑）安装个人防火墙软件或等效的功能，并且也用于访问CDE。防火墙（或等同物）配置包括： • 特定配置设置定义。 • 个人防火墙（或等效功能）正在积极运行。 • 个人防火墙（或等效功能）是不是由所述便携式计算设备的用户可改变的。	**1.4.a 检查政策和 配置标准验证：** • 个人防火墙软件或等效的功能是必需的所有便携式计算设备（包括公司和/或员工自备）连接到Internet的网络之外时（例如，员工使用的笔记本电脑），并且也用于访问CDE。 • 特定的配置设置是为个人防火墙（或等效功能）来定义。 • 个人防火墙（或等效功能）被配置为主动地运行。 • 个人防火墙（或等效功能）被配置为不是由便携式计算设备的用户可将其改变。 **1.4.b 检查公司和/或员工自有设备，以验证样本：** • 个人防火墙（或等效功能）安装和每个企业的具体配置设置中配置。 • 个人防火墙（或等效功能）正在积极运行。 • 个人防火墙（或等效功能）是不是由所述便携式计算设备的用户可改变的。	被允许从企业防火墙外部连接到互联网的便携式计算设备更容易受到基于Internet的威胁。防火墙功能（例如，个人防火墙软件或硬件）的使用有助于保护设备免受基于Internet的攻击，它可以使用该设备来访问组织的系统和数据一旦设备被重新连接到网络。具体的防火墙配置设置由组织决定。 ***注意：这一要求适用于员工 - 拥有和公司拥有的便携计算设备。****不能由企业策略管理系统引入的弱点，并提供恶意的人可能利用各种机会。允许不可信系统连接到一个组织的CDE可能会导致访问被授予攻击者和其他恶意用户。*
1.5 保证管理的防火墙安全政策和操作程序记录，在使用中，和已知的所有当事方。	**1.5 检查文件和面试人员核实管理的防火墙安全政策和操作程序是：** • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全政策和操作程序，以确保防火墙和路由器的持续经营，以防止未经授权的网络访问。

要求2：不要使用系统密码和其他安全参数供应商提供的默认值

恶意个人（外部和内部的实体）经常使用供应商默认密码和其他供应商默认设置来攻击系统。这些密码和设置都深受黑客社区都知道，而且很容易通过公共信息来确定。

PCI DSS要求	测试程序	指导
2.1 随时改变供应商提供的默认值，并删除或禁用不必要默认账户 之前 安装在网络上的系统。这适用于所有默认密码，包括但不限于那些由操作系统使用，提供安全的服务，应用和系统帐户的软件，点销售 **（ POS）终端，支付应用，简单网络管理协议（SNMP）团体字符串，等等）。**	**2.1.A 选择系统组件样本，并尝试登录（以系统管理员的帮助），以使用默认的**供应商提供的帐号和密码，设备和应用程序，以确认所有默认密码（包括那些对操作系统，提供安全服务软件，应用程序和系统账户，POS终端，和简单网络管理协议（SNMP）团体字符串）已被更改。（使用供应商手册和网上找供应商提供的帐号/密码上。）	恶意个人（外部和内部的组织）经常使用供应商默认设置，账户名和密码妥协的操作系统软件，应用程序和安装在他们的系统。因为这些默认设置经常发表在黑客社区是众所周知的，更改这些设置会离开系统不容易受到攻击。即使一个默认的帐户不打算使用，更改默认密码以强大的独特的密码，然后禁用帐户将防止恶意个人从重新启用该帐户并获得使用默认密码访问。
	2.1.B 对于系统组件的样品，验证所有不必要的默认账户（包括操作系统，安全软件，应用程序，系统，POS终端，SNMP等使用的帐户）被去除或禁用。	
	2.1.c 面试人员并检查证明文件，以确认： • 安装在网络上之前的系统供应商的所有默认值（包括操作系统，软件提供安全服务，应用程序和系统账户，POS终端，简单网络管理协议（SNMP）团体字符串，等等默认密码）被改变。 • 不必要默认账户（包括操作系统，安全软件，应用程序，系统，POS终端，SNMP等使用的帐户）被去除或禁用被安装在网络上之前的系统。	

PCI DSS要求	测试程序	指导
2.1.1 对于连接到持卡人数据环境或传输持卡人数据的无线环境，在安装改变所有无线厂商默认值，包括但不限于默认无线加密密钥，密码，和SNMP社区字符串。	**2.1.1.a** 采访专人负责检查证明文件，以确认： • 加密密钥从默认安装时改变 • 加密密钥改变与按键的知识随时随地任何人离开公司或改变位置。	如果无线网络不具有足够的安全配置（包括更改默认设置）来实现，无线嗅探器就可以窃听流量，轻松捕捉数据和密码，很容易进入并攻击网络。此外，对于旧版本的802.11x加密（有线等效保密，或WEP）密钥交换协议已经被打破，可以使加密变得毫无价值。固件的设备进行更新，以便支持更多的安全协议。
	2.1.1.b 面试人员并检查政策和程序来验证： • 需要默认的SNMP社区字符串在安装时被改变。 • 默认密码/所需的接入点，密码短语在安装时被改变。	
	2.1.1.c 检查供应商文档并登录到无线设备，以系统管理员的帮助，以验证： • 默认的SNMP社区字符串未使用。 • 默认密码/不使用的接入点，密码短语。	
	2.1.1.d 检查供应商文档和观察无线配置设置，以验证在无线设备上固件更新以支持强大的加密： • 验证通过无线网络 • 传输通过无线网络。	
	2.1.1.e 检查供应商文档和观察无线配置设置以确认其他与安全相关的无线供应商默认设置被改变，如果适用。	

PCI DSS要求	测试程序	指导
2.2 制定所有系统组件的配置标准。确保这些标准解决所有已知的安全漏洞，并与行业认可的系统强化标准保持一致。 业界公认的系统强化标准的来源可能包括，但不限于： • 互联网安全中心（CIS） • 国际标准化组织（ISO） • 系统管理员审核网络安全（SANS）研究所 • 标准技术研究院（NIST）。	**2.2.a 检查组织的系统配置标准，为所有类型的系统组件和验证系统配置标准与工业接受强化标准保持一致。** **2.2.B 检查政策和面试人员核实新的漏洞问题确定了系统配置标准进行更新，如要求定义** 6.1。 **2.2.c 检查政策和面试人员，以验证系统的新系统时配置和验证为安装在网络上的前一个系统，是配置标准应用。** **2.2.d 验证系统配置标准包括所有类型的系统组件以下程序：** • 不必要的默认帐户的所有供应商提供的默认值，并消除改变 • 实现每个服务器只能有一个主功能，以防止从需要不同的安全级别功能的共存在同一台服务器上 • 仅启用必要的服务，协议，进程等，如需要对系统的功能 • 对于被认为是不安全的任何需要的服务，协议或守护程序实施额外的安全功能 • 配置系统安全参数，防止误操作 • 删除所有不必要的功能，如脚本，驱动程序，功能，子系统，文件系统和不必要的Web服务器。	有许多操作系统，数据库和企业应用已知的弱点，也有已知的方法来配置这些系统来修复安全漏洞。为了帮助那些没有安全专家，一些安全组织已经建立了系统强化指导和建议，这些建议如何纠正这些弱点。 的来源上配置标准指导实例包括，但不限于：www.nist.gov，www.sans.org，和www.cisecurity.org，www.iso.org和产品供应商。系统配置标准必须保持更新，以确保新发现的弱点之前的系统被安装在网络上的修正。

PCI DSS要求	测试程序	指导
2.2.1 实现每个服务器只能有一个主功能，以防止需要来自共存同一服务器上的不同安全级别的功能。（例如，web服务器，数据库服务器和DNS应该在不同的服务器来实现。） ***注意：** 当虚拟化技术都在使用，实现每个虚拟系统部件只有一个主要功能。*	**2.2.1.a** 选择系统部件的一个样品和检查系统配置，以验证仅一个主要功能是每个服务器实现。 **2.2.1.b** 如果使用虚拟化技术，检查系统配置，以验证仅一个主要功能是每个虚拟系统组件或设备实现。	如果需要不同安全级别的服务器功能位于同一台服务器上，具有较高的安全性需求函数的安全水平将由于较低的安全功能存在而降低。此外，具有较低安全级别的服务器功能，可在同一台服务器上引入安全漏洞的其他功能。通过考虑不同的服务器功能安全需求的系统配置标准和相关流程的一部分，组织可以确保需要不同安全级别的功能做在同一台服务器上不可同时存在。
2.2.2 只启用必要的服务，协议，进程等，如需要对系统的功能。	**2.2.2.a** 选择系统组件样本，并检查启用的系统服务，守护程序和协议验证，只有必要的服务或协议都被启用。 **2.2.2.b** 确定启用任何不安全的服务，守护程序或协议和面试人员核实他们每个记录配置标准合理。	如要求陈述1.1.6，但是也有一些常用的个人恶意破坏网络，一个企业可能需要（或已默认启用）许多协议。包括这一要求作为一个组织的配置标准和相关流程的一部分可确保只有必要的服务和协议都被启用。
2.2.3 实施额外的安全功能对于任何需要的服务，协议，或者被认为是不安全的守护进程。	**2.2.3** 检查配置设置，以确认安全特性文件，并为所有不安全的服务，守护程序或协议来实现。	启用安全功能，安装与配置不安全的环境中之前部署会阻止服务器新的服务器。确保所有不安全的服务，协议和守护进程充分适当的安全保护功能，使之更难以对恶意个人采取网络中的优势妥协常用点。请参阅行业标准和最佳做法的信息强大的加密和安全协议（例如，NIST SP 800-52和SP 800-57，OWASP等）。 ***注意：** SSL / TLS早期不考虑强大的加密，并且可以不被用作安全控制，除了由被验证为不易受已知漏洞，并如附录A2定义它们所连接的终端点POS POI终端。*

PCI DSS要求	测试程序	指导
2.2.4 配置系统安全参数，以防止误操作。	**2.2.4.a 面试系统管理员和/或安全管理人员，以确认他们有系统组件的共同**安全参数设置的知识。	系统配置标准和相关流程应具体讨论具有已知的安全问题对于正在使用的每个类型的系统的安全设置和参数。为了让系统进行安全配置，负责配置和/或管理系统的人员必须在应用到系统的特定安全参数和设置知识渊博。
	2.2.4.b 检查系统配置标准，以验证是否包含常见的安全参数设置。	
	2.2.4.c 选择系统部件的一个样品并检查常见的安全参数，以验证它们适当设置，并根据配置的标准。	
2.2.5 删除所有不必要的功能，如脚本，驱动程序，功能，子系统，文件系统和不必要的Web服务器。	**2.2.5.a 选择系统部件的一个样品并检查配置，以验证所有不必要的功能**（例如，脚本，驱动程序，特征，子系统，文件系统等）被除去。	不必要的功能可提供更多的机会为恶意个人获得对系统的访问。通过删除不必要的功能，企业可以集中精力确保所需，并减少未知的功能将被利用的风险的功能。在服务器硬化标准和过程，包括这个（通过移除/禁用FTP或web服务器如果服务器将不被执行的那些功能，例如，）解决了与不必要的功能相关联的特定的安全隐患。
	2.2.5.b. 检查文档和安全参数，以验证启用的功能是记录并支持安全配置。	
	2.2.5.c. 检查文档和安全参数，以验证仅记录功能存在于采样系统组件。	
2.3 加密使用强大的加密所有非控制台管理访问。	**2.3 选择系统部件的一个样品，并验证非控制台管理访问是通过执行以下加**密：	如果非控制台（包括远程）管理不使用安全认证和加密通信，敏感的行政或业务层面的信息（如管理员ID和密码），可以透露给窃听者。恶意个人可以使用该信息来访问网络，成为管理员，并窃取数据。
	2.3.A 观察的管理员登录到每个系统并检查系统配置，以验证请求管理员的密码之前强大的加密方法被调用。	
	2.3.B 在系统回顾服务和参数文件，以确定Telnet和其他不安全的远程登录命令不适用于非控制台访问。	明文协议（如HTTP，Telnet等）不加密流量或登录细节，很容易使窃听者截获这些信息。

（接下页）

PCI DSS要求	测试程序	指导
	2.3.c 观察的管理员登录到每个系统验证到任何基于Web的管理界面，管理员访问与强大的加密加密。	被认为是“强密码”，行业认可的适当的主要优势和密钥管理协议应在地方**作为适用技术的使用类型。（请参阅“强大的加密”的** ***条款的PCI DSS和PA-DSS术语，缩写词和缩略词，*** **与行业标准和最佳实践，如**NIST SP 800-52和SP 800-57，OWASP等）
	2.3.d 检查供应商文档和面试人员核实了在使用中根据行业最佳做法和/或供应商的建议实施的技术，强大的加密。	***注意：SSL / TLS早期不考虑强大的加密，并且可以不被用作安全控制，除了由被验证为不易受已知漏洞，并如附录A2定义它们所连接的终端点POS POI终端。***
2.4 保持在范围上的PCI DSS系统部件的清单。	**2.4.a** 检查系统库存来验证硬件和软件组件的列表被维持，并包括用于每个功能/应用的描述。	维护所有系统组件的最新列表将会使组织能够准确，高效地界定其范围的环境中实现PCI DSS控制。如果没有库存，一些系统组件可以被遗忘，被无意中从组织的配置标准之外。
	2.4.b 面试人员核实所记录的库存保持电流。	

PCI DSS要求	测试程序	指导
2.5 确保管理供应商违约等安全参数记录，在使用中，和已知的所有当事方的安全政策和操作程序。	**2.5** 检查文件和面试人员核实管理供应商违约等安全参数的安全政策和操作程序是： • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全政策和日常运作程序，以确保供应商的违约和其他安全参数被连续管理，以防止不安全的配置。
2.6 共享主机提供商必须保护每个实体的托管环境和持卡人数据。在详细介绍这些供应商必须满足特定要求 *附录A1：对共享主机提供商其他PCI DSS要求*。	**2.6** 执行测试程序 **A1.1** 通过 **A1.4** 在详细 ***附录A1：对共享主机提供商其他PCI DSS要求*** 共享主机提供商的PCI DSS评估，以确认共享托管提供商保护他们的实体（商家和服务提供商）托管环境和数据。	这是为了主办这次提供相同的服务器上共享多个客户端的主机环境提供者。当所有的数据都在同一台服务器上，并在单一环境的控制，往往是这些共享服务器上的设置不受个人客户管理。这使得客户端添加不安全功能和脚本影响所有其他客户端环境的安全; 从而很容易让恶意的个体妥协一个客户的数据，从而获取到所有其他客户的数据。看到 ***附录A1*** **对于要求的详细信息。**

保护持卡人数据

要求3：保护存储的持卡人数据

保护的方法，例如加密，截短，掩蔽，和散列是持卡人数据保护的关键组件。如果入侵者规避了其他的安全控制，并获得访问加密数据，如果没有适当的加密密钥，数据不可读和不可用的那个人。保护存储数据的其他有效的方法也应被视为潜在的风险缓解的机会。例如，对于最大限度地降低风险的方法包括不存储持卡人数据，除非绝对必要的，如果不需要完整的PAN截断持卡人数据，并使用终端用户通讯技术，**如电子邮件和即时消息不发送未受保护的PAN。请参阅 *PCI DSS和条款的PA-DSS术语，缩写词和缩略词* 对于"强加密"和其他PCI DSS术语的定义。**

PCI DSS要求	测试程序	指导
3.1 保持持卡人数据存储到最低限度通过实施数据保留和处置政策，程序和流程，包括至少对所有持卡人数据（CHD）存储以下内容： • 限制数据存储量和滞留时间延长到这是需要的法律，法规和/或业务需求 • 持卡人数据的具体保留要求 • 流程数据的安全删除不再需要时 • 用于鉴定和安全地删除超过定义的保留存储的持卡人数据的季度过程。	**3.1.A 检查数据保留和处置政策，程序和流程，以验证它们包括所有的持卡人数据**（CHD）存储以下内容： • 限制数据存储量和滞留时间延长到这是需要的法律，法规和/或业务需求。 • 持卡人数据保留的具体要求（例如，持卡人的数据需要保持X期间用于Y业务的原因）。 • 需要的法律，法规或业务原因时不再持卡人数据的安全删除过程。 • 用于鉴定和安全地删除超过定义的保留要求存储的持卡人数据的季度过程。	正式的数据保留策略确定需要什么样的数据被保留，并在该数据驻留，因此它可以被安全地销毁或只要它不再需要删除。可以存储授权之后唯一持卡人数据是主帐号或PAN（不可读），到期日期，持卡人姓名，和服务代码。理解持卡人数据位于是必要的，这样它可以被正确地保留或设置当不再需要的。为了确定适当的保存要求，实体首先需要了解自己的业务需求，以及适用于他们的行业的任何法律或法规的义务，和/或适用于数据的类型被保留。
	3.1.B 面试人员核实： • 存储持卡人数据的所有位置都包括在数据保留和处置过程。 • 或者每季自动或手动过程是否到位，以确定和安全地删除存储的持卡人的数据。 • 季度自动或手动处理持卡人数据的所有位置进行。	

（接下页）

PCI DSS要求	测试程序	指导
	3.1.c 对于存储持卡人数据的系统组件的一个示例： • 检查文件和系统记录，以验证存储的数据不超过数据保留策略定义的要求 • 观察删除机制来验证数据被安全地删除。	识别和删除已经超过其指定的保留期限存储的数据，从而防止数据的不必要的保留，其不再需要。该过程可以是自动的或手动的或两者的组合。例如，一个程序化的过程（自动或手动），以找到并删除数据和/或可以执行数据存储区的人工审核。实现安全的删除方法确保当不再需要它的数据无法恢复。 ***记住，如果你不需要它，不要保存它！***
3.2 不要授权之后，敏感的验证数据存储（即使加密）。 如果收到敏感验证数据，使授权过程完成后，所有的数据无法恢复。 *这是允许的发行和支持发行服务，如果存储敏感验证数据的公司：* • *有商家理由和* • *的数据被安全地存储。* 敏感的验证数据包括数据，如以下要求引 3.2.1通过3.2.3：	**3.2.a 对于发行人及/或支持发卡服务并存储敏感的认证数据，审查政策和面试人员核实公司有敏感的验证数据的存储文件化的商业理由。** **3.2.b 对于发行人及/或支持发卡服务并存储敏感验证数据，检查数据存储和系统配置，以验证该敏感的验证数据安全的公司。** **3.2.c 对于所有其他实体，如果收到敏感验证数据，审查政策和程序，并检查系统配置，以验证授权后的数据不保留。**	敏感的验证数据包括全磁道数据，卡验证代码或值，PIN数据。授权之后，敏感的身份验证数据的存储是禁止的！这个数据是恶意的个体，因为它允许他们产生伪造支付卡并创建欺诈交易非常有价值的。实体发行的支付卡或执行或支持发行服务通常会创建和控制敏感验证数据的发布功能的一部分。这是允许的执行，有利于企业，或支持发行服务，以存储敏感验证数据，只有当他们有合法的业务需要来存储这些数据。 应当指出的是，所有的PCI DSS要求适用于发行人，以及为发行人及发行人的处理器，唯一的例外是，如果有正当理由这样做敏感的认证数据可以被保留。有正当的理由之一被设置用于发行人的功能的性能是必要的，方便没有之一。任何这样的数据必须安全，并符合所有PCI DSS和具体的支付品牌的要求储存。 *（接下页）*

PCI DSS要求	测试程序	指导
	3.2.d 对于所有其他实体，如果收到敏感验证数据，审查程序和审查流程，安全地删除数据，以验证数据是不可恢复的。	对于非发卡实体，保持敏感的验证数据后授权是不允许的。
3.2.1 不存储任何曲目的完整内容（从位于卡背面的磁条，包含在芯片上的等效数据，或其他地方）的授权后。该数据也可称为全磁道，磁道1，磁道2，和磁条数据。 ***注意：在业务的正常过程中，从以下磁条数据元素可能需要保留：*** • *该持卡人姓名* • *主账号（PAN）* • *截止日期* • *服务代码* *为了最大限度地减少风险，需要企业只存储这些数据元素。*	**3.2.1 对于系统组件的一个样本，检查数据源，包括但不限于以下内容，并验证**从卡或等效数据的芯片背面的磁条任何轨道的全部内容授权之后没有存储： • 输入的交易数据 • 所有日志（例如交易，历史，除错，错误） • 历史文件 • 跟踪文件 • 几个数据库模式 • 数据库的内容。	如果全程跟踪数据存储，恶意个人谁获得的数据可以用它来复制支付卡和完整的欺诈性交易。
3.2.2 不存储卡验证代码或值（三位数或四位数字印在正面或背面的支付卡的用于验证卡不可–本交易）授权之后。	**3.2.2 对于系统组件的一个样本，检查数据源，包括但不限于以下内容，验证该**三位或四位卡验证代码或值印刷在卡或签名板（CVV2，CVC2的前，CID，CAV2数据）不被存储的授权之后： • 输入的交易数据 • 所有日志（例如交易，历史，除错，错误） • 历史文件 • 跟踪文件 • 几个数据库模式 • 数据库的内容。	卡验证代码的目的是为了保护“卡不在场”的交易 - 互联网或邮购/电话订购（MO / TO）交易，其中消费和卡不存在。如果此数据被窃取，恶意个人可以执行欺诈互联网和MO / TO交易。

PCI DSS要求	测试程序	指导
3.2.3 不存储个人识别号码（PIN）或授权后的加密PIN块。	**3.2.3** 对于系统组件的一个样本，检查数据源，包括但不限于下面，并验证PIN和加密PIN块授权之后不存储： • 输入的交易数据 • 所有日志（例如交易，历史，除错，错误） • 历史文件 • 跟踪文件 • 几个数据库模式 • 数据库的内容。	这些值应该只知道持卡人或银行发卡。如果此数据被窃取，恶意个人可以执行欺诈基于PIN的借记卡交易（例如，ATM取款）。
3.3 显示时面膜PAN（前六位和最后四位是要显示的最大位数），这样，只有拥有合法业务需求的人员能看到比前六/最后四个PAN的数字更多。 ***注意：** 这个要求并不取代为销售终端（POS）收据点 - 为持卡人数据，例如，法律或支付卡品牌要求显示在地方更严格的要求。*	**3.3.a** 检查掩蔽的PAN验证的显示书面政策和程序： • 需要访问的显示器多角色的列表中的前六/最后四个（包括完整的PAN）的记录，具有合法经营需要为每个角色有这样访问起来。 • 显示时，使得只有合法业务需求的人员能看到比前六/最后四个PAN的数字更PAN必须屏蔽。 • 所有角色不是特别授权看到完整的PAN只能看到蒙面的PAN。	未经授权的个人而得到全PAN的项目，如计算机屏幕，支付卡收据，传真，或文件报告可能会导致该数据的显示和欺诈使用。确保全PAN只显示那些有合法业务需要查看完整的PAN减少获得访问PAN数据的非授权人员的风险。 掩蔽方法应始终确保只显示必要的最小位数来执行特定的业务功能。例如，如果只需要最后四位数字来执行业务功能，可以屏蔽PAN，使执行该功能的个人只能查看最后四位数字。作为另一个例子，如果一个函数需要访问路由目的银行识别号（BIN），仅揭露该函数在BIN的数字（传统的前六位数字）。这一规定涉及PAN的保护
	3.3.b 检查系统配置，以验证全PAN仅显示与记录的业务需要的用户/角色和PAN为掩盖所有其他请求。	
	3.3.c 检查PAN的显示装置（例如，在屏幕上，在纸上收据），以验证显示持卡人数据时的PAN被屏蔽，而只有那些具有合法业务需求都能够看到比前六/最后四位的数字更泛。	***显示*** **在屏幕上，纸质收据，打印输出等，且不能与要求相混淆** **3.4 PAN时的保护** ***存储*** **在文件，数据库等。**

PCI DSS要求	测试程序	指导
3.4 通过以下任一方式渲染PAN不可读的任何地方存储（包括便携式数字媒体，备份媒体，并在日志中）： • 基于强大的加密单向散列（哈希必须是整个PAN的） • 截断（散列不能用来代替PAN的截段） • 索引令牌和焊盘（焊盘必须安全地存储） • 强大的加密与相关密钥管理流程和程序。 ***注意：这是一个怀有恶意的个体相对平凡的努力来重建原始PAN数据，如果他们有机会获得既PAN的截断和散列版本。当散列和相同的PAN截短形式存在于一个实体的环境，更多的控制必须到位，以确保散列和截断版本不能被关联到重建原始PAN。***	**3.4.a 检查有关用来保护PAN系统，包括供应商，系统/过程的类型，以及加密算法**（如果适用），以验证该PAN用以下任一方法的不可读文档： • 基于强大的加密单向哈希， • 截断 • 指数令牌和垫，与垫被安全地存储 • 强大的加密，与相关密钥管理流程和程序。	存储在主存储（数据库，或平面文件如文本文件电子表格）以及非主存储（备份，审计日志，异常或故障排除日志）的PAN都必须受到保护。可用于基于强大的加密单向散列函数来呈现持卡人数据不可读。当没有必要取回原来的号码（单向哈希值是不可逆的）Hash函数是适当的。建议，但目前没有要求，即一个附加的，随机的输入值被添加到持卡人数据散列，以减少攻击者比较针对数据的可行性（以及从所述PAN）预先计算的散列的表之前值。截短的意图是永久删除PAN数据段，使得仅一部分（一般不超过第一六位与后四位）PAN的被存储。索引标记是加密令牌，取代基于用于不可预测的值的给定索引的PAN。一次性垫是其中一个随机生成的私有密钥仅被使用一次来加密一个消息，然后，使用匹配的一次性密码和密钥解密的系统。
	3.4.b 检查几个表或文件从数据储存库的样品，以验证PAN不可读（即，不存储在纯文本）。	
	3.4.c 检查可移动介质（例如，备份磁带）的一个样本，以确认PAN不可读。	
	3.4.d 检查审计日志，包括支付应用程序日志的样本，以确认PAN不可读或不存在在日志中。	
	3.4.e 如果 相同的PAN的散列和截短形式存在于环境中，检查实施的控制，以验证该散列和截短版本不能被关联到重建原始PAN。	**强加密的意图（如在定义 *PCI DSS和条款的PA-DSS术语，缩写词和缩略词*）的是，所述加密可以基于业界测试和接受算法（不是专**有或“主页 - 生长”算法）具有较强的密码密钥。由给定的PAN的散列和截断版本相关，恶意个人可以很容易地获取原始的PAN值。防止这种数据的相关性控制将有助于确保原始PAN仍然无法读取。

PCI DSS要求	测试程序	指导
3.4.1 如果磁盘加密使用（而不是文件级或列级数据库加密），逻辑访问必须单独地和独立地的本机操作系统的认证和访问控制机制管理（例如，通过不使用本地用户帐户数据库或通用的网络登录证书）。解密密钥不能与用户帐户相关联。 ***注意：** 此要求适用于除了所有其他PCI DSS加密和键盘管理的要求。*	**3.4.1.a** 如果使用磁盘加密，检查配置和观察验证过程，以验证到加密文件系统经由与从本机操作系统的认证机制分开的机构来实现该逻辑访问（例如，不使用本地用户帐户数据库或一般网络登录凭据）。 **3.4.1.b** 观察过程和面试人员验证密钥安全地存储（例如，存储在有充分和强大的访问控制保护可移动媒体）。 **3.4.1.c** 检查的配置和观察的过程，以验证任何地方存储在可移动媒体持卡人数据进行加密。 ***注意：** 如果磁盘加密，不使用可移动介质进行加密，存储在该媒体上的数据需要通过一些其它方法无法读取。*	这一要求的目的是解决磁盘级加密的可接受渲染持卡人数据不可读。磁盘级加密加密的计算机上的整个磁盘/分区，并自动当授权用户请求它解密的信息。许多基于磁盘加密解决方案拦截操作系统读/写操作，并进行相应的密码变换，而不比提供密码或短语通过在系统启动时或在会议开始时，其它用户的任何特殊操作。基于磁盘级加密这些特点，都符合这一要求，该方法不能： 1）使用相同的用户帐户认证器作为操作系统，或 2）使用与相关或从系统的本地用户帐户数据库或一般的网络登录凭据获得的解密密钥。全磁盘加密有助于保护在磁盘的物理损失的事件数据，因此可能适用于存储持卡人数据的便携式设备。
3.5 编制和实施程序，以保护用于保护免遭泄露与误存储持卡人数据的密钥： ***注意：** 这一要求适用于用来加密存储持卡人数据的密钥，也适用于用于保护数据的加密密钥，这种密钥 - 加密密钥必须至少与数据加密密钥一样强的密钥加密密钥。*	**3.5** 检查密钥管理政策和程序，以验证过程被指定为保护用于防止泄露和滥用持卡人数据的加密密钥，并至少包括以下内容： • 访问键仅限于数量最少的必要保管人。 • 密钥加密密钥至少与他们保护数据 - 加密密钥一样强。 • 密钥加密密钥从数据 - 加密密钥分开存储。 • 密钥安全地存储在尽可能少的地点和形式。	加密密钥必须严加保护，因为那些谁获得访问将能够解密数据。密钥加密密钥，如果使用的话，必须至少一样强，以数据加密密钥，以确保对数据进行加密，以及使用该密钥加密数据的密钥的适当保护。保护密钥被泄露和滥用的要求适用于数据加密密钥和密钥加密密钥。因为一个键 - 加密密钥可以授权访问数据 - 许多加密密钥，该密钥加密密钥需要强有力的保护措施。

PCI DSS要求	测试程序	指导
3.5.1 ***只有服务提供商附加要求：*** **维持密码体系结构，**其包括的记录的描述： • 所有的算法，协议和用于持卡人数据的保护密钥，包括密钥的强度和有效期的详细信息 • 每个密钥的密钥的使用说明 • 任何HSM产品的库存及用于密钥管理的其他的SCD	**3.5.1** **面试责任人员和审查文件，验证文件的存在是为了描述加密架构，包括：** • 所有的算法，协议和用于持卡人数据的保护密钥，包括密钥的强度和有效期的详细信息 • 每个密钥的密钥的使用说明 • 任何HSM产品的库存及用于密钥管理的其他的SCD	***注意：此要求仅适用于被评估的实体是服务提供商。*** 维持密码体系结构的当前文档允许一个实体了解算法，协议和加密用来保护持卡人数据键，以及生成，使用和保护密钥的设备。这使得实体，以跟上不断变化的威胁到他们的架构，使他们能够计划更新由不同的算法/密钥强度变化所提供的保障水平的步伐。维护这些文件还允许实体检测丢失或丢失的钥匙或密钥管理设备，并确定擅自增加自己的加密架构。
3.5.2 **限制访问密钥，以尽可能少的必要保管人。**	**3.5.2** **检查用户访问列表，以验证访问键仅限于数量最少的必要保管人。**	应该有极少数谁有权访问加密密钥（减少撕心裂肺未经授权者可见持卡人数据的潜力），通常只有那些谁拥有钥匙保管责任。

PCI DSS要求	测试程序	指导
3.5.3 存储用于加密密钥和私有密钥/解密在任何时候都以下列形式之一（或更多）的持卡人数据： • 与至少与数据 - 加密密钥作为强密钥加密密钥加密，并且从该数据加密密钥分开存储 • 内的安全的加密装置（例如，硬件（主机）的安全模块（HSM）或PTS批准的点的交互装置） • 作为至少两种全长的关键部件或密钥份，根据一工业接受方法 ***注意：它不是必需的公用密钥存储在这些形式之一。***	**3.5.3.a 检查文件的程序，以验证用于加密的加密密钥/解密持卡人数据仅必须在**任何时候都在以下形式中的一种（或多种）存在。 • 与至少与数据加密密钥一样强密钥加密密钥加密，并且从该数据加密密钥分开存储 • 内的安全的加密装置（例如，硬件（主机）的安全模块（HSM）或PTS批准的点的交互装置） • 作为关键部件或密钥份，按照一种业内可接受的方法	加密密钥必须安全地存储，以防止未经授权的或不必要的访问，可能会导致持卡人数据的曝光。这并不意味着该密钥加密密钥进行加密，但是他们免遭泄露与误被保护，如要求3.5定义。如果使用密钥加密密钥，存储在从数据 - 加密密钥物理和/或逻辑上分离的位置上的密钥加密密钥减少到两个键的未授权访问的风险。
	3.5.3.b 检查系统配置和密钥存储位置，以验证所使用的密码密钥来加密/解密中在任何时候都采用以下形式的一个（或多个）存在持卡人的数据。 • 加密与密钥加密密钥。 • 内的安全的加密装置（例如，硬件（主机）的安全模块（HSM）或PTS批准的点的交互装置）。 • 作为关键部件或密钥份，按照一种业内可接受的方法。	
	3.5.3.c 无论使用的密钥加密密钥，检查系统配置和密钥存储位置来验证： • 密钥加密密钥至少与他们保护数据 - 加密密钥一样强。 • 密钥加密密钥从数据 - 加密密钥分开存储。	
3.5.4 存储在尽可能少的地方加密密钥。	**3.5.4 检查密钥存储位置和观察的过程来验证密钥存储在尽可能少的位置。**	在最少的位置存储加密密钥可帮助企业跟踪和监控所有关键位置，并最大限度地减少潜在的钥匙暴露在未经授权的第三方。

PCI DSS要求	测试程序	指导
3.6 全面编制和实施用于用于持卡人数据，包括以下内容的加密密钥的所有密钥 - 管理流程和程序： ***注意：** 密钥管理众多的行业标准都可以从各种资源，包括NIST，可在http://csrc.nist.gov找到。*	**3.6.a** ***只有服务供应商的评估进一步的测试过程：*** **如果与他们的客户服务提供商共**享密钥传输或持卡人数据的存储，检查服务提供商提供给他们的客户，以确认它包含了如何安全地传输更新客户键指导，存储，并根据文件符合要求3.6.1通过以下3.6.8。	在该加密密钥的管理方式是加密解决方案的持续安全的一个关键部分。一个良好的键 - 管理过程中，无论是手动或自动的作为加密产品的一部分，是基于行业标准和地址通过3.6.8 3.6.1在所有关键要素。提供指导客户如何安全地传输，存储和更新加密密钥可以帮助防止经营不善或泄露给未经授权的实体键。这个要求适用于用于加密存储的持卡人数据键，以及任何相应的键 - 加密密钥。 ***注意：** 测试程序3.6.a是仅适用如果被评估的实体是服务提供商的附加程序。*
	3.6.b 检查对用于持卡人数据的加密密钥的密钥管理程序和过程，并执行以下：	
3.6.1 强大的加密密钥的生成	**3.6.1.a** 验证密钥管理程序指定如何生成强密钥。	**加密解决方案必须产生强键，如在限定的** *PCI DSS和条款的PA-DSS术语，缩写词和缩略词* 在"密钥生成"。强大的加密密钥的使用显著增加加密的持卡人数据的安全级别。
	3.6.1.b 观察用于生成密钥以验证生成强密钥的程序。	
3.6.2 安全密钥分发	**3.6.2.a** 验证密钥管理程序规定如何安全地分发密钥。	加密解决方案必须安全地分发密钥，这意味着密钥只分配到3.5.2的要求确定的监护人，并且永远不会分布在明确的。
	3.6.2.b 观察为分发密钥来验证密钥被安全地分发的方法。	
3.6.3 安全密钥存储	**3.6.3.a** 验证密钥管理程序指定如何安全地存储密钥。	加密解决方案必须安全地存储密钥，例如，通过将它们与一键 - 加密密钥加密。如果没有适当的保护存储密钥可以提供访问攻击者，导致解密和持卡人数据泄露。
	3.6.3.b 观察，用于存储的密钥来验证密钥被安全地存储在方法。	

PCI DSS要求	测试程序	指导
3.6.4 已达到其加密周期的结尾密钥加密密钥的变化（例如，在经过规定的时间段已经过去和/或一定量的密文已经由一个给定的密钥产生之后），如由相关联的定义的应用程序供应商或密钥所有者，并基于行业最佳做法和准则（例如，NIST特刊800-57）。	**3.6.4.a** 验证密钥管理程序包括用于在使用中每个键型定义的加密周期和用于在所定义的加密周期（一个或多个）的结束键的变化限定的方法。 **3.6.4.b** 面试人员确认键在定义的加密周期（S）的一端开始变化。	甲加密周期是时间跨度期间其中特定密码密钥可以被用于其限定的目的。用于限定加密周期的考虑包括，但不限于，底层算法，大小或密钥长度，密钥泄露的风险，并且数据的敏感性的强度被加密。加密密钥的定期更换，当钥匙已经达到了他们的加密周期的结束是必要的，以尽量减少别人的获得加密密钥，并用它们来解密数据的风险。
3.6.5 在认为必要时，当密钥的完整性被削弱了键的退休或替换（例如，归档，破坏和/或撤销）（例如，用一个明文关键组成部分的知识雇员的离开），或按键被怀疑受到损害。 ***注意：*** *如果退役或更换的密码密钥需要被保留，这些键必须被牢固地（例如，通过使用密钥加密密钥）存档。存档的加密密钥只能用于解密/验证。*	**3.6.5.a** 验证密钥管理程序如下指定进程： • 当密钥的完整性已被削弱键退休或更换。 • 更换已知或疑似泄露的密钥的。 • 退休或更换后保留的任何密钥不用于加密操作。 **3.6.5.b** 面试人员核实以下过程实现： • 键是退休或当密钥的完整性已被削弱，包括当有人用钥匙的知识离开公司，必要时进行更换。 • 如果已知或怀疑被泄露的密钥将被替换。 • 退休或更换后保留的任何密钥不用于加密操作。	已知或怀疑密钥中不再使用或需要，或键被破坏，应予以撤销和/或销毁，以确保密钥不能再使用。如果这样的按键需要保持（例如，为了支持归档，加密数据），他们应大力保护。加密溶液应提供和促进的处理，以取代到期更换或已知是或疑似被，泄露的密钥。

PCI DSS要求	测试程序	指导
3.6.6 如果使用手动明文密钥管理操作，这些操作必须使用分割知识和双重控制进行管理。 ***注意：** 手动键 - 管理操作的实例包括，但不限于：密钥生成，传输，加载，存储和破坏。*	**3.6.6.a** 确认手动明文密钥管理程序使用下列指定的过程： • 键，以便关键组件是至少两个人谁只有拥有自己的关键部件知识的控制下分离的知识; 和 • 按键的双重控制，使得至少需要两个人来执行任何密钥管理操作，没有一个人可以访问认证材料（例如，口令或密钥）的另一种。	分离的知识和密钥的双重控制用于消除能够访问整个键一个人的可能性。这种控制适用于手动密钥管理操作，或密钥管理不被加密产品来实现。分离的知识是在两个或两个以上的人分别有关键部件，每个人只知道自己的关键组成部分，个别关键零部件传达没有原始密钥的知识的方法。
	3.6.6 b 面试人员和/或观察过程，以确认手动明文密钥与管理： • 拆分知识， • 双控	双控需要两个或更多的人来执行的功能，并没有任何一个人可以访问或使用另一人的认证材料。
3.6.7 防止加密密钥的未授权替代。	**3.6.7.a** 验证密钥管理程序指定进程，以防止按键的未经授权的替换。	加密溶液不应该允许或接受来自未经授权源的或意外的过程来键的取代。
	3.6.7.b 面试人员和/或观察的过程，以验证防止键的未经授权的替换。	
3.6.8 要求对密钥托管人正式承认他们理解和接受他们的键 - 托管人的责任。	**3.6.8.a** 验证密钥管理程序，指定过程的关键托管人确认（以书面或电子），他们理解和接受他们的键 - 托管人的责任。	这一过程将有助于确保充当钥匙保管人提交到主要的托管人角色，理解和接受的责任人。
	3.6.8.b 观察资料或表明钥匙保管人已确认（以书面或电子），他们理解和接受他们的密钥 - 托管人职责的其他证据。	
3.7 确保各项保护存储的持卡人数据的安全政策和操作程序记录，在使用中，和已知的所有当事方。	**3.7** 检查文件和采访人员，以验证安全政策和运作程序来保护存储的持卡人数据有： • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全策略和管理一个连续的基础上持卡人数据的安全存储记录的操作程序。

要求4：在各种开放的公共网络持卡人数据的加密传输

敏感信息必须在传输过程中过度，很容易被恶意的人进入网络进行加密。配置不当的无线网络和传统的加密和认证协议的漏洞仍然是恶意个人谁利用这些漏洞获取对持卡人数据环境的特权访问的目标。

PCI DSS要求	测试程序	指导
4.1 使用强大的加密和安全协议传输在开放的公共网络，其中包括以下过程中保护敏感的持卡人数据： • 只有可信的密钥和证书被接受。 • 在使用该协议仅支持安全版本或配置。 • 加密强度是适合使用的加密方法。 *开放的例子，公共网络包括但不限于：* • *互联网* • *无线技术，包括802.11和蓝牙* • *蜂窝技术，例如，全球移动通信系统通信系统（GSM），码分多址（CDMA）* • *通用分组无线业务（GPRS）* • *卫星通信*	**4.1.a 确定持卡人数据的发送或在开放的公共网络接收到的所有位置。检查记录**标准，并比较系统配置，以验证使用的安全协议和强大的加密功能的所有位置。	敏感信息必须传输通过公共网络中被加密，因为它很容易与常见的恶意个人拦截和/或在运输过程中转移数据，而。持卡人数据的安全传输，需要利用可信密钥/证书，用于传输安全协议，和适当的加密强度来加密持卡人数据。从不支持所需的加密强度，这将导致不安全的连接系统的连接请求，不应该被接受。请注意，某些协议的实现（如SSL，SSH V1.0，和TLS早期）已经知道，一个攻击者可以用它来获得受影响的系统的控制的漏洞。取其安全协议时，确保其配置为仅使用安全版本和配置，以防止在使用不安全的连接 - 例如，通过仅使用受信任的证书和仅支持强加密（不支持较弱，不安全的协议或方法）。验证证书是可信的（例如，没有过期，并从受信任的源发行）有助于确保安全连接的完整性。
	4.1.b 审查报告的政策和程序，以验证过程以下规定： • 验收只有可信密钥和/或证书的 • 对于所使用的协议只支持安全的版本和配置（即不安全版本或配置不受支持） • 为了实现每所使用的加密方法正确的加密强度	
	4.1.c 选择和它们发生（例如，通过观察系统进程或网络流量），以验证所有持卡人数据与运输过程中强大的加密加密观察入站和出站传输的一个样品。	
	4.1.d 检查密钥和证书，以确认只有受信任的密钥和/或证书被接受。	
	4.1.e 检查系统配置，以验证该协议是实现仅使用安全配置，并且不支持不安全的版本或配置。	
	4.1.f 检查系统配置，以确认正确的加密强度为正在使用的加密方法来实现。（查看供应商建议/最佳实践。）	*（接下页）*

PCI DSS要求	测试程序	指导
	4.1.g 对于TLS实施方式中，检查系统配置以验证持卡人每当数据被发送或接收的TLS被启用。例如，对于基于浏览器的实现： • “HTTPS”显示作为浏览器的通用记录定位符（URL）协议，和 • 如果“HTTPS”显示为URL的一部分持卡人数据的唯一要求。	一般情况下，该网页的网址应该以“HTTPS”和/或web浏览器在浏览器窗口某处显示一个挂锁图标开始。许多TLS证书供应商还提供了一个非常明显的扣钉的验证有时被称为“安全密封”，“安全站点密封”或“安全信任印章”）- 这可以提供点击密封透露有关信息的能力网站。请参阅行业标准和最佳实践的信息，强大的加密和安全协议（例如，NIST SP 800-52和SP 800-57，OWASP等） ***注意：** SSL / TLS早期不考虑强大的加密，并且可以不被用作安全控制，除了由被验证为不易受已知漏洞，并如附录A2定义它们所连接的终端点POS POI终端。*
4.1.1 确保无线网络传输持卡人数据或连接到持卡人数据环境，使用行业最佳实践来实现认证和传输强加密。	**4.1.1 识别所有的无线网络发送持卡人数据或连接到持卡人数据环境。检查记**录标准，并比较系统配置设置来验证标识的所有无线网络的以下内容： • 行业最佳实践来实现认证和传输强加密。 • 弱加密（例如，WEP，SSL）不被用作用于认证或传输的安全控制。	恶意用户使用免费的和广泛使用的工具来窃听无线通信。强大的加密的使用可以帮助整个无线网络的敏感信息的限制披露。用于认证和持卡人数据传输强加密需要防止恶意用户获得接入无线网络或利用无线网络来访问其他内部网络或数据。

PCI DSS要求	测试程序	指导
4.2 切勿通过终端用户通讯技术发送未受保护的PAN（例如，电子邮件，即时消息，短信，聊天等）。	**4.2.a** 如果最终用户的消息传递技术被用于发送持卡人数据，观察过程用于发送PAN和它们发生验证时，它是通过终端用户通讯技术传送PAN为不可读或具有强加密固定检查出站传输的一个样品。	电子邮件，即时消息，短信和聊天可以通过数据包嗅探跨内部和公共网络在分娩过程中很容易被截获。不要使用这些通讯工具，除非它们被配置为提供强大的加密发送PAN。此外，如果实体通过终端用户通讯技术要求PAN，实体应提供的工具或方法，以保护使用强大的加密这些知会或提供的PAN传输之前不可读。
	4.2.b 审查书面政策以验证策略，指出未受保护的PAN不通过终端用户通讯技术发送的存在。	
4.3 确保用于加密持卡人数据的传输被记录在案，在使用中，和已知的所有当事方的安全政策和操作程序。	**4.3** 检查文件和采访人员，以验证安全政策和操作程序，用于加密持卡人数据的传输是： • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全策略和管理一个连续的基础上持卡人数据的安全传输操作程序。

维护漏洞管理计划

要求5：防范恶意软件的所有系统，并定期更新杀毒软件或程序

恶意软件，通常被称为“恶意软件”-包括病毒，蠕虫，而且在许多米的商务批准的活动，包括员工电子邮件和使用互联网，移动计算机和存储设备木马，进入网络，导致开采的系统漏洞。防病毒软件必须经常受恶意软件的所有系统被用来保护系统免受当前和不断变化的恶意软件威胁。其他反恶意软件解决方案可能被视为补充到反病毒软件; 然而，这些额外的解决方案不更换需要反病毒软件必须到位。

PCI DSS要求	测试程序	指导
5.1 上常见的感染恶意软件（特别是个人电脑和服务器中的所有系统上部署防病毒软件。	**)5.1 对于系统组件，包括通常受恶意软件影响所有操作系统类型的样本，验证是否**适用的反病毒技术存在防病毒软件部署。	存在使用广泛发布漏洞攻击络绎不绝，通常被称为“零日”（即利用了先前未知漏洞的攻击），反对以其他方式固定系统。如果没有防病毒解决方案，定期更新，恶意软件的这些新的形式可以攻击系统，禁用网络，或导致数据的妥协。
5.1.1 确保防病毒程序能够检测，消除和防止所有已知类型的恶意软件。	**5.1.1 审查供应商文档，检查防病毒配置，以验证防病毒程序;** • 检测所有已知类型的恶意软件， • 删除所有已知类型的恶意软件，以及 • 抵御所有已知类型的恶意软件。 *类型的恶意软件的示例包括病毒，木马，蠕虫，间谍软件，广告软件和rootkit。*	**这是为了防止重要 所有 类型和恶意软件的形式。**

PCI DSS要求	测试程序	指导
5.1.2 对于认为是不常见的感染恶意软件系统，定期进行评估，以识别和评估，以确认这些系统是否继续不需要杀毒软件演变的恶意软件。	**5.1.2** 面试人员核实演变的恶意软件进行监测和评估目前并不认为被普遍受恶意软件影响的系统，以确认这些系统是否继续不需要杀毒软件。	通常，大型机，中型计算机（诸如AS / 400）和类似的系统可能不是目前被共同定位或受恶意软件。但是，对于恶意软件的行业趋势变化很快，因此对于机构了解新的恶意软件，可能会影响他们的系统，例如，通过监控供应商的安全注意事项和防病毒新闻组，以确定他们的系统是否可能是很重要的从下新的和不断变化的恶意软件威胁的到来。在恶意软件趋势应该包括在新的安全漏洞，方法来解决新趋势的确定应纳入公司的配置标准和保护机制需要
5.2 确保所有的反病毒机制，保持如下： • 保持电流， • 执行定期扫描 • 产生这是每个PCI DSS要求保留审计日志 10.7。	**5.2.a** 检查政策和程序，以验证所需的反病毒软件和定义保持最新状态。	即使是最好的防病毒解决方案在效果有限的，如果他们不维护和保持电流与最新的安全更新，签名文件，或恶意软件保护。审计日志提供监控病毒和恶意软件活动和反恶意软件反应的能力。因此，至关重要的是，反恶意软件的解决方案被配置成生成审计日志，并且这些日志按照要求10进行管理。
	5.2.B 检查防病毒配置，包括主安装该软件，以验证反病毒机制是： • 配置为执行自动更新， • 配置为执行定期扫描。	
	5.2.c 检查系统组件，包括通常受恶意软件影响所有类型的操作系统，以验证样本： • 防病毒软件和定义是最新的。 • 定期扫描进行。	
	5.2.d 检查防病毒配置，包括主安装的软件和系统组件的样本，以验证： • 防病毒软件日志生成已启用， • 日志被保持在根据PCI DSS要求10.7。	

PCI DSS要求	测试程序	指导
5.3 确保防病毒机制有效运行，并且不能被禁用或由用户改变，除非管理层特别授权的情况下，逐案在有限的时间段。 ***注意：*** *反病毒解决方案，可如果有合法的技术需要暂时只禁用，因为授权管理层根据具体情况逐案。如果防病毒保护需要为特定目的而被禁用，则必须经过正式批准。额外的安全措施也可能需要的时间段，在此期间的防病毒保护不主动实施。*	**5.3.a 检查防病毒配置，包括主安装的软件和系统组件的样本，以验证防病毒软件正**在积极运行。	反病毒持续运行，是无法被改变将提供持续的安全防范恶意软件。
	5.3.b 检查防病毒的配置，包括主安装的软件和系统组件的样品，以验证该防病毒软件不能被禁用或由用户改变。	基于策略的控制的所有系统上使用，以确保反恶意软件保护，不能改变或禁止将有助于防止系统的弱点被恶意软件所利用。额外的安全措施也可能需要的时间周期中实现，在此期间防病毒保护不活跃，例如，从互联网上断开未受保护的系统，而防病毒保护被禁用，后运行一个完整的扫描重新启用的。
	5.3.c 采访专人负责观察的过程，以验证防病毒软件无法被用户停用或改变，除非管理层特别授权的情况下，逐案在有限的时间段。	
5.4 确保防护恶意软件的系统文件，在使用中，和已知的所有当事方的安全政策和操作程序。	**5.4 检查文件和采访人员，以验证安全政策和操作程序保护系统免受恶意软件主要**有： • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全策略和运作程序，以确保系统是一个连续的基础上免受恶意软件。

要求6：开发并维护安全系统和应用程序

不法个人使用安全漏洞获得对系统的特权访问。许多这些漏洞是由于厂商提供的安全补丁，这必须由管理系统实体进行安装固定。所有系统都必须拥有所有适当的软件补丁，以防止恶意个人和恶意软件的开发和持卡人数据的妥协。

***注意：** 相应的修补软件是进行了评估，充分测试，以确定补丁不与现有安全配置冲突的补丁。对于内部开发的应用程序，许多漏洞可以通过使用标准的系统开发流程和安全编码技术来避免。*

PCI DSS要求	测试程序	指导
6.1 建立一个流程来识别安全漏洞，利用安全漏洞信息外有信誉的来源，并分配风险等级（例如，“高”，“中”或“低”），以新发现的安全漏洞。 ***注意：** 风险排名应基于行业最佳实践，以及考虑的潜在影响。例如，对于排名漏洞标准可以包括考虑到CVSS基本分数的，和/或由供应商进行分类，和/或受影响的系统类型。评估漏洞和分配风险评级方法会根据企业的环境和风险 - 评估策略。风险排名应该在最低限度，确定被认为是一个“高风险”的环境中的所有漏洞。除了风险等级，如果他们对环境造成的迫在眉睫的威胁的漏洞可以被认为是“危急”，影响关键系统和/或将导致潜在的妥协如果不加以解决。关键系统的例子可以包括安全系统，面向公众的设备和系统，*	**6.1.a** 检查政策和程序，以验证过程以下定义： • 为了确定新的安全漏洞 • 要分配一个风险等级，以漏洞，其中包括所有的“高风险”和“关键”漏洞的识别。 • 要使用的安全漏洞信息，信誉外部来源。 **6.1.b** 采访专人负责观察的过程来验证： • 新的安全漏洞被识别。 • 风险等级评估被分配到包括所有的“高风险”和“关键”漏洞识别漏洞。 • 工作，以确定新的安全漏洞包括使用安全漏洞信息的信誉外部来源。	这一要求的目的是使企业跟上新的漏洞，该漏洞可能会影响他们的环境。对漏洞信息的来源应该是值得信赖的，通常包括供应商网站，行业新闻组，邮件列表，或者RSS提要。一旦企业确定一个漏洞，可能影响他们的环境，该漏洞会必须进行评估和排名的风险。因此，组织必须有一个适当的方法，在现有基础上评估漏洞和风险分配给排名这些漏洞。这不是由ASV扫描或内部漏洞扫描实现的，而这需要一个过程，积极监控漏洞信息行业人士。判断的风险（例如，如“高”，“中等”或“低”）允许组织鉴别，优先

PCI DSS要求	测试程序	指导
6.2 确保所有的系统组件和软件从已知的漏洞通过安装适用的供应商提供的安全补丁的保护。发布后一个月内安装关键的安全补丁。 ***注意：关键的安全补丁应根据要求6.1所定义的风险等级过程加以识别。***	**6.2.a 检查相关安全 - 补丁安装验证程序的政策和程序的定义：** • 发布后的一个月内适用的关键供应商提供的安全补丁的安装。 • 适当的时间帧之内的所有适用供应商提供的安全补丁（例如，三个月内）的安装。	存在使用广泛发布漏洞攻击络绎不绝，通常被称为“零日”（即利用了先前未知漏洞的攻击），反对以其他方式固定系统。如果最近的补丁没有关键系统上尽快实现，恶意个人可以利用这些漏洞来攻击或禁用系统，或访问敏感数据。优先补丁的关键基础设施，确保高优先级的系统和设备从漏洞尽快补丁发布后受到保护。优先考虑修补程序的安装，从而对重要的或有风险的系统安全补丁在30天内安装，以及其他低风险的补丁2-3个月内安装。这一要求适用于所有已安装的软件适用的修补程序，
	6.2.b 对于系统组件和相关软件的样本，比较每个系统上安装到最新的供应商安全补丁列表，确认以下的安全补丁列表： • 这适用的关键供应商提供的安全补丁安装版本后一个月内。 • 所有适用的供应商提供的安全补丁的适当的时间框架内安装的（例如，三个月内）。	
6.3 制定内部和外部的软件应用程序（包括应用程序基于Web的管理访问）安全地，如下所示： • 根据PCI DSS（例如，安全认证和记录） • 基于行业标准和/或最佳实践。 • 在整个软件开发生命周期。把信息安全 ***注意：这也适用于内部开发以及由第三方开发的定制软件或定制软件的所有软件。***	**6.3.a 检查书面软件开发流程，以验证该方法是基于行业标准和/或最佳实践。**	如果没有需求定义中包含的安全性，设计，软件开发的分析和测试阶段，安全漏洞可能无意或恶意地引入到生产环境中。了解敏感数据的应用程序，包括存储时，传输和处理时，内存可以帮助确定哪些需要保护的数据。
	6.3.b 检查书面软件开发流程，以核实信息安全是整个生命周期。	
	6.3.c 检查书面软件开发流程，以验证应用程序按照PCI DSS开发的软件。	
	6.3.d 面试软件开发者验证写软件开发过程中实现的。	

PCI DSS要求	测试程序	指导
6.3.1 删除开发，测试和/或自定义应用程序帐户，用户ID和应用程序之前，密码变得活跃或者向客户发布。	**6.3.1 检查书面软件开发程序和面试责任人员的应用程序投入生产或发布给客**户之前，以验证和/或密码被删除，该预生产和/或自定义应用程序账户，用户ID。	开发，测试和/或自定义应用程序账户，用户ID和密码应该从生产代码的应用程序变得活跃之前或发布给客户，因为这些项目可能放弃对应用程序的运行信息被删除。这些信息的占有可以方便应用的妥协和相关持卡人数据。
6.3.2 事前审查自定义代码，以释放到生产或客户，以识别任何可能的编码漏洞（使用手动或自动工艺），以包括至少以下： • 代码更改比原始代码作者的其他个人审查，并通过个人知识的有关代码审查技术和安全编码实践。 • 代码审查确保代码是根据开发的安全编码指南 • 适当的修正被释放之前实现。 • 代码审查结果进行审查并在发布之前管理层批准。 *（接下页）*	**6.3.2.a 检查书面软件开发程序和面试负责人员，以确认所有的自定义应用程**序代码的更改必须（使用手动或自动处理）进行审查，如下： • 代码更改比原始代码作者的其他个人审查，并通过个人谁是在代码审查技术和安全编码实践。 • 代码审查确保代码开发，根据安全编码指南（请参阅PCI DSS要求6.5）。 • 适当的修正被释放之前实现。 • 代码审查结果进行审查并在发布之前管理层批准。	在自定义代码中的安全漏洞通常被恶意利用的个体来访问网络和妥协的持卡人数据。 一个人的知识和代码审查技术经验应参与审查过程。代码审查应该比代码的开发者之外的人允许一个独立的，客观的审查进行。自动化工具或流程也可以代替人工审核使用，但请记住，它可能是困难的，甚至是不可能的自动化工具，以确定一些编码的问题。纠正错误编码代码之前被部署到生产环境或发布给客户防止代码暴露的环境中潜在的漏洞。故障代码也更加困难和昂贵，已部署或释放到生产环境后解决。

PCI DSS要求	测试程序	指导
注意： *代码审查这一要求适用于所有自定义代码（包括内部和面向公众的），作为系统开发生命周期的一部分。* *代码审查可以通过知识的内部人员或第三方进行。面向公众的Web应用程序也受到额外的控制，实施后，应对现有的威胁和漏洞，如PCI DSS要求6.6定义。*	**6.3.2.b 选择最近的自定义应用程序变化的一个样例，并确认自定义应用程序代码是根据6.3.2.a审查，上面。**	
6.4 按照变更控制流程和程序，使所有更改的系统组件。该过程必须包括以下内容：	**6.4 检查政策和程序，以验证定义如下：** • 开发/测试环境是从生产环境在适当位置执行的分离访问控制分开。 • 分配到开发/测试环境和那些分配到生产环境中的人员之间的职责分离。 • 生产数据（活的PAN）不用于测试或开发。 • 生产系统被激活之前的测试数据和帐户将被删除。 • 与实施安全补丁和软件修改的变更控制程序被记录在案。	如果没有适当的记录和执行变更控制，安全功能可以无意或故意忽略或无法工作，可能会发生违规行为的处理，或者可以引入恶意代码。
6.4.1 从生产环境独立的开发/测试环境，并执行与访问控制的分离。	**6.4.1.a 检查网络文档和网络设备配置，以验证开发/测试环境是从生产环境（多个）分离。**	由于开发和测试环境的不断变化的状态，他们往往比生产环境不太安全。如果没有环境之间有足够的分离，它可能用于生产环境是可能的，和持卡人数据，受到损害由于less-在测试或开发环境严格的安全配置和可能的漏洞。
	6.4.1.b 检查的访问控制设置以确认访问控制到位，以执行开发/测试环境和生产环境（多个）之间的分离。	

PCI DSS要求	测试程序	指导
6.4.2 开发/测试和生产环境之间的职责分离	**6.4.2** 观察分配到分配到的生产环境，以验证职责的分离是在开发/测试环境和生产环境之间进行开发/测试环境和人事程序和面试人员。	减少人员的数量与访问生产环境和持卡人数据的风险降至最低，并有助于确保访问仅限于与企业需要了解这些人。 这一要求的目的是从生产函数单独开发和测试功能。例如，开发者可以在开发环境中使用具有高特权管理员级别帐户，并与用户级访问生产环境的单独帐户。
6.4.3 生产数据（活的PAN）不用于测试或开发	**6.4.3.a** 观察测试流程和面试人员核实程序，以确保生产数据（活的PAN）不用于测试或开发。	安全控制通常不是在测试或开发环境一样严格。生产数据的使用提供了恶意的个人有机会获得生产数据（持卡人数据）未经授权的访问。
	6.4.3.b 检查测试数据的样品，以验证生产数据（活PAN）的不用于测试或开发。	
6.4.4 从系统组件的测试数据和账户删除的系统变为有效之前/投产。	**6.4.4.a** 观察测试流程和面试人员核实的测试数据和帐户被删除生产系统才能起作用。	系统组件之前变为活动的（在生产中），因为这些物品可能放弃有关应用程序或系统的功能的信息的测试数据和帐户应被删除。这些信息的占有可以促进系统的妥协和相关持卡人数据。
	6.4.4.b 检查来自最近安装或更新，以验证测试数据和所述系统变为有效之前帐户移除生产系统数据和帐户的样品。	

PCI DSS要求	测试程序	指导
6.4.5 变更控制程序必须包括以下内容：	**6.4.5.a 检查记录的变更控制程序和检验程序的定义：** • 影响的文档 • **记录 由授权方变更批准** • 功能测试，以验证该变化不会产生不利的系统的安全造成影响 • BACK-手续	如果管理不当，制度变迁，如硬件或软件更新和安装安全补丁的影响，可能无法完全实现，并可能产生意想不到的后果。
	6.4.5.b 对于系统组件样本，采访负责人员，以确定最近的变化。跟踪这些更改回相关的变更控制文件。对于每一个变化检测，执行以下步骤：	
6.4.5.1 影响的文档。	**6.4.5.1 验证冲击的该文档包括针对每个采样的变化改变控制文档。**	变化的影响应记录在案，使所有有关各方能够为任何处理的变化适当地规划。
6.4.5.2 记录 改变由授权方的批准。	**6.4.5.2 验证由授权方，所记录的批准存在每个抽样改变。**	批准授权方表示这种变化是由该组织所认可的合法批准的变更。
6.4.5.3 功能测试，以验证该变化不会产生不利的系统的安全性产生影响。	**6.4.5.3.a 对于每一个采样的变化，验证功能测试进行验证该变化不会产生不**利的系统的安全性产生影响。	全面测试应进行验证环境的安全性没有被实施的改变降低。测试应该验证所有现有的安全控制留在原地，与同样强烈的控制将被替换，或任何改变后的环境得到了加强。
	6.4.5.3.b 对于自定义代码修改，验证所有的更新都被部署到生产环境之前，符合PCI DSS要求6.5测试。	
6.4.5.4 回手续。	**6.4.5.4 验证背出程序为每个采样变化做好准备了。**	对于每一个变化，如果变化发生故障或产生不利影响的应用程序或系统的安全性，允许对系统进行恢复到以前的状态应该是有记录回手续。

PCI DSS要求	测试程序	指导
6.4.6 在一个显著变动完成后，所有相关的PCI DSS要求，必须对所有新的或更改系统和网络来实现，文档更新适用。	**6.4.6** 对于显著变化的样品，检查变更记录，面试人员，并观察受影响系统/网络，以验证适用PCI DSS要求得到落实，文档更新变化的一部分。	有流程分析显著变化有助于确保所有适当的PCI DSS控制应用到在范围内的环境中添加或更改任何系统或网络。建立此验证到变更管理流程帮助确保设备库存和配置标准的不断更新和安全控制应用需要的地方。变更管理流程应包括配套的证据表明，PCI DSS要求实施或通过迭代过程保存下来。中可能受到影响的包括但不限于PCI DSS要求的例子： • 网络图被更新，以反映更改。 • 系统是每个配置的标准配置，所有的默认口令更改和不必要的服务禁用。 • 系统与所需的控制 - 保护 例如，文件完整性监控（FIM），防病毒，补丁，审计日志记录。 • 敏感的验证数据（SAD）不存储，所有持卡人数据（CHD）存储记录并纳入DATA-保留策略和程序 • 新系统包括在季度漏洞扫描过程。

PCI DSS要求	测试程序	指导
6.5 解决软件开发过程中常见的编码漏洞如下： • **培养** 开发人员每年至少在向上最新的安全编码技术，包括如何避免常见的编码漏洞。 • 开发基于安全编码指南的应用。 ***注意：*** *当这个版本的PCI DSS的发表在6.5.1通过6.5.10中列出的漏洞都与行业最佳实践的电流。然而，对于漏洞管理行业最佳实践是更新的（例如，OWASP指南，SANS CWE前25名，CERT安全编码等），目前的最佳做法，必须用于这些要求。*	**6.5.a** 检查软件开发的政策和程序，以确认在安全编码技术跟上时代的训练需要开发人员至少每年一次，基于行业最佳实践和指导。 **6.5.b** 检查的培训记录，以验证软件开发商收到了最新培训的安全编码技术每年至少一次，包括如何避免常见的编码漏洞。 **6.5.c** 验证过程中的地方保护，应用程序在最低限度，以下漏洞：	应用层是高风险的，并且可以通过内部和外部的威胁进行定位。要求6.5.1通过6.5.10是应该到位的最低控制和组织应纳入相关安全编码实践的适用于特定的技术在他们的环境。应用程序开发人员应进行适当的培训，以识别和解决与这些（及其他）常见编码漏洞的问题。有工作人员知识渊博的安全编码规则应尽量减少通过糟糕的编码实践引入的安全漏洞的数量。可在公司内部或由第三方提供的开发人员培训和使用的技术应当是适用的。 作为业界公认的安全编码实践变革，组织编码实践和开发人员的培训也同样应更新，以应对新的威胁，例如，内存刮攻击。通过6.5.10 6.5.1标识的漏洞提供了一个最小的基准。它是由该组织保持最新与脆弱性趋势，并纳入相应的措施纳入其安全编码实践。

PCI DSS要求	测试程序	指导
注意：要求6.5.1通过6.5.6，下面，适用于（内部或外部）的所有应用程序。		
6.5.1 注入攻击，特别是SQL注入。也可以考虑OS命令注入，LDAP和XPath注入漏洞以及其他注入漏洞。	**6.5.1 检查软件开发政策和程序，负责面试的人员，以确认注入漏洞是由编码技术，其中包括解决：** • 验证输入来验证用户数据不能修改命令和查询的意思。 • 利用参数化查询。	注射攻击，特别是SQL注入，是危及应用的常用的方法。当用户提供的数据被发送到一个解释作为命令或查询的一部分发生注射。攻击者的恶意数据招数解释为执行无意命令或更改数据，并允许攻击者通过应用程序攻击的组件在网络里面，发起诸如缓冲区溢出攻击，或者显示两者机密信息和服务器应用程序的功能。信息应该被发送到该应用程序，例如，通过检查所有字母字符被验证之前，混合字母和数字字符等的
6.5.2 缓冲区溢出	**6.5.2 检查软件开发政策和程序，负责面试的人员，以验证缓冲区溢出是由编码技术，其中包括解决：** • 验证缓冲区的边界。 • 截断输入字符串。	当一个应用程序没有适当的边界上的缓冲空间检查缓冲区溢出发生。这会导致缓冲区中的信息被推出缓冲区的内存空间，并为可执行的内存空间。当这发生时，攻击者在缓冲区的末尾插入恶意代码的能力，并且然后推恶意代码转换成可执行的存储空间通过溢出缓冲器中。恶意代码然后被执行，并且通常能够应用程序和/或受感染的系统攻击者的远程访问。
6.5.3 不安全的加密存储	**6.5.3 检查软件开发政策和程序，负责面试的人员，以验证不安全的加密存储是通过编码技术来解决：** • 防止密码缺陷。 • 使用强大的加密算法和密钥。	不正确使用强大的加密功能来存储数据的应用程序是在被泄露的风险增加，而暴露身份验证凭证和/或持卡人数据。如果攻击者能够利用弱密码处理，则他们可能能够获得对加密数据的明文访问。

PCI DSS要求	测试程序	指导
6.5.4 不安全的通信	**6.5.4** 检查软件开发政策和程序，负责面试的人员，以验证不安全的通信由编码正确验证和加密所有敏感的通信技术解决。	未能充分加密的网络流量使用了强加密，应用程序是在受到损害和暴露持卡人数据的风险增加。如果攻击者能够利用弱密码处理，则他们可能能够获得一个应用程序的控制，甚至获得对加密数据的明文访问。
6.5.5 不当的错误处理	**6.5.5** 检查软件开发政策和程序，负责面试的人员，以验证不正确的错误处理是通过编码不通过的错误信息泄露的信息技术解决（例如，通过返回通用的，而不是特定错误详细信息）。	应用程序可以无意中泄露关于他们的配置或内部工作信息，或暴露通过不正当的错误处理方法特权信息。攻击者利用这个弱点来窃取敏感数据或完全破坏整个系统。如果恶意个人可以创建应用程序不能正确处理错误，他们能够获得详细的系统信息，创建拒绝服务中断，导致安全失效，或使服务器崩溃。例如，消息“提供不正确的密码”讲述了一个攻击者提供的用户ID是准确的，他们应该集中精力只上的密码。使用更通用的错误信息，如“数据无法验证。”
6.5.6 所有的“高风险”漏洞在漏洞识别过程中识别（如在PCI DSS要求6.1定义）。	**6.5.6** 检查软件开发政策和程序，负责面试的人员，以验证编码技术解决任何“高危”安全漏洞，可能影响应用程序，如PCI DSS要求6.1确定。	由组织的脆弱性风险分级过程中发现的所有漏洞（在要求6.1所定义的）为“高风险”，并可能影响应用程序应该被识别和应用程序的开发过程中解决。
注意：要求6.5.7通过6.5.10，下面，适用于网络应用程序和应用程序接口（内部或外部）：		Web应用程序，包括内部和外部（公共）面对，具有基于他们的架构以及相对容易和损害发生独特的安全隐患。
6.5.7 跨站点脚本（XSS）	**6.5.7** 检查软件开发政策和程序，负责面试的人员来验证跨站点脚本（XSS）是通过编码技术，包括解决 • 验证纳入之前的所有参数 • 利用上下文相关转义。	XSS缺陷发生每当应用需要用户提供的数据并将它发送到Web浏览器而无需首先验证或编码该内容。XSS允许攻击者在受害者的浏览器，它可以劫持用户会话中执行脚本，污损网站，可能引进蠕虫等

PCI DSS要求	测试程序	指导
6.5.8 不当访问控制（如不安全直接对象引用，未能限制URL访问，目录遍历，以及未能限制用户对功能的访问）。	**6.5.8 检查软件开发政策和程序，负责面试的人员，以验证不正确的访问控制**，如不安全的直接对象引用，未能限制URL访问和目录遍历，是通过编码技术，包括解决： • 用户进行正确的验证 • 消毒输入 • 不暴露于用户内部对象引用 • 用户界面，不允许访问未经授权的功能。	当开发人员暴露于内部实现对象的引用，如文件，目录，数据库记录，或键，如一个URL或形式参数时，发生直接对象引用。攻击者可以操纵这些引用来访问其他对象未经授权。始终如一地坚持在表示层和业务逻辑，对所有URL的访问控制。通常情况下，一个应用程序保护敏感的功能的唯一方法是通过防止链接或URL以未经授权的用户的显示。攻击者可以利用这个弱点来访问和直接访问这些网址进行未经授权的操作。攻击者可能能够枚举和浏览网站（目录遍历）的目录结构，从而获得访问未经授权的信息，以及获得进一步洞悉网站以后开发的工作。如果用户界面允许访问未经授权的功能，这种访问可能导致未经授权的个人获得访问特权凭证或持卡人数据。只有授权用户才应该被允许访问敏感资源的直接对象引用。限制访问数据资源将有助于防止被提交给未经授权的资源持卡人数据。只有授权用户才应该被允许访问敏感资源的直接对象引用。限制访问数据资源将有助于防止被提交给未经授权的资源持卡人数据。只有授权用户才应该被允许访问敏感资源的直接对象引用。限制访问数据资源将有助于防止被提交给未经授权的资源持卡人数据。
6.5.9 跨站点请求伪造（CSRF）	**6.5.9 检查软件开发政策和程序，负责面试的人员来验证跨站请求伪造（CSRF）**是通过编码技术，确保应用程序不依赖于授权证书和令牌自动浏览器提交的解决。	CSRF攻击迫使登录的受害者的浏览器发送一个预先验证的请求到易受攻击的Web应用程序，然后使攻击者可以执行任何状态更改操作受害人被授权执行（例如更新帐户的详细信息，进行购买，甚至认证到应用程序）。

PCI DSS要求	测试程序	指导
6.5.10 残破的认证和会话管理。	**6.5.10 检查软件开发政策和程序，负责面试的人员，以验证破认证和会话管理**通过编码技术，通常包括得到解决： • 标记会话令牌（例如饼干）为“安全” • 不暴露会话ID的URL • 登录成功后，将适当的超时和会话ID的转动。	安全认证和会话管理防止未经授权的人员损害合法的帐户凭据，密钥或会话令牌，否则将使得入侵者承担授权用户的身份。
6.6 对于面向公众的Web应用程序，解决在现有基础上的新的威胁和漏洞，并确保这些应用程序是针对通过下列方法已知攻击的保护： • 审查通过手动或自动应用程序漏洞安全评估工具或方法，每年至少任何更改后面向公众的Web应用程序 ***注意：这种评估是不一样的要求11.2进行漏洞扫描。*** • 安装检测并防止基于网络的攻击（例如，基于web的应用防火墙）中的面对公营web应用前的自动化技术方案中，以不断地检查所有流量。	**6.6 对于*面向公众*Web应用程序，确保*或***以下方法中的一个是在适当位置如下： • 检查记录的流程，面试人员，并检查应用程序安全评估记录，验证面向公众的Web应用程序手动或自动漏洞安全评估工具或使用审核的方法，如下： - 至少每年一次 - 任何更改后 - 由专门从事应用安全组织 - 也就是说，至少，在要求6.5所有漏洞都纳入评估 - 这所有漏洞进行修正 - 更正后，该应用程序重新评估。 • 检查系统配置设置和面试责任人员来验证检测和阻止基于网络的攻击的自动化技术解决方案（例如，一个web应用防火墙）是安排如下： - 坐落在面向公众的Web应用程序前检测和防止基于Web的攻击。 - 正在运行时，最新的适用。 - 正在生成审计日志。 - 被配置为阻止基于网络的攻击，或者产生立即调查警报。	面向公众的Web应用程序是攻击者的主要目标，而编码不良的web应用程序提供了攻击者访问敏感数据和系统轻松升级。审查应用程序或安装网络应用防火墙的要求是为了妥协，对面向公众的Web应用程序的数量减少由于不良编码或应用管理实践。 • 手动或自动漏洞安全评估工具或方法的审查和/或测试漏洞的应用程序 • web的应用防火墙过滤器和块非必需的流量在应用层。使用与基于网络的防火墙的同时，适当配置的web应用防火墙阻止应用层攻击如果应用程序不正确地编码或配置。这可以通过技术和工艺的组合来实现。基于流程的解决方案必须有利于为了满足这一要求，这是为了防止攻击的意图警报及时的反应机制。 ***注意：“专门从事应用安全的机构”可以是第三方公司或内部组织，只要评审专注于应用程序的安全性，并能证明从开发团队的独立性。***

PCI DSS要求	测试程序	指导
6.7 确保开发和维护安全的系统和应用程序文件，在使用中和已知的所有当事方的安全政策和操作程序。	**6.7** 检查文件和采访人员，以验证安全策略，并开发和维护安全的系统和应用程序的操作流程是： • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全策略和运作程序，以确保系统和应用程序在连续的基础上开发的安全和漏洞影响的。

实施强访问控制措施

要求7：按业务需要知道限制访问持卡人数据

为了确保关键数据只能由授权人员，系统和流程进行访问必须到位，根据需要知道，并根据工作职责来限制访问。

“需要知道”是当访问权授予仅执行任务所需的数据和特权量最少。

PCI DSS要求	测试程序	指导
7.1 限制进入系统组件和持卡人数据，只有那些人，他们的工作需要这样的访问。	**7.1 检查访问控制书面政策，并确认政策包含7.1.1通过7.1.4如下：** • 定义每个角色的访问需要和权限分配 • 访问特权的用户ID需要执行的工作职责最低权限的限制 • 基于个别人员的职称评定和功能访问的分配 • 批准文件（电子或书面）由授权方对所有访问，包括批准的特定权限上市。	更多的人谁有权访问持卡人数据时，更多的风险存在，用户的帐户将被恶意使用。限制访问那些具有合法的商业理由访问帮助企业防止持卡人数据的处理不当，缺乏经验或恶意。
7.1.1 定义访问需要的每个角色，包括： • 系统组件和数据资源的每个角色需要访问他们的工作职能 • 用于访问所需的资源（例如，用户，管理员等）的特权级别。	**7.1.1 选择角色的样品和 验证每个角色的定义，包括接入需求：** • 系统组件和数据资源的每个角色需要访问他们的工作职能 • 每个角色所需的权限的识别履行工作职责。	为了限制访问持卡人数据仅谁需要这样的访问的个人，首先需要定义每个角色的访问需求（例如，系统管理员，呼叫中心人员，店员），该系统/设备/数据中的每一角色需要访问和权限等级每个角色需要有效地执行所分配的任务。一旦角色和相应的接入需求的定义，个人可以进行相应的授权访问。
7.1.2 限制访问权限的用户ID需要执行的工作职责最低权限。	**7.1.2.a 负责分配访问验证访问权限的用户ID是面试人员：** • 仅分配给特别需要这样的特权访问角色 • 受限于必须进行岗位职责最低权限。	在分配特权的ID，它指定的个人只需要执行他们的工作（以下简称“最低权限”）的权限是非常重要的。例如，数据库管理员或备份管理员不应该被赋予相同的权限整个系统管理员。 *（接下页）*

PCI DSS要求	测试程序	指导
	7.1.2.b 选择具有特权访问和采访负责管理人员的用户ID的样本来验证分配的权限是： • 必要时作此人的工作职能 • 受限于必须进行岗位职责最低权限。	分配最小权限有助于防止用户没有关于从错误或意外更改应用程序配置或者改变其安全设置的应用程序足够的知识。强制实施最低权限也有助于损害的范围最小化，如果未经授权的人获得访问用户ID。
7.1.3 分配基于个体人员的职称评定和功能的访问。	**7.1.3 选择用户ID和面试负责管理人员的样本来验证分配的权限是基于个人的职业分类和功能。**	一旦需求的用户角色（每个PCI DSS要求7.1.1）中定义的，它很容易授人根据自己的职业分类和功能通过使用已创建的角色的访问。
7.1.4 需要由授权方指定所需的权限文件的批准。	**7.1.4 选择用户ID的样品，并记录在案的批准，以验证比较：** • 批准文件存在指定的特权 • 审批是由授权方 • 这指定的权限匹配分配给各个角色。	批准文件（例如，以书面或电子）确保那些访问和权限是已知的，由管理授权，他们的访问是必要的工作职责。
7.2 建立制约根据用户的需要知道的访问，并设置为“拒绝所有”除非明确允许系统组件的访问控制系统（S）。此访问控制系统（S）必须包括以下内容：	**7.2 检查系统设置和供应商文档，以验证访问控制系统（一个或多个）执行如下：**	如果没有一个机制来限制基于用户需要知道的访问，用户可以在不知不觉中被授权访问持卡人数据。门禁系统自动限制访问和分配权限的过程。此外，一个默认的“全部拒绝”设置，确保没有人被授予访问权限之前，除非规则建立专门授予此类访问。实体可以有一个或多个接入控制系统来管理用户访问。
7.2.1 所有系统组件的覆盖面	**7.2.1 确认系统中所有设备的访问控制系统到位。**	
7.2.2 权限分配基于职业分类和功能的个人。	**7.2.2 确认系统配置为强制分配给基于职业分类和功能的个人特权访问控制。**	***注意：一些访问控制系统被默认设置为“允许，所有”，从而允许访问，除非/直到一个规则被写入明确否认。***
7.2.3 默认的“全部拒绝”设置。	**7.2.3 确认访问控制系统有一个默认的“全部拒绝”设置。**	

PCI DSS要求	测试程序	指导
7.3 确保限制访问持卡人数据的安全政策和操作程序都记录，在使用中，和已知的所有当事方。	**7.3** 检查文件和面试人员核实限制访问持卡人数据的安全政策和操作程序是： • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全政策和操作程序，以确保访问的控制，并根据需要 - 方知和最小特权，在连续的基础上。

要求8：识别和验证访问系统部件

分配一个唯一的标识（ID）给每个人的访问确保每个个体是对自己的行为唯一负责。当这样的问责到位，采取的行动对关键数据和系统被执行，并且可以追溯到已知和授权的用户和进程。

密码的有效性在很大程度上取决于设计和实施认证的系统，特别是如何频繁的密码尝试可以被攻击者造的，安全的方法来保护用户密码，在入境点，在传输过程中，并同时确定在存储。

***注意：** 这些要求适用于所有帐户，包括点销售帐户，具有管理功能，用于和持卡人数据查看或访问持卡人数据或访问系统中的所有账户。这包括由供应商和其他第三方使用的帐户（例如，用于支持或维护）。这些要求不适用于由消费者（例如，持卡人）使用的帐户。然而，需求8.1.1，8.2，8.5，8.2.3通过8.2.5，8.1.6和8.1.8通过不打算到销售点支付应用程序，只需要一个接入内，向用户帐户在为了便于在单个事务（诸如出纳帐户）时卡号。*

PCI DSS要求	测试程序	指导
8.1 制定和实施的政策和程序，以确保非消费用户和管理员对所有系统组件正确的用户身份管理，如下所示：	**8.1.a** 审查程序，并确认它们定义流程，每一个低于8.1.1通过8.1.8项的	通过确保每个用户唯一identified-而不是使用一个ID为几个员工，企业可以保持动作和每名员工的有效审计跟踪个人的责任。这将有助于加快问题的解决和遏制滥用时或恶意时。
	8.1.b 确认程序为用户识别管理来实现，通过执行以下操作：	
8.1.1 允许他们访问系统组件或持卡人数据之前分配的所有用户一个唯一的ID。	**8.1.1** 记者采访的管理人员，以确认所有的用户分配一个唯一的ID访问系统组件或持卡人数据。	
8.1.2 控制添加，缺失，和用户ID，凭证和其它标识符的对象的修饰。	**8.1.2** 对于特权用户ID和一般用户ID的样品，检查关联的授权和观察系统设置，以验证每个用户ID和特权用户ID已经与只在记录批准规定的特权实现。	为了确保用户帐户授予访问系统都是有效和认可的用户，强大的流程必须管理所有更改用户ID和其他认证证书，包括添加新的和修改或删除现有的。
8.1.3 立即撤销对任何终止用户的访问。	**8.1.3.a** 选择过去六个月终止用户的样本，并检查当前用户访问列表 - 本地和远程访问，以验证他们的ID已停用或从访问列表中删除。	如果员工离开公司，仍然有通过自己的用户账号访问网络，可能会发生，无论是对持卡人数据的不必要或恶意访问由前雇员或谁利用了旧的和/或不使用的帐户恶意用户。为了防止未经授权的访问，用户凭据和其他身份验证方法，因此需要及时根据员工的离职（尽快）撤销。
	8.1.3.b 验证所有的物理身份验证方法，如智能卡，令牌等，已退还或停用。	

PCI DSS要求	测试程序	指导
8.1.4 在90天内删除/禁用不活动的用户帐户。	**8.1.4** 观察用户帐户，以确认所有无效帐户，超过90天的要么删除或禁用。	那些不常用的账户往往是攻击目标，因为它是不太可能的任何更改（如更改后的口令）将被注意到。因此，这些账户可以更容易地利用和用于访问持卡人数据。
8.1.5 管理用于由第三方通过远程访问来访问，支持或保持系统组件如下编号： • 启用仅在时间段需要和残疾人在不使用时。 • 在使用时监控。	**8.1.5.a** 面试人员和观察的过程，用于管理第三方接入，支持账户，或维持系统组件来验证帐户用于远程访问是： • 残疾人在不使用时 • 在需要时由第三方才启用，禁用和不使用时。	允许厂商有全天候访问到您的网络中，他们需要支持您的系统的情况下增加了未授权访问的机会，无论是从供应商的环境中的用户或恶意的个人谁发现并使用这个始终可用的外部入口点进入您的网络。启用仅在需要的时间段访问，并且只要它不再需要禁用它，有助于防止这些连接的滥用。的供应商接入监控只在批准的时限规定，供应商只能访问必要的和系统的保证。
	8.1.5.b 面试人员和观察的过程，以验证第三方远程访问帐户同时被使用进行监控。	
8.1.6 通过限制不超过6次尝试后锁定了用户ID重复的访问尝试。	**8.1.6.a** 对于系统组件样本，检查系统配置设置，以验证认证参数设置为需要不超过6个无效的登录尝试后，该用户帐户被锁定。	没有适当的帐户锁定机制，攻击者可以不断尝试猜测通过手动或自动工具的密码（例如，密码破解），直到他们取得成功，并获得用户的帐户。
	8.1.6.b ***只有服务供应商的评估进一步的测试过程：*** 检查内部流程和客户/用户文档，并观察执行的过程来验证非消费用户的用户帐户被暂时锁定的不超过6个无效访问尝试后。	***注意：*** *测试过程8.1.6.b是仅适用如果被评估的实体是服务提供商的附加程序。*
8.1.7 锁定时间设定为至少30分钟或直到管理员使用户ID。	**8.1.7** 对于系统组件的一个样本，检查系统配置设置，以验证被设置为需要，一旦一个用户帐户密码参数被锁定，它保持锁定最少30分钟或直到系统管理员复位帐户。	如果一个帐户被锁定由于有人不断尝试猜测密码，控制延缓这些锁定帐户激活从不断猜测的密码，停止恶意的个人（他们将不得不停止最少30分钟，直到该帐户被重新激活）。另外，如果必须要求重新激活，管理员或帮助台可以验证它是真正的帐户拥有者要求重新激活。

PCI DSS要求	测试程序	指导
8.1.8 如果会话已闲置超过15分钟，要求用户重新认证，重新激活终端或会话。	**8.1.8** 对于系统组件的一个样本，检查系统配置设置，以验证系统/会话空闲超时功能已被设置为15分钟或更少。	当用户离开从打开机与访问关键系统组件或持卡人数据，该机器可通过其他人在用户不在时使用，导致未经授权访问帐户和/或滥用。重新认证可以在系统级别来保护计算机上运行的所有会话，或在应用级应用。
8.2 除了分配一个唯一的ID，确保对非消费用户和管理员对所有系统组件正确的用户认证管理通过采用以下方法来认证所有用户中的至少一个： • 您知道的东西，如密码或口令 • 你拥有的东西，如令牌设备或智能卡 • 你的东西是，如生物。	**8.2** 要验证用户使用唯一的ID和附加的认证验证（例如，一个口令/短语）访问持卡人数据环境中，执行以下： • 检查文档描述中使用的认证方法（一个或多个）。 • 对于每种类型的使用的认证方法和用于每个类型的系统组分，观察的认证，以验证认证功能归档的认证方法（一个或多个）是一致的。	这些认证方法中，除了唯一的ID使用时，有利于保护用户的ID被攻破，因为一个试图妥协需要知道两者的唯一ID和密码（或使用其他身份验证）。需要注意的是数字证书，只要它是一个特定的用户独特的“你有什么”正确的选项。 由于恶意个人会采取危及系统安全的第一步是利用薄弱或不存在的口令，它实施认证管理良好的过程是非常重要的。

PCI DSS要求	测试程序	指导
8.2.1 使用强加密，渲染所有认证凭证（例如密码/短语）的传输和存储的所有系统组件中不可读。	**8.2.1.a** 检查供应商文档和系统配置设置验证密码传输和存储过程中使用强大的加密保护。	许多网络设备和应用程序通过网络传输和/或存储的密码加密的，可读的密码不加密。恶意个人可以容易地截取使用传输期间未加密的密码“嗅探器”，或直接访问在其中它们被存储的文件未加密的密码，并使用该数据，以获得未经授权的访问。
	8.2.1.b 对于系统组件样本，检查密码文件，以验证密码是储存过程中不可读。	
	8.2.1.c 对于系统组件的一个样本，检查数据传输，以验证密码是在传输过程中读取。	***注意：*** *测试程序8.2.1.d和8.2.1.e是，只有当被评估的实体是服务提供者申请额外的程序。*
	8.2.1.d ***只有服务供应商的评估进一步的测试过程：*** 注意密码的文件，以确认非消费者客户密码的存储过程中不可读。	
	8.2.1.e ***只有服务供应商的评估进一步的测试过程：*** 观察数据传输，以验证非消费用户密码传输过程中不可读。	
8.2.2 修改任何认证凭证，例如，在执行密码重置，供应新的令牌，或生成新密钥前验证用户身份。	**8.2.2** 审查修改认证证书的认证程序，并观察安全人员，以验证，如果用户通过电话，电子邮件，网络或其他非面对面的面对面方式请求鉴定证书的复位，用户的身份验证前的认证凭证被修改。	许多恶意个人使用“社会工程” - 例如，呼叫服务台并作为合法用户有一个密码更改，以便他们可以利用用户ID。考虑使用一个‘秘密问题’，只有正确的用户可以回答以帮助管理员识别用户在重新设定或修改认证证书。

PCI DSS要求	测试程序	指导
8.2.3 口令/密码短语必须符合以下条件： • 至少需要七个字符的最小长度。 • 同时包含数字和字母字符。可替换地，密码/密码短语必须有复杂性和强度至少等同于上面指定的参数。	**8.2.3a** 对于系统组件的一个样本，检查系统配置设置，以验证用户的口令/通行短语的参数被设定为需要至少以下强度/复杂度： • 至少需要七个字符的最小长度。 • 同时包含数字和字母字符。	强密码/密码短语是防御的第一线成网，因为一个恶意的个体往往会首先尝试找到薄弱或根本不存在密码的帐户。如果密码很短或简单的猜测，这是比较容易的怀有恶意的个体找到这些微弱的账户和有效的用户ID的幌子下妥协的网络。
	8.2.3.b ***只有服务供应商的评估进一步的测试过程：*** 检查内部流程和客户/用户文档，以确认非消费用户的密码/密码短语必须至少满足以下强度/复杂性： • 至少需要七个字符的最小长度。 • 同时包含数字和字母字符。	此要求指定的最小的七个字符和两个数字和字母字符应该用于密码/密码短语。对于在这个最低不能由于技术的限制满足的情况下，实体可使用"等效强度"来评估其替代品。有关可变性和的密码强度等值信息（也被称为熵）为不同的格式的口令/通行短语，指的工业标准（例如，NIST SP 800-63的当前版本）。 ***注意：*** *测试过程8.2.3.b是仅适用如果被评估的实体是服务提供商的附加程序。*
8.2.4 更改用户 口令/密码短语至少每90天。	**8.2.4.a** 对于系统组件的一个样本，检查系统配置设置，以验证用户的口令/通行短语的参数被设定为要求用户更改密码每90天至少一次。	口令/密码短语是有效的很长一段时间没有变化提供恶意的个体有更多的时间来打破密码/短语工作。
	8.2.4.b ***只有服务供应商的评估进一步的测试过程：*** *内部审查* 流程和客户/用户文档，以确认： • 非消费用户的用户密码/需要密码短语定期更改; 和 • 非消费顾客的用户给予指导何时，在何种情况下，密码/密钥必须改变。	***注意：*** *测试过程8.2.4.b是仅适用如果被评估的实体是服务提供商的附加程序。*

PCI DSS要求	测试程序	指导
8.2.5 不要让一个人提交新的密码/密码短语与任何他或她已经习惯了过去的4个密码/密码短语。	**8.2.5.a** 对于系统组件的样本，获得并检查系统配置设置，以验证密码参数设定为规定新的口令/通行短语不能是相同的四个先前使用的口令/通行短语。	如果不保持历史密码，更改密码的有效性降低，因为先前的密码可以一遍又一遍地重复使用。要求密码不能一段时间内重复使用减少了已经猜到或野蛮强制密码将在未来被使用的可能性。
	8.2.5.b ***只有服务供应商的评估进一步的测试过程：*** 检查内部流程和客户/用户文档，以验证新的非消费类的客户用户口令/密码不能相同，以前的4个密码。	***注意：*** *测试过程8.2.5.b是仅适用如果被评估的实体是服务提供商的附加程序。*
8.2.6 设置密码/密码短语为首次使用，在复位时为每个用户独特的价值，并第一次使用后立即更改。	**8.2.6** 检查密码程序，观察安全人员，以验证新用户是首次口令/密码短语，并重置现有用户的密码/密码短语，被设置为每个用户独特的价值和一次使用后更改。	如果相同的密码用于每个新用户，内部用户，前雇员，或怀有恶意的个体可能知道或容易发现这个密码，并用它来访问账户。
8.3 固定所有个人非控制台管理访问，并使用多因素认证的CDE所有远程访问。 ***注意：*** *多因素认证要求最少两个的三种认证方法（见的认证方法的描述，要求8.2）被用于认证。使用一个因素两次（例如，使用两个单独的密码）不被认为是多因素认证。*		多因素认证要求个人呈现最小的认证的两个单独的形式（如要求8.2所述），被授权访问之前。多因素身份验证提供了额外的保证，个人试图访问是他们声称是谁。随着多因素认证，攻击者需要妥协至少两个不同的身份验证机制，增加妥协的难度，从而降低风险。多因素认证不同时在系统级和应用级用于特定系统组件需要。多因素认证可以在认证时的特定网络或系统的组件来执行。多因素的技术的实例包括但不限于远程认证和拨号与令牌服务（RADIUS）; 终端访问控制器访问控制系统（TACACS）与令牌; 以及促进多因素认证等技术。

PCI DSS要求	测试程序	指导
8.3.1 结合多因素身份验证对所有非控制台访问到CDE对人员的管理权限。	**8.3.1.a** 检查网络和/或系统配置（如适用），以验证多因素认证要求所有非控制台管理访问CDE。 **8.3.1.b** 观察管理员人员登录到CDE样本，并确认至少有两个三种认证方式被使用。	这一要求旨在适用于与在CDE管理权限的所有人员。此要求仅适用于具有管理权限，并只适用于非控制台访问CDE人员; 它并不适用于应用程序或系统帐户进行自动功能。如果实体不使用分段的CDE从他们的网络的其余部分分开，管理员可以登录到CDE网络或登录到系统时，或者当使用多因素认证。如果CDE从实体网络的其余部分分割，管理员将需要从非CDE网络连接到CDE系统时使用的多因素认证。多因素认证可以在网络级别或在系统/应用程序级别来实现; 它不必是两者兼而有之。
8.3.2 结合多因素认证所有远程网络访问（包括用户和管理员，并包括支持或维护的第三方接入）源自实体的网络之外。	**8.3.2.a** 检查远程访问服务器和系统来验证多因素认证系统配置需要： • 通过人员所有远程访问，用户和管理员，和 • 所有第三方/供应商的远程访问（包括访问应用程序和系统组件的支持或维护的目的）。 **8.3.2.b** 观察人员的样品（例如，用户和管理员）远程连接至网络，并验证所使用的至少两个的三个认证方法。	这一要求旨在适用于所有人员，包括普通用户，管理员和供应商（支持或维护）用的网络，其中远程访问可能会导致访问CDE的远程访问。如果远程访问到具有适当的分割，使得远程用户无法访问或影响持卡人数据环境中的实体网络，将不需要为到该网络的远程接入的多因素认证。然而，需要对任何远程访问网络，获取持卡人数据环境多因素认证，并建议到实体的网络中的所有远程访问。

PCI DSS要求	测试程序	指导
8.4 文档和沟通认证政策和程序的所有用户，包括： • 指导选择强大的身份验证凭据 • 指导用户如何保护自己的身份验证凭据 • 说明不重用以前使用的密码 • 说明更改密码，如果有任何怀疑密码可能会大打折扣。	**8.4.a 检查 程序和面试人员检查验证政策和程序分发给所有用户。**	通信密码/认证政策和程序，所有用户可帮助这些用户理解和政策遵守。例如，在选择强密码引导可以包括建议，以帮助工作人员选择不包含字典中的字难以猜测的密码，并且不包含用户（信息，如用户ID，家庭成员的姓名，出生日期等）。指导保护认证证书可包括不写下密码或保存在不安全的文件，并且是恶意的个人谁可能会试图利用他们的密码警报（例如，通过调用一个员工，并要求他们的密码，以便调用者可以“疑难解答一个问题”）。
	8.4.b 被分发给用户，并验证它们审查认证政策和程序，包括： • 指导选择强大的身份验证凭据 • 指导用户如何保护自己的身份验证凭据。 • 说明用户不要再使用以前用过的密码 • 说明更改密码，如果有任何怀疑密码可能会大打折扣。	
	8.4.c 记者采访的用户样本，以验证他们所熟悉的认证政策和程序。	
8.5 如下不要使用组，共享或通用的ID，密码或其他身份验证方法： • 一般用户ID被禁用或删除。 • 共享用户ID不存在系统管理等关键功能。 • 共享和通用用户ID不被用于管理任何系统组件。	**8.5.a 对于系统组件的一个样本，检查用户ID列表来验证以下内容：** • 一般用户ID被禁用或删除。 • 不存在系统管理活动和其他重要功能的共享用户ID。 • 共享和通用用户ID不被用于管理任何系统组件。	如果多个用户共享相同的身份验证凭据（例如，用户帐号和密码），就不可能跟踪系统访问和活动的个人。这又防止实体从因为给定的行动可能已被任何人拥有的认证证书的知识组中进行分配的责任，或具有，一个人的行为有效的记录。
	8.5.b 检查验证政策和程序，以确认使用组共享ID和/或密码或其他认证方法都明确禁止。	
	8.5.c 采访系统管理员，以验证组和共享ID和/或密码或其他认证方法不分布，即使请求。	

PCI DSS要求	测试程序	指导
8.5.1 ***只有服务提供商附加要求：*** **与到客户端的远程**访问（例如，用于支持POS系统或服务器的）服务供应商必须使用一个唯一的验证凭证（例如密码/短语）为每一个客户。 ***注意：*** *这个要求并不打算适用于共享托管服务提供商访问自己的托管环境，其中多客户环境托管。*	**8.5.1** ***只有服务供应商的评估进一步的测试过程：*** **检查验证政策和程序，面试**人员核实，不同的身份验证凭据用于访问每一位客户。	***注意：*** *此要求仅适用于被评估的实体是服务提供商。* 为了防止多个客户通过使用一组凭据的妥协，具有远程访问帐户的供应商客户的环境应使用不同的身份验证凭据为每一个客户。技术，如多因素的机制，其提供为每个连接一个独特的凭证（例如，经由单次使用的密码）也可满足此要求的意图。
8.6 当其他认证机制被使用（例如，物理或逻辑安全令牌，智能卡，证书等），这些机制的使用必须分配如下： • 身份验证机制，必须分配到个人账户和多个帐户之间不共享。 • 物理和/或逻辑控制必须到位，以确保只有预期的帐户可以使用该机制来获得。	**8.6.a 检查验证政策和程序来验证程序使用的认证机制，如物理安全令牌，智能卡和证书的定义，其中包括：** • 认证机制被分配给单独的帐户和多个帐户之间不共享。 • 物理和/或逻辑控制被定义为保证只有预期的帐户可以使用该机制来访问。 **8.6.b 面试保安人员核实身份验证机制被分配到一个帐户，多个帐户之间不共享。** **8.6.c 检查系统配置设置和/或物理控件，如适用，以验证控制被执行，以确保只有预期的帐户可以使用该机制来访问。**	如果诸如令牌，智能卡，和证书的用户认证机制可以由多个帐户使用，它可能是不可能识别使用认证机构的个人。具有物理和/或逻辑控制器（例如，PIN，生物测量数据，或密码）来唯一地标识的帐户的用户将阻止未授权用户通过使用一个共享的认证机制获得访问权。

PCI DSS要求	测试程序	指导
8.7 所有接入到包含持卡人数据（包括应用程序，管理员，和所有其他用户访问）的任何数据库限制如下： • 于用户的查询，以及用户操作的所有用户访问的数据库是通过编程方法。 • 只有数据库管理员可以直接访问或查询数据库的能力。 • 数据库应用程序的应用程序ID可以仅由应用程序（由个人用户或其他非应用程序进程和不）被使用。	**8.7.a 检查数据库和应用程序的配置设置，并验证所有用户之前获得认证。** **8.7.b 检查数据库和应用程序的配置设置，以验证 于用户的查询，以及用户操作的所有**用户访问的（例如，移动，复制，删除），该数据库是通过编程方法只（例如，通过存储过程）。 **8.7.c 检查数据库访问控制设置和数据库应用程序的配置设置，以验证用户直接访问**或数据库的查询只限于数据库管理员。 **8.7.d 审查数据库访问控制设置，数据库应用程序的配置设置，以及相关的应用程序**ID来验证应用程序ID可以仅由应用程序使用（而不是由个人用户或其它进程）。	而不用于访问数据库和应用程序的用户认证中，由于用户还没有被认证，并且因此不知道该系统可以不被记录为未授权的或恶意的访问的电势增加，并且这样的访问。此外，数据库访问应该通过编程方法只（例如，通过存储过程），而不是通过直接访问最终用户数据库（除了数据库管理员，谁可能需要为他们的行政职务直接访问数据库）授予。
8.8 确保识别和认证的安全政策和操作程序都记录，在使用中，和已知的所有当事方。	**8.8 检查文件和采访人员，以验证安全策略和身份识别和验证操作流程是：** • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全策略和一个连续的基础上管理身份和授权操作流程。

要求9：限制对持卡人数据的物理访问

任何物理访问那家持卡人数据所规定的个人访问设备或数据，并删除系统或硬拷贝，并应适当限制的机会，数据或系统。对于要求9的目的，“现场工作人员”指的是全职和兼职员工，临时员工，承包商和顾问谁是身体上存在实体的场所。A“访客”是指供应商，任何现场工作人员的客人，服务人员或任何人谁需要进入机构的持续时间短，一般不超过一天。“媒体”是指所有纸张和包含持卡人数据的电子媒体。

PCI DSS要求	测试程序	指导
9.1 使用合适的设备条目的控制来限制和监控持卡人数据环境的系统物理访问。	**9.1 验证的物理安全控制存在的每个机房，数据中心，并在持卡人数据环境系统等物理领域。** • 验证接入控制与标记阅读器或其他设备，包括授权徽章和锁和钥匙。 • 观察系统管理员试图登录到控制台在持卡人数据环境中随机抽取系统，并验证它们被“锁定”，以防止未经授权的使用。	如果没有物理访问控制，如徽章系统和车门控制，未经授权的人可能会获得进入工厂行窃，禁用，破坏或销毁关键系统和持卡人数据。锁定控制台登录屏幕防止获取敏感信息，改变系统配置，引入漏洞到网络，或销毁记录未经授权的人。
9.1.1 请使用摄像机或访问控制机制（或两者）来监控敏感区域单独的物理访问。回顾收集的数据，并与其他相关的条目。存储至少三个月，除非法律另有限制。 ***注意：“敏感区”是指任何数据中心，服务器室或容纳存储系统中，过程中，或传输持卡人数据的任何区域。这不包括仅销售点终端都存在面向公众的领域，如在零售商店收银员领域。***	**9.1.1.a 验证无论是视频摄像机或访问控制机制（或两者）到位，以监控入口/出口点敏感区域。** **9.1.1.b 验证无论是视频摄像机或访问控制机制（或两者）都被篡改或禁用保护。**	当调查物理漏洞，这些控件可以帮助识别物理访问敏感区域，以及当他们进入和退出的个人。罪犯试图获得对敏感区域的物理访问会经常试图禁用或绕过监视控制。为了保护这些控件不被篡改，摄像机可以放置所以他们遥不可及的和/或进行监测，以检测篡改。同样，访问控制机制，可以监测或具有安装的物理保护措施，以防止它们被损坏或恶意的个人禁用。

（接下页）

PCI DSS要求	测试程序	指导
	9.1.1.c 验证从摄像机和/或访问控制机制，数据审核，数据存储至少三个月。	敏感区域的例子包括企业数据库服务器机房，后台客房存储持卡人数据的零售点，并为大量的持卡人数据的存储区域。敏感区域应该由每个组织来鉴定，以确保适当的体质监测的控制措施。
9.1.2 实现物理和/或逻辑控制来限制访问公开访问的网络插孔。 *例如，位于公共区域和游客进入的区域网络插孔可以被禁用，只有当启用网络访问明确授权。或者，过程可以实施，以确保游客在活动网络插孔地区随时护航。*	**9.1.2** 采访专人负责观察可公开访问的网络插孔的位置，以验证物理和/或逻辑的控制措施以限制对公共访问的网络插孔。	限制访问网络插孔（或网络端口）将防止堵到现成的网络插孔恶意的个人和访问到内部网络资源。是否逻辑或物理控件，或两者的组合，使用时，它们应该是足够的，以防止未明确从能够连接到网络授权的个人或设备。
9.1.3 限制对无线接入点，网关，手持设备的物理访问， 网络/通信硬件和电信线路。	**9.1.3** 验证到无线接入点，网关，手持设备，网络/通信硬件和电信线路物理访问被适当地限制。	没有安全，在访问无线组件和设备，恶意用户可以利用组织的无人值守的无线设备访问网络资源，甚至他们自己的设备连接到无线网络中未经授权的访问。此外，固定网络和通信硬件防止恶意用户拦截网络流量或物理自己的设备连接到有线网络资源。

PCI DSS要求	测试程序	指导
9.2 制定程序可以轻松地现场工作人员和来访者进行区分，包括： • 确定现场工作人员和来访者（例如，分配徽章） • 更改访问需求 • 撤销或终止现场人员和过期访问者标识（如ID徽章）。	**9.2.a 查看记录的流程来验证程序识别和现场工作人员和观众之间的区分定义。** • 验证程序包括以下内容： • 确定现场工作人员和来访者（例如，分配徽章） • 更改访问要求和 • 撤消终止现场人员和过期访问者标识（如ID卡）	识别授权的访问者，使他们很容易从现场工作人员区分开来防止未经授权的访问者被授予访问包含持卡人数据的区域。
	9.2.b 检查识别方法（如ID徽章）和观察过程用于识别和现场人员和访客，以验证区分： • 游客被明确确定，并 • 这是很容易现场工作人员和观众之间的区别。	
	9.2.c 验证访问识别过程（例如徽章系统）被限制到授权的人员。	
9.3 控制现场人员如下敏感区域的物理访问： • 访问必须经过授权，并根据个人的工作职能。 • 访问被终止时立即撤回，和所有的物理访问机制，如钥匙，门禁卡等，返回或禁用。	**9.3.a 对于敏感区域的物理访问现场工作人员的样本，采访负责人员和观察访问控制列表来验证：** • 进入敏感区域授权。 • 访问需要个人的工作职能。	控制对敏感区域的物理访问有助于确保合法业务只需要经过授权的人员授予访问权限。当人员离开组织，所有的物理访问机制应退还或（尽快）在他们的离开及时停用，以确保人员，一旦他们的就业已经结束不能获得对敏感区域的物理访问。
	9.3.b 观察人员访问敏感的区域，以确认所有人员都被授予访问权限之前授权。	
	9.3.c 选择最近离职员工的样本，并查看访问控制列表来验证人员不必敏感区域的物理访问。	

PCI DSS要求	测试程序	指导
9.4 实施程序，以识别和授权的访客。 程序应包括以下内容：	**9.4 验证访客授权和访问控制措施如下：**	访客控制是很重要的，以减少非法和恶意的人来访问设备（和潜在的，对持卡人数据）的能力。
9.4.1 访问者在进入前内授权，并且在任何时候都护送，其中持卡人数据被处理或维持的领域。	**9.4.1.a 遵守程序和面试人员核实，游客必须他们被授予访问权限之前内的授权，并且在任何时候都护送，持卡人数据的处理或维护的区域。**	访客控制确保游客识别为访客，让工作人员可以监控他们的活动，他们的访问仅限于自己的合法访问的只是时间。确保游客徽章是在访问到期或完成返回防止使用之前授权的传球来获得物理访问进入大楼参观结束后，恶意的人。
	9.4.1.b 观察使用访客徽章或其他标识的，以验证物理令牌徽章不允许到持卡人的数据被处理或维持物理区域护送访问。	
9.4.2 游客识别和考虑到到期徽章或其他识别和区分明显，从现场工作人员的参观者。	**9.4.2.a 观察人们在设备内以验证使用访客徽章或其他标识的，而且游客从现场工作人员很容易分辨。**	访问者日志记录上的访问者最少的信息是很容易和廉价的维护，并协助查明建筑物或房间，以及对持卡人数据的潜在访问物理访问。
	9.4.2.b 验证访客徽章或其他标识过期。	
9.4.3 参观者被要求离开机构之前或在到期日交出徽章或标识。	**9.4.3 离开设施验证访客观察的游客被要求在出发时或到期时交出他们的徽章或其他标识。**	
9.4.4 访问者日志用于保持访问者对设施的物理审计跟踪以及计算机房和持卡人数据的存储或传输的数据中心。记录访问者的姓名，所代表的公司，和现场工作人员授权的日志物理访问。保留此日志最少三个月，除非法律另有限制。	**9.4.4.a 验证访客数在使用记录对设施的物理访问，以及计算机房和持卡人数据的存储或传输的数据中心。**	
	9.4.4.b 验证日志包含： • 访问者的名字， • 该公司表示， • 酒店内的人员授权的物理访问。	
	9.4.4.c 验证日志至少保留三个月。	

PCI DSS要求	测试程序	指导
9.5 物理安全的所有媒体。	**9.5** 验证保护持卡人数据的程序包括用于控制物理保护所有的媒体（包括但不限于电脑，移动电子媒体，纸质收据，纸质报告和传真）。	为确保物理媒体的控制是为了防止未经授权的人在任何类型的媒体获得访问持卡人数据。持卡人数据易受未授权查看，复制，或者如果它是不受保护的扫描，而这是在可移动或便携式媒体，打印出来，或留在某人的办公桌。
9.5.1 商店媒体备份在安全的位置，优选为场外设施，如备用或备份站点，或商业储存设施。至少每年审查位置的安全。	**9.5.1** 验证存储位置的安全性至少每年审核，以确认备份介质存储是安全的。	如果存储在非安全设施，包含持卡人数据的备份可能容易丢失，被盗或复制用于恶意目的。定期审查储存设施使组织解决所发现的安全问题及时，最大限度地减少潜在的风险。
9.6 保持在任何类型的媒体，包括下列的内部或外部的分布严格控制：	**9.6** 验证有一个策略来控制媒体分发，并且该政策涵盖了所有的分布式媒体包括分配给个人。	程序和流程有助于保护分布式内部和/或外部用户的媒体持卡人数据。如果没有这样的程序，数据可能丢失或被盗，并用于欺诈目的。
9.6.1 分类媒体所以数据的灵敏度可以被确定。	**9.6.1** 确认所有介质被分类所以数据的灵敏度可以被确定。	重要的是，媒体进行识别，例如，它的分类地位可以很容易辨别。不认定为机密的媒体可能无法得到充分的保护或可能丢失或被盗。 ***注意：** 这并不意味着该媒体需要有一个"机密"的标签附着; 其目的是，该组织已确定包含敏感数据，因此它可以保护它的媒体。*
9.6.2 通过安全的快递或可以被准确地追踪其他递送方法发送媒体。	**9.6.2.a** 面试人员和检验记录，以验证设施外发送的所有媒体被记录，并通过安全的快递或可跟踪其他交付方式发送。	媒体可能会丢失或被盗，如果通过非可追踪的方法发送如定期邮寄。使用安全信使发送包含持卡人数据的任何媒体允许企业使用他们的跟踪系统，以维持出货量的库存和位置。
	9.6.2.b 选择一个最近的所有离线介质跟踪日志的几天样品，并验证跟踪细节都会记录在案。	

PCI DSS要求	测试程序	指导
9.6.3 确保管理层批准是从安全区域（包括当媒体被分发到个人）移动的任何和所有的媒体。	**9.6.3** 选择一个最近的所有离线介质跟踪日志的几天样品。从日志中，并与负责人员面谈的审查，核实，每当媒体从安全区域（包括当媒体被分发到个人）移动则可得到适当的管理权限。	如果没有确保媒体从安全区域删除之前所有的媒体运动中获得通过的公司的过程中，媒体也不会被跟踪或适当保护，它的位置是未知的，从而导致丢失或被盗的媒体。
9.7 保持对存储和媒体无障碍严格控制。	**9.7** 获取并检查用于控制所有媒体的存储和维护，并验证该政策需要定期的媒体库存的策略。	如果不仔细盘点方法和存储控制，被盗或丢失的媒体可能会被忽视的时间无限期量。如果媒体没有清点，被盗或丢失的媒体可能没有注意到时间长或根本。
9.7.1 妥善维护所有媒体的存货记录和每年至少进行媒体库存。	**9.7.1** 回顾媒体盘点日志以验证日志维护和媒体库存至少每年进行一次。	
9.8 销毁介质时，它不再需要为商业或法律原因如下：	**9.8** 检查周期性媒体破坏策略，并确认它涵盖了所有媒体，并规定了以下要求： • 硬拷贝材料必须横切粉碎，焚烧或打浆，使得有合理保证的硬拷贝材料无法重建。 • 用于将要被销毁的材料储存容器必须是安全的。 • 电子媒介上的持卡人数据必须呈现不可恢复的（例如，经由安全按照业界公认的标准安全删除，或者通过物理地破坏介质擦拭程序）。	如果不采取措施销毁包含在处置前，硬盘，移动硬盘，CD / DVD或纸张的信息，恶意的人也许能够检索从该设置的媒体信息，导致数据泄漏。例如，恶意个人可以使用被称为“垃圾箱”，他们通过垃圾桶和回收站寻找，他们可以用它来发动攻击信息搜索的技术。固定用于那些将要被销毁的材料储存容器防止的同时，将回收的物料被捕获的敏感信息。例如，“要被切碎的”容器可以有一个锁防止访问其内容或物理烯丙基防止进入容器的内部。为安全地销毁电子媒介的方法的例子包括安全擦除，消磁，
9.8.1 撕碎，焚烧，或纸浆硬拷贝材料以便持卡人数据不能被重建。用于将要被销毁的材料安全储存容器。	**9.8.1.a** 面试人员和检验程序，以验证硬拷贝材料横切粉碎，焚烧或打浆，使得有合理的保证硬拷贝材料无法重建。	
	9.8.1.b 检查用于包含待销毁的信息，以验证该容器被固定的材料的存储容器。	
9.8.2 渲染电子媒介上的持卡人数据不可恢复，使持卡人数据不能被恢复。	**9.8.2** 验证在电子媒体呈现不可恢复的持卡人数据（例如，经由安全按照业界公认的标准安全删除，或者通过物理地破坏介质擦拭程序）。	

PCI DSS要求	测试程序	指导
9.9 保护装置捕获支付卡通过与卡直接物理相互作用篡改和替代数据。 ***注意：这些要求适用于卡 - 卡存在的交易中使用阅读器（即刷卡或DIP）在销售点。这个要求并不适用于手动键输入组件，如计算机键盘和POS键盘。***	**9.9 检查文件的政策和程序，以验证它们包括：** • 维护设备的列表 • 定期检查设备，以寻找篡改或替换 • 培养人才要注意可疑行为，并报告设备的篡改或替换。	罪犯试图通过窃取和/或操纵读卡设备和终端来窃取持卡人的数据。例如，他们会去抢设备，使他们能够学会如何闯入他们，他们经常尝试用每次输入卡时，向他们发送支付卡信息欺诈手段，以取代合法设备。犯罪分子也将尝试，通过在合法读卡器，这样的顶部安装一个额外的读卡器加上"撇油"成分的设备，其目的是为了获取支付卡信息，他们甚至进入设备，例如之前的外支付卡细节被捕获两次：一次通过罪犯的组件，然后通过设备的合理成分。通过这种方式，交易可能仍然没有中断，而犯罪是"走过场"的过程中的支付卡信息完成。建议这一要求，但不是必需的，手动键输入组件，如计算机键盘和POS键盘。上一掠预防其他最佳实践可在PCI SSC网站上。
9.9.1 保持设备的先进的最新名单。该清单应包括以下内容： • 制作，设备的型号 • 设备的位置（例如，其中该装置位于该场地或设施的地址） • 设备序列号或唯一标识的其它方法。	**9.9.1.a 检查设备，以验证它包含的列表：** • 制作，设备的型号 • 设备的位置（例如，其中该装置位于该场地或设施的地址） • 设备序列号或唯一标识的其它方法。	保持设备的跟上时代的列表可以帮助的，其中设备被认为是，并快速识别，如果设备丢失或丢失的组织跟踪。用于保持设备的列表的方法可以是自动的（例如，一个设备管理系统）或手动（例如，在电子或纸质记录记录）。有关路线的装置，该位置可以包括为之设备分配的人员的名字。
	9.9.1.b 从列表中选择设备的样品，观察设备和设备的位置，以验证清单的准确性和及时更新。	
	9.9.1.c 面试人员核实设备列表更新时添加的设备，搬迁，退役等。	

PCI DSS要求	测试程序	指导
9.9.2 定期检查设备表面来检测篡改（例如，除了卡撇油器的装置），或者取代（例如，通过检查序列号或其它的器件特性以验证它没有被交换与欺诈装置）。 ***注意：** 该设备可能已被篡改或被取代标志的例子包括意外附件或插入设备电缆，丢失或改变的防伪标签，破损或不同颜色的外壳，或更改序列号或其他外部标记。*	**9.9.2.a 检查文件的程序，以验证被定义为包括以下过程：** • 程序检查设备 • 检查的频率。 **9.9.2.b 采访专人负责观察检验过程来验证：** • 工作人员都知道的用于检查设备的程序。 • 所有设备都定期检查篡改和取代的证据。	设备的定期检查将帮助企业更迅速地检测篡改或更换设备，从而最大限度地减少使用欺诈手段的潜在影响。该类型的检查将取决于装置 - 例如，被称为是安全设备的照片，可用于设备的当前外观比较原来的样子，看它是否已经改变。另一个选项可以是使用一个安全的标记笔，诸如UV光的标记，以标记设备的表面和设备的开口，从而任何篡改或替换是显而易见的。罪犯将经常更换外壳的装置的隐藏自己的篡改，并且这些方法可以帮助检测此类活动。设备供应商也能够提供安全指导和"如何"指南，帮助确定设备是否被篡改。检查的频率将取决于多种因素，例如设备的位置，以及是否该装置参与或无人参与。例如，留在公共区域，而由该组织的人员实施监察设备可具有比保持在安全区域或他们是向公众开放时被监控设备更频繁的检查。类型和检查的频率由商家决定的，通过他们的年度风险评估过程的定义。由该组织的人员留在公共场所没有监督的设备可能有比保持在安全区域或他们是向公众开放时被监控设备更频繁的检查。类型和检查的频率由商家决定的，通过他们的年度风险评估过程的定义。由该组织的人员留在公共场所没有监督的设备可能有比保持在安全区域或他们是向公众开放时被监控设备更频繁的检查。类型和检查的频率由商家决定的，通过他们的年度风险评估过程的定义。

PCI DSS要求	测试程序	指导
9.9.3 提供培训人员要意识到企图篡改或更换的设备。培训应包括以下内容： • 验证任何第三方的人自称是修理或维修人员，之前授予他们访问和修改或排除设备的身份。 • 不要安装，更换或无需验资返回装置。 • 请注意周围的设备（例如，身份不明的人试图拔掉或打开设备）可疑行为。 • 报告可疑行为和篡改设备的指示或替换，以适当的人员（例如，经理或保安人员）。	**9.9.3.a 在点销售地点人员审查培训材料，以核实它们包括以下训练：** • ，授予他们访问之前验证任何第三方的人自称修理或维护人员的身份修改或排除设备故障 • 不安装，更换或无需验资返回装置 • 意识到可疑行为的周围设备（例如，身份不明的人试图拔掉或打开设备） • 报告可疑行为和篡改设备的指示或替换，以适当的人员（例如，经理或保安人员）。 **9.9.3.b 在点销售地点面试人员的样本，以验证他们已经接受了培训，并了解以下的步骤：** • ，授予他们访问之前验证任何第三方的人自称修理或维护人员的身份修改或排除设备故障 • 不安装，更换或无需验资返回装置 • 意识到可疑行为的周围设备（例如，身份不明的人试图拔掉或打开设备） • 报告可疑行为和篡改设备的指示或替换，以适当的人员（例如，经理或保安人员）。	犯罪分子往往会伪装成授权的维修人员，为了获取POS设备。请求**访问设备的所有第三方应始终被设置访问之前进行验证 - 例如，通过**与管理检查或打电话的POS维修公司（如供应商或获取部）进行验证。许多犯罪分子将试图通过敷料的部分（例如，携带工具箱和工作装打扮）愚弄人员，也可以是知识渊博的有关设备的位置，所以它的人员进行培训，以遵守在任何时候都程序的重要。另一个技巧犯罪分子喜欢用是发送一个“新”的POS系统指令具有合法的系统和“返回”的合法系统交换到一个指定的地址。犯罪分子甚至可以提供来回邮费，因为他们都非常渴望得到他们的手在这些设备上。人才始终与他们的经理或供应商，该装置是合法的，并安装它或将其用于业务前，从可信的来源进行验证。
9.10 确保限制对持卡人数据的物理访问的安全政策和操作程序都记录，在使用中，和已知的所有当事方。	**9.10 检查文件和采访人员，以验证安全政策和操作程序，从而限制对持卡人数据的物理访问是：** • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全策略和限制在连续的基础上对持卡人数据和CDE系统物理访问操作程序。

定期监控和测试网络

要求10：跟踪并监控所有访问网络资源和持卡人数据

记录机制和跟踪用户活动的能力是在预防，检测，或最小化数据妥协的影响是至关重要的。日志在所有环境中的存在使深入跟踪，警报和分析时，确实存在错误。确定妥协的原因是非常困难的，如果不是不可能的，没有系统活动日志。

PCI DSS要求	测试程序	指导
10.1 实行审计跟踪所有访问系统部件链接到每个用户。	**10.1** 检查，通过观察和访谈系统管理员，即： • 审计跟踪已启用，积极为系统组件。 • 系统组件的访问链接到个人用户。	这是关键的是具有链接用户访问系统组件访问的过程或系统。该系统产生的审计日志，并提供可疑活动追溯到特定用户的能力。
10.2 实现对所有系统组件以重建以下事件自动化审计跟踪：	**10.2** 通过责任人员，审计日志的观察，以及审计日志设置检查的采访，执行以下操作：	可疑活动产生的审计跟踪提醒系统管理员，将数据发送到其他的监督机制（如入侵检测系统），并为事故后跟进历史踪迹。以下事件的记录使组织能够识别和追踪潜在的恶意活动
10.2.1 所有个人用户访问持卡人数据	**10.2.1** 验证持卡人数据的所有个人访问记录。	恶意个人可以获取用户帐户的知识，对系统的访问在CDE，或者他们可以以访问持卡人数据创建一个新的，未经授权的帐户。所有单个的记录访问持卡人数据的可识别可能已被破坏或误用的帐户。
10.2.2 任何个人采取的所有行动以根用户或管理员权限	**10.2.2** 验证由具有root权限或管理权限的任何个人采取的所有行动将被记录。	帐户具有增加的特权，如“管理员”或“根”的帐户，有可能极大地影响系统的安全性或操作功能的潜力。如果没有日志进行的活动，一个组织是无法追溯从管理失误或特权滥用回到具体的行动和个人造成任何问题。

PCI DSS要求	测试程序	指导
10.2.3 访问所有审计线索	**10.2.3** 验证访问所有的审计跟踪记录。	恶意用户经常试图改变审计日志隐藏自己的行动，并获得的记录使企业能够跟踪任何不一致或日志的潜在篡改的个人账户。能够访问日志标识的改变，添加和删除可以帮助追溯未经授权的人员作出步骤。
10.2.4 无效的逻辑访问尝试	**10.2.4** 验证无效的逻辑访问尝试登录。	恶意的个体往往会进行有针对性的系统多址接入尝试。多次无效的登录尝试可能是未经授权的用户企图以“强力”的指示或猜到的密码。
10.2.5 使用和更改标识和认证机制，包括但不限于创建新的账户和升高的特权，和所有的修改，增加或删除账目以根用户或管理员权限	**10.2.5.a** 验证使用的身份识别和认证机制登录。	不知道谁是在事件发生时登录，它是不可能识别可能已被使用的账户。此外，恶意用户可能会尝试操纵验证控制与绕过他们或模仿有效帐户的意图。
	10.2.5.b 检查的权限的所有海拔记录。	
	10.2.5.c 验证所有的变化，增加或删除任何帐户以根用户或管理员权限登录。	
10.2.6 初始化，停止或审计日志暂停	**10.2.6** 验证记录如下： • 审计日志的初始化 • 停止或审计日志的暂停。	转动审计注销（或暂停它们）执行的非法活动之前是希望避免检测恶意用户的通常做法。审计日志的初始化，这可能表明日志功能被用户禁用隐藏自己的行动。
10.2.7 创建和删除系统级对象	**10.2.7** 验证创建和系统级对象的删除记录。	恶意软件，例如恶意软件，常常创建或以控制该系统中的特定的功能或操作的目标系统上替换系统级对象。通过系统级的对象，如数据库表或存储过程，创建或删除记录时，它会更容易确定这种改变是否被授权。

PCI DSS要求	测试程序	指导
10.3 至少记录所有系统组件的每个事件的下列审计跟踪条目：	**10.3** 通过访谈和审计日志的观察，对于每个可审计事件（从10.2），执行以下步骤：	通过在10.2记录这些细节的审计事件，潜在的妥协，可以快速识别，并有足够的细节，知道是谁，什么，在哪里，何时以及如何。
10.3.1 用户识别	**10.3.1** 验证用户标识包含在日志条目。	
10.3.2 事件的类型	**10.3.2** 事件的验证类型包含在日志条目。	
10.3.3 日期和时间	**10.3.3** 检查日期和时间标记包含在日志条目。	
10.3.4 成功或失败指示	**10.3.4** 验证成功或失败的指示被包括在日志条目。	
10.3.5 事件的起源	**10.3.5** 验证事件的起源是包含在日志条目。	
10.3.6 身份或受影响的数据，系统组件或资源的名称。	**10.3.6** 验证身份或受影响的数据，系统组件或资源的名称包含在日志条目。	
10.4 使用时间同步技术，同步所有重要的系统时钟和时间，并确保以下是采集，分配和存储时间来实现。 ***注意：** 时间同步技术的一个例子是网络时间协议（NTP）。*	**10.4** 检查配置标准和过程，以验证时间同步技术被实施并且保持每PCI DSS要求6.1和6.2的电流。	时间同步技术用于同步在多个系统时钟。如果时钟不正确同步，也可以是困难的，如果不是不可能的，比较从登录不同的系统文件，并（在违约的情况下进行取证分析是至关重要的）建立事件的确切顺序。对于事后取证团队，准确性和所有系统的时间一致性和每个活动的时间是确定系统是如何被泄露的关键。
10.4.1 关键系统有正确和一致的时间。	**10.4.1.a** 检查获取，分配和存储在正确的时间在组织内，以验证过程： • 只有指定的中央时间服务器（S）从外部源接收时间信号，以及来自外部的时间信号是根据国际原子时或UTC。 • 哪里有不止一个指定的时间服务器，时间服务器彼此同行保持准确的时间， • 系统只接收来自指定的中央时间服务器（S）的时间信息。	

PCI DSS要求	测试程序	指导
	10.4.1.b 观察系统组件来验证的样本的时间相关系统参数设置： • 只有指定的中央时间服务器（S）从外部源接收时间信号，以及来自外部的时间信号是根据国际原子时或UTC。 • 凡有一个以上的指定时间服务器，彼此指定的中央时间服务器（S）等，以保持精确的时间。 • 系统只接收来自指定的中央时间服务器（一个或多个）时间。	
10.4.2 时间数据是受保护的。	**10.4.2.a 检查系统配置和时间同步设置，以验证访问时间数据仅限于人员与业务需要**访问实时数据。	
	10.4.2.b 检查系统配置，时间同步设置和日志，和过程，以验证对关键系统时间设置的任何变化被记录，监控和审查。	
10.4.3 时间设置是由业界公认的时间源接收。	**10.4.3 检查系统配置，以验证时间服务器（一个或多个）接受特定的，业界公认的外**部来源的时间更新（以防止恶意个人更改时钟）。任选地，这些更新可以使用对称密钥被加密，和访问控制列表可以创建指定将被提供的时间更新（以防止未经授权的使用的内部时间服务器）的客户端计算机的IP地址。	
10.5 安全审计跟踪，使他们不能被改变。	**10.5 面试系统管理员和检查系统配置和权限验证审计跟踪固定，使它们不能被**改变，如下所示：	通常谁已进入网络的恶意个人会尝试以隐藏自己的活动来编辑，审核日志。如果没有审计日志的充分保护，他们的完整性，准确性和完整性无法保证，且审计日志可以作为一种妥协经过调查工具形同虚设。

PCI DSS要求	测试程序	指导
10.5.1 审计的限制观看落后于那些与工作相关的需要。	**10.5.1** 只有谁有工作有关的需求可以查看审计跟踪文件的人。	审计日志的充分保护包括强大的访问控制（限制访问基于日志的“需要知道”只），以及使用物理或网络隔离，使日志很难发现和修改。及时备份日志，是难以改变集中式日志服务器或媒体不断即使系统生成的日志被泄露保护的日志。
10.5.2 从未经授权的修改保护审计跟踪文件。	**10.5.2** 当前审核记录文件通过访问控制机制，物理分离和/或网络隔离保护，未经授权的修改。	
10.5.3 及时的审计线索文件备份到难以改变集中式日志服务器或媒体。	**10.5.3** 当前审核记录的文件及时备份到很难改变集中式日志服务器或媒体。	
10.5.4 写面向外部的技术，登录到一个安全，集中，内部日志服务器或媒体设备。	**10.5.4** 对于面向外部的技术（例如，无线，防火墙，DNS，邮件）日志被写入到一个安全，集中，内部日志服务器或媒体。	通过从面向外部的技术，如无线，防火墙，DNS和邮件服务器的日志写入，丢失或改变这些日志的风险被降低，因为它们在内部网络中更安全。日志可被直接写入，或卸载或从外部系统复制到安全内部系统或媒体。
10.5.5 使用文件完整性监控或变更检测软件对日志，以确保现有的日志数据在不产生警报（尽管添加新的数据应该不会引起警报）来改变。	**10.5.5** 从监测活动，以验证监测使用的文件的完整性或更改检测软件对日志检查系统设置，监视的文件，和结果。	文件完整性监控或变更检测系统检查更改重要文件，当这样的变化说明通知。对于文件级的完整性监控目的，实体通常监控不定期更改的文件，但改变的时候表示可能的妥协。
10.6 所有系统组件的审查日志和安全事件来识别异常或可疑的活动。 ***注意：** 日志收集，分析和报警工具，可以用来满足这一要求。*	**10.6** 执行以下操作：	许多违规行为发生在被发现前几天或几个月。由人员或自动方式进行定期日志检查可以识别并主动解决持卡人数据环境的未授权访问。日志审查过程并不一定是手动。使用日志收集，分析的，和报警工具可以帮助方便识别需要进行审查日志事件的过程。

PCI DSS要求	测试程序	指导
10.6.1 每天至少查看以下内容： • 所有安全事件 • 储存，处理或传输CHD和/或SAD的所有系统组件的日志 • 所有关键系统组件的日志 • 执行安全功能（例如，防火墙，入侵检测系统/入侵预防系统（IDS / IPS），认证服务器，电子商务重定向服务器等）中的所有服务器和系统组件的日志。	**10.6.1.a** 检查安全政策和程序，以手动或通过日志工具验证程序每天至少阅读下列定义： • 所有安全事件 • 储存，处理或传输CHD和/或SAD的所有系统组件的日志 • 所有关键系统组件的日志 • 执行安全功能（例如，防火墙，入侵检测系统/入侵预防系统（IDS / IPS），认证服务器，电子商务重定向服务器等）中的所有服务器和系统组件的日志	日常检查记录最大限度地减少时间和潜在的违反曝光量。安全事件 - 每日复习例如，从执行安全功能的系统，如防火墙通知或标识从关键系统组件可疑或异常活动，以及日志警报和日志，IDS / IPS，文件完整性监控（ FIM ）系统等是必要的，以确定潜在的问题。请注意，“安全事件”的决心会为每个组织有所不同，可能包括技术，位置和设备的功能类型考虑。企业还可能希望维持“正常”流量基线，以帮助识别异常行为。
	10.6.1.b 观察过程和面试人员核实了以下每天至少综述： • 所有安全事件 • 储存，处理或传输CHD和/或SAD的所有系统组件的日志 • 所有关键系统组件的日志 • 执行安全功能（例如，防火墙，入侵检测系统/入侵预防系统（IDS / IPS），认证服务器，电子商务重定向服务器等）中的所有服务器和系统组件的日志。	
10.6.2 所有其他系统组件的审查日志，定期根据组织的政策和风险管理策略，由该组织的年度风险评估来确定。	**10.6.2.a** 检查安全策略和程序，以验证程序审查所有其他系统组件周期性手动或通过日志记录工具的定义，根据该组织的政策和风险管理策略。	对于所有其他系统组件的日志也应该定期审查，以确定潜在的问题指示或试图获得通过不太敏感的系统访问敏感系统。这些审查的频率应该由一个实体的年度风险评估来确定。
	10.6.2.b 检查组织的风险评估资料和面试人员核实评论是根据组织的政策和风险管理战略的执行。	
10.6.3 后续在审查过程中发现的异常和异常。	**10.6.3.a** 检查安全策略和程序，以验证程序对在审查过程中发现的异常和异常跟进定义。	如果在日志审查过程中发现的异常和异常不调查，该实体可能不知道被自己的网络内发生未经授权的和潜在的恶意活动。
	10.6.3.b 观察过程和面试人员核实被执行的后续例外和异常。	

PCI DSS要求	测试程序	指导
10.7 保留审计线索历史记录至少一年，以最小的立即可用于分析三个月内（例如，在线归档，或者从备份恢复原状）。	**10.7.a** 检查安全政策和程序，以验证其定义如下： • 审计日志保留策略 • 程序，以便审计日志至少一年，以最小的立即三种可用个月的在线。	保留日志至少一年允许的事实，它往往需要一段时间才能发现的妥协已经发生或正在发生，并允许调查人员提供足够的日志记录，以更好地确定潜在的违反和潜在的系统的时间长度（S）的影响。通过具有3个月日志立即可用，实体可以快速识别和减少数据泄露的影响。在离线位置存储日志可以防止它们被容易获得，从而导致较长的时间帧，以恢复的日志数据，执行分析，并确定受影响的系统或数据。
	10.7.b 面试人员和检查审计日志，以验证审计日志至少保留一年。	
	10.7.c 面试人员和观察的过程，以确认至少在过去三个月的日志，可立即进行分析。	
10.8 ***只有服务提供商附加要求：*** **实施一个流程，及时发现和关键安全控制系统故障的报告，包括但不限于失败：** • 防火墙 • IDS / IPS • FIM • 反病毒 • 物理访问控制 • 逻辑访问控制 • 审计日志机制 • 分割控制（如果使用）	**10.8.a** 检查文件的政策和程序，以验证过程，以便及时发现和关键安全控制系统的故障报告定义，包括但不限于失败： • 防火墙 • IDS / IPS • FIM • 反病毒 • 物理访问控制 • 逻辑访问控制 • 审计日志机制 • 分割控制（如果使用）	***注意：此要求仅适用于被评估的实体是服务提供商。*** 没有经过正规程序来检测和警报时的重要安全控制失效，故障可能未被发现长时间，并为攻击者提供充足的时间来从持卡人数据环境破坏系统，窃取敏感数据。特定类型的故障可以根据设备和技术在使用的函数而变化。典型故障包括系统停止执行其安全功能或在其预期的方式无法运作; 例如，防火墙删除其所有的规则或脱机。
	10.8.b 检查检测和报警流程及面试人员确认过程为所有关键安全控制来实现，并在警报产生严重的安全控制结果失败。	

PCI DSS要求	测试程序	指导
10.8.1 ***只有服务提供商附加要求：*** **应对任何关键的安全控制的故障及时。为应对故障的安全控制必须包括流程：** • 恢复安全功能 • 确定和记录安全故障时间（日期和时间开始到结束） • 确定和记录失败的原因（S），包括根本原因，和记录补救，以解决根本原因需要 • 识别和解决故障期间出现的任何安全问题 • 执行风险评估，以确定进一步的行动是否需要为安全故障导致 • 实施控制，以防止故障原因再次发生 • 安全控制的恢复监测	**10.8.1.a 检查记录的政策和程序，面试人员核实过程定义和实现对安全控制的故障响应，包括：** • 恢复安全功能 • 确定和记录安全故障时间（日期和时间开始到结束） • 确定和记录失败的原因（S），包括根本原因，和记录补救，以解决根本原因需要 • 识别和解决故障期间出现的任何安全问题 • 执行风险评估，以确定进一步的行动是否需要为安全故障导致 • 实施控制，以防止故障原因再次发生 • 安全控制的恢复监测 **10.8.1.b 检查记录，验证安全控制失效都记录包括：** • 失败的原因（一个或多个）的鉴定，包括根本原因 • 持续安全故障（日期和时间开始和结束） • 整治的细节需要解决的根本原因	***注意：此要求仅适用于被评估的实体是服务提供商。*** 如果关键的安全控制故障警报是不能迅速有效地回应，攻击者可能利用这段时间来插入恶意软件，获得系统的控制权，或窃取从实体的环境数据。书面证据（例如，问题管理系统中记录）应支持流程和程序到位，以安全故障响应。此外，工作人员应在发生故障时意识到自己的责任。操作和响应故障应在书面证据被捕获。
10.9 确保监控所有访问网络资源和持卡人数据的安全政策和操作程序都记录，在使用中，和已知的所有当事方。	**10.9 检查文件和采访人员，以验证安全政策和操作程序监控所有访问网络资源和持卡人数据有：** • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全政策和监督在连续的基础上的所有访问网络资源和持卡人数据的日常运作程序。

要求11：定期测试安全系统和流程。

漏洞被恶意个人和研究人员不断发现，并通过新的软件被引入。系统组成，流程和定制软件应经常测试，以确保安全控制继续反映不断变化的环境。

PCI DSS要求	测试程序	指导
11.1 实施过程以测试的无线接入点（802.11）的存在，以及检测和识别每季所有授权和未授权的无线访问点。 ***注意：*** *可在过程中使用的包括但不限于无线网络的扫描，系统组件和基础设施，网络访问控制的物理/逻辑检查（NAC）的方法，或无线IDS / IPS。* *无论使用方法，就必须有足够的探测和识别授权和未授权的设备。*	**11.1.a 检查政策和程序，以验证过程进行检测和授权和未经授权的无线接入点的**识别每季定义。	实施和/或网络中的无线技术的开发是一些恶意用户最常用的路径来访问网络和持卡人数据。如果无线设备或网络没有一家公司的知识安装，它可以使攻击者很容易和“无形”进入网络。未授权的无线设备可以内被隐藏或连接到计算机或其他系统部件，或直接连接到网络端口或网络设备，诸如交换机或路由器。任何非授权的设备可能会导致未经授权的接入点到环境中。知道哪些无线设备被授权可以帮助管理员快速识别非授权的无线设备，和响应未经授权的无线接入点的识别，有助于最大限度地减少主动CDE暴露于恶意的人。由于与该无线接入点可以连接到一个网络，在检测它们的存在的困难的容易性，并且被未授权的无线设备呈现的增加的风险，即使在策略存在禁止使用无线技术的这些过程必须被执行。特定环境将决定适当的工具和流程的规模和复杂性，以用于提供足够的保证，一个流氓无线接入点没有安装在环境中。和未经授权的无线设备出现的风险增加，这些流程必须即使存在政策禁止使用无线技术的执行。特定环境将决定适当的工具和流程的规模和复杂性，以用于提供足够的保证，一个流氓无线接入点没有安装在环境中。和未经授权的无线设备出现的风险增加，这些流程必须即使存在政策禁止使用无线技术的执行。特定环境将决定适当的工具和流程的规模和复杂性，以用于提供足够的保证，一个流氓无线接入点没有安装在环境中。 *（接下页）*
	11.1.b 验证方法是足够的探测和识别任何未经授权的无线接入点，至少包括以下内容： • 插入到系统组件WLAN卡 • 附接到系统组件的便携式或移动设备创建一个无线接入点（例如，通过USB等） • 无线设备连接到网络端口或网络设备。	
	11.1.c 如果利用无线扫描，检查从最近的无线扫描以验证输出： • 授权和未授权的无线接入点被识别，并 • 该扫描所有系统组件和设备进行至少每季度一次。	
	11.1.d 如果自动监视被利用（例如，无线IDS / IPS，NAC等），验证配置将生成警报以通知工作人员。	

PCI DSS要求	测试程序	指导
11.1.1 维持授权的无线接入点的清单包括记录商业理由。	**11.1.1** 检查记录的记录，验证授权的无线接入点的库存维护和业务理由是记录所有授权的无线接入点。	***例如：*** *在一个商场的单个独立零售亭，其中所有的通信组件都包含防篡改和防篡改外壳内，执行所述售货亭的详细物理检查的情况下本身可足以提供保证，即一个恶意无线接入点尚未连接或安装。然而，在具有多个节点（例如，在一个大型零售商店，呼叫中心，服务器室或数据中心）的环境中，详细的物理检查是困难的。在这种情况下，多种方法可被组合以达到要求，如结合无线分析器的结果进行物理系统检查。*
11.1.2 落实在事件中检测到未经授权的无线接入点的事件响应程序。	**11.1.2.a** 检查组织的事故应急预案（12.10需求）来验证它定义和规定，检测到未经授权的无线接入点的事件的响应。	
	11.1.2.b 负责面试的人员和/或检查最近的无线扫描和相关的应答验证行动时，发现未经授权的无线接入点取。	

PCI DSS要求	测试程序	指导
11.2 运行的内部和外部网络漏洞扫描至少每季度和网络中的任何显著改变（如新系统组件的安装，在网络拓扑结构的变化，防火墙规则的修改，产品升级）后。 ***注意：*** *多重扫描报告可以合并为季度扫描过程表明，所有的系统进行扫描和所有适用的安全漏洞已经得到解决。附加文件可能需要验证非修复漏洞是在被寻址的进程。* *对于最初的PCI DSS合规性，它并不要求通过扫描四个季度如果评估验证完成1）最近的扫描结果是通过扫描，2）实体已经成文的政策和程序，要求每季度扫描，以及3）在扫描结果指出漏洞已经被校正，如图重新扫描（一个或多个）。对于最初的PCI DSS审查之后随后的几年中，通过扫描的四个季度中必须发生。*	**11.2** 检查扫描报告和支持文件来验证内部和外部漏洞扫描如下进行：	漏洞扫描是自动或手动工具，技术的组合，和/或方法运行针对外部和内部网络设备和服务器，被设计以暴露可能被发现并且由恶意的个人利用的潜在漏洞。有三种类型的PCI DSS要求的漏洞扫描： • （不需要使用一个PCI SSC授权扫描供应商（ASV）的）由合格人员内部季度漏洞扫描 • 外部季度漏洞扫描，这必须由ASV来执行 • 根据需要，之后一旦这些弱点显著变化确定内部和外部扫描，实体纠正他们并重复扫描，直到所有的漏洞已得到纠正。识别和及时解决脆弱性降低被利用的漏洞和系统组件或持卡人数据的潜在损害的可能性。
11.2.1 每季度进行内部漏洞扫描。地址漏洞并进行重新扫描，以确认所有的“高风险”漏洞是按照实体的脆弱性排名解析（按要求 6.1）。扫描必须由合格的专业人员进行。	**11.2.1.a** 查看扫描报告，确认四个季度内扫描发生在最近的12个月期间。 **11.2.1.b** 查看扫描报告，并确认所有的“高风险”漏洞得到解决和扫描流程包括重新扫描，以验证“高风险”漏洞（如PCI DSS要求6.1所定义的）都解决了。	用于识别在内部系统上的漏洞建立的过程要求漏洞扫描每季度进行。构成最大风险的环境中的漏洞（例如，每排6.1的要求“高”）应具有最高优先级来解决。 *（接下页）*

PCI DSS要求	测试程序	指导
	11.2.1.c 面试人员核实，该扫描是由合格的内部资源（S）或合格的外部第三方执行，如果测试仪的应用，组织上的独立性存在（不是一个QSA或ASV需要）。	内部脆弱性扫描可以由有资格的，内部的工作人员，是相当独立的被扫描的系统组件（或多个）的情况下进行（例如，防火墙管理员不应该负责扫描防火墙），或实体可以选择具有内部脆弱性通过扫描一个公司，专门从事漏洞扫描进行。
11.2.2 执行季度外部漏洞扫描，通过由支付卡行业安全标准委员会（PCI SSC）批准的授权扫描供应商（ASV）。执行重新扫描可以根据需要，通过之前的扫描来实现的。 ***注意：季度外部漏洞扫描必须由授权扫描供应商（ASV），由支付卡行业安全标准委员会（PCI SSC）批准执行。*** *请参阅PCI SSC网站扫描客户的责任，扫描制剂等上公布的ASV计划指南*	**11.2.2.a 回顾从外部脆弱性扫描最近四个季度的输出，并验证四次季度外部漏洞**扫描发生在最近的12个月期间。	由于外部网络是在妥协的风险更大，每季度外部漏洞扫描必须由PCI SSC授权扫描供应商（ASV）来执行。一个强大的扫描程序确保了扫描被执行，并且漏洞及时解决。
	11.2.2.b 查看每个季度的扫描结果并重新扫描，以确认对路过的扫描ASV计划指南的要求已得到满足（例如，没有漏洞评为4.0或更高版本由CVSS，并没有自动失效）。	
	11.2.2.c 查看扫描报告，以验证扫描，通过PCI SSC授权扫描供应商（ASV）完成。	
11.2.3 执行内部和外部的扫描，并重新扫描根据需要，任何显著变化之后。扫描必须由合格的专业人员进行。	**11.2.3.a 检查和相关的变更控制文件和扫描报告，以验证系统组件受到**被扫描的任何显著的变化。	什么构成显著变化的确定在很大程度上取决于给定环境的配置。如果升级或改造可能允许访问持卡人数据或影响持卡人数据环境的安全性，那么就可以考虑显著。由任何显著更改后扫描的环境中确保变更完成适当使得环境的安全不受损害的变化的结果。受变更影响的所有系统组件都需要进行扫描。
	11.2.3.b 查看扫描报告，并确认扫描流程包括重新扫描，直到： • 对于外部扫描，不存在安全漏洞了由CVSS得分4.0或更高。 • 对于内部扫描，如PCI DSS要求6.1所定义的所有“高危”漏洞得到解决。	

PCI DSS要求	测试程序	指导
	11.2.3.c 验证扫描由合格的内部资源（S）或合格的外部第三方执行，如果测试仪的应用，组织上的独立性存在（不是一个QSA或ASV需要）。	
11.3 实施包括以下渗透测试的方法： • 基于行业认可的渗透测试方法（例如，NIST SP800-115） • 包括覆盖整个CDE的周长和关键系统 • 包括来自内，外网测试 • 包括测试，以验证任何分割和范围的还原控制 • 定义应用层渗透测试包括，在最低限度，漏洞要求6.5所列 • 定义网络层渗透测试以包括支持网络功能的组件以及操作系统 • 包括在过去12个月中经历威胁和脆弱性审查和审议 • 指定渗透测试结果和整治活动成果的保留。	**11.3 检查渗透测试方法和面试负责人员核实的方法来实现，包括以下内容：** • 基于行业认可的渗透测试方法（例如，NIST SP800-115） • 包括覆盖整个CDE的周长和关键系统 • 从内部和外网测试 • 包括测试，以验证任何分段和scope-还原控制 • 定义应用层渗透测试包括，在最低限度，漏洞要求6.5所列 • 定义网络层渗透测试以包括支持网络功能的组件以及操作系统 • 包括在过去12个月中经历威胁和脆弱性审查和审议 • 指定渗透测试结果和整治活动成果的保留。	渗透测试的目的是模拟真实世界的攻击情况与识别攻击者将在多大程度上能够渗透到的环境的目标。这允许更好地了解他们的潜在风险，并制定一项战略，以抵御攻击的实体。渗透测试从漏洞扫描不同，作为渗透测试是一个积极的过程，其可以包括利用确定的漏洞。在进行漏洞扫描可以是第一步骤的渗透测试将为了计划测试策略执行一个，虽然它并不是唯一的步骤。即使漏洞扫描没有检测已知的漏洞，渗透测试者往往会获得足够的知识有关的系统来识别可能的安全漏洞。渗透测试通常是高度手动过程。虽然可以使用一些自动化工具，测试人员使用他们的系统知识渗透到环境中。通常情况下，测试者将链几种类型的漏洞通过层层设防突破的目标共同努力。例如，如果测试人员发现来访问应用程序服务器的手段，他们会再使用被感染的服务器作为一个点阶段基于服务器可以访问资源的新的攻击。通过这种方式，测试能够模拟攻击者进行识别环境中潜在的薄弱环节的方法。如果测试人员发现来访问应用程序服务器的手段，他们会再使用被感染的服务器作为一个点阶段基于服务器可以访问资源的新的攻击。通过这种方式，测试能够模拟攻击者进行识别环境中潜在的薄弱环节的方法。如果测试人员发现来访问应用程序服务器的手段，他们会再使用被感染的服务器作为一个点阶段基于服务器可以访问资源的新的攻击。通过这种方式，测试能够模拟攻击者进行识别环境中潜在的薄弱环节的方法。 *渗透测试技术将是不同的组织不同，类型，深度和测试的复杂性将取决于具体的环境和组织的风险评估。*

PCI DSS要求	测试程序	指导
11.3.1 演出 *外部* 渗透测试至少每年和任何显著基础设施或应用程序升级或修改后（如操作系统升级，子网络添加到环境中，或添加到环境中的web服务器）。	**11.3.1.a 检查从最近的外部渗透测试工作和结果的范围，以验证如下执行的**渗透测试： • 每所定义的方法 • 至少每年一次 • 后对环境造成任何显著的变化。	定期和环境显著变化后进行渗透测试是主动的安全措施，有助于最大限度地减少被恶意个人的CDE潜在的访问。 什么构成显著升级或修改相关的确定在很大程度上取决于给定环境的配置。如果升级或改造可能允许访问持卡人数据或影响持卡人数据环境的安全性，那么就可以考虑显著。网络升级和修改后执行渗透测试提供了保证，假设在地方控制仍处于升级或修改后有效地开展工作。
	11.3.1.b 验证测试是由合格的内部资源或合格的外部第三方执行，如果测试仪的应用，组织上的独立性存在（不是一个QSA或ASV需要）。	
11.3.2 演出 *内部* 渗透测试至少每年和任何显著基础设施或应用程序升级或修改后（如操作系统升级，子网络添加到环境中，或添加到环境中的web服务器）。	**11.3.2.a 检查工作和结果的范围从最近的内部渗透测试，以验证如下执行的**渗透测试。 • 每所定义的方法 • 至少每年一次 • 后对环境造成任何显著的变化。	
	11.3.2.b 验证测试是由合格的内部资源或合格的外部第三方执行，如果测试仪的应用，组织上的独立性存在（不是一个QSA或ASV需要）。	
11.3.3 渗透测试期间发现利用的漏洞被校正和测试被重复以验证校正。	**11.3.3 检查渗透测试结果验证注意利用的漏洞进行修正和反复测试确认该漏**洞已得到纠正。	

PCI DSS要求	测试程序	指导
11.3.4 如果分割用于将CDE从其它网络隔离，至少每年进行渗透测试和任何改变之后在分段控制/方法来验证该分割方法是可操作的和有效的，并且隔离系统中的所有外的范围系统在在CDE。	**11.3.4.a 检查分段控制和审查渗透测试方法来验证penetration-测试程序被定义为测试所有的分割方法，以确认它们是可操作的和有效的，并且隔离所有外的范围从系统在CDE系统。**	渗透测试是确认到位的CDE与其他网络隔离任何分割是有效的一个重要工具。渗透测试应该集中在分割控制，无论是从实体的网络之外，来自网络内部，而是外部的CDE的，以确认它们无法通过分割控制，以获得访问CDE。例如，网络测试和/或扫描打开的端口，以验证在范围内和外的范围网络之间没有连接。
	11.3.4.b 检查从最近的渗透测试，以验证结果： • 渗透测试，以验证分割控制至少每年进行任何更改后分割控制/方法。 • 渗透测试涵盖了所有在用分段控制/方法。 • 渗透测试验证分割控制/方法的操作和有效的，并且从在CDE系统隔离所有外的范围的系统。	
	11.3.4.c 验证测试是由合格的内部资源或合格的外部第三方执行，如果测试仪的应用，组织上的独立性存在（不是一个QSA或ASV需要）。	
11.3.4.1 ***只有服务提供商附加要求：*** **如果使用了分割，**确认PCI DSS范围由上分割控制进行渗透测试，至少每6个月进行任何更改后分割控制/方法。	**11.3.4.1.a 检查从最近的渗透测试，以验证结果：** • 进行渗透测试，以验证分段控制至少每6个月进行任何更改后分割控制/方法。 • 渗透测试涵盖了所有在用分段控制/方法。 • 渗透测试验证分割控制/方法的操作和有效的，并且从在CDE系统隔离所有外的范围的系统。	***注意：此要求仅适用于被评估的实体是服务提供商。*** 对于服务提供商的PCI DSS范围确认应尽可能频繁地进行尽可能确保PCI DSS范围保持最新且不断变化的业务目标保持一致。

PCI DSS要求	测试程序	指导
	11.3.4.1.b 验证测试是由合格的内部资源或合格的外部第三方执行，如果测试仪的应用，组织上的独立性存在（不是一个QSA或ASV需要）。	
11.4 使用入侵检测和/或入侵防御技术来检测和/或防止侵入网络。监控所有的流量在持卡人数据环境的周边，以及在持卡人数据环境中的关键点，并提醒工作人员涉嫌妥协。 保留所有入侵检测和防御引擎，基线和签名是最新的。	**11.4.a** 检查系统配置和网络图来验证技术（例如入侵检测系统和/或入侵防御系统）到位，以监视所有流量： • 在持卡人数据环境的周边 • 在持卡人数据环境中的关键点。	入侵检测和/或入侵防御技术（如IDS / IPS），比较流量进入网络与已知的“签名”和/或十万妥协类型的行为（黑客工具，木马和其他恶意软件），并发送警报和/或停止尝试，因为它发生。如果没有一个积极的态度，未经授权的活动检测（或误用）计算机资源的攻击者可以去实时忽视。通过这些技术产生的安全警报应监测，以便企图侵入可以被停止。
	11.4.b 检查系统配置和面试负责人员确认入侵检测和/或入侵防御技术涉嫌妥协的警觉人员。	
	11.4.c 检查IDS / IPS配置和供应商文档验证入侵检测和/或预防intrusion-技术配置，维护和每个供应商的指令更新，以确保最佳的保护。	
11.5 部署一个变化检测机构（例如，文件完整性监控工具），以提醒人员未经授权的修改（包括改变，添加和缺失）的关键的系统文件，配置文件，或内容文件; 并配置该软件至少每周执行关键文件进行比较。 *（接下页）*	**11.5.a** 通过观察系统设置和监视的文件，以及审查的监督活动结果验证了利用变化检测机制。需要监控的文件示例： • 系统可执行文件 • 应用程序的可执行文件 • 配置和参数文件 • 集中存储，历史或存档，日志和审计文件 • 确定由实体（例如，通过风险评估或其他方式）的附加的重要文件。	变化检测解决方案，如文件完整性监控（FIM）工具检查更改，添加和重要文件删除，并在检测到这种变化时通知。如果没有正确实施和监督的变化检测解决方案的输出，恶意个人可以添加，删除或修改配置文件内容，操作系统程序或应用程序的可执行文件。未经授权的更改，如果未被发现，可以使现有的安全控制不力和/或导致持卡人数据与没有明显影响到正常的处理被盗。

PCI DSS要求	测试程序	指导
注意： *对于变化检测的目的，关键文件通常是那些不经常改变，但它的修改可能表明妥协系统受损或风险。更改检测机制，如文件完整性监控产品通常会与前对相关的操作系统的重要文件进行配置。其他重要文件，如自定义应用程序，必须进行评估，并由实体定义（即商户或服务提供商）。*	**11.5.b 验证机制配置，以提醒人员未经授权的修改（包括更改，添加和删除）的**关键文件，并至少每周执行关键文件进行比较。	
11.5.1 实施的处理，以通过变化 - 检测溶液中产生的任何响应警报。	**11.5.1 面试人员核实了所有警报被调查和解决。**	
11.6 确保安全监测和测试的安全政策和操作程序都记录，在使用中，和已知的所有当事方。	**11.6 检查文件和采访人员，以验证安全策略和进行安全监控和测试操作程序**是： • 记载， • 在使用中，和 • 已知的所有当事方。	人员需要了解并遵循安全策略和进行安全监控和测试一个连续的基础上运行程序。

维护信息安全策略

要求12：维护针对所有人员的信息安全策略。

强大的安全策略决定了整个实体的安全音，并通知工作人员对他们的期望的。所有人员都应该知道数据的敏感性及其在保护它的责任。对于要求12的目的，“工作人员”指的是全职和兼职员工，临时员工，承包商和顾问谁在实体的网站“驻留”或以其他方式访问持卡人数据环境。

PCI DSS要求	测试程序	指导
12.1 制定，发布，维护和传播安全策略。	**12.1 检查信息安全政策，并确认政策发布和传播到所有相关人员（包括供应商和业务合作伙伴）。**	一个公司的信息安全政策为执行安全措施，以保护其最有价值的资产的路线图。所有人员都应该知道数据的敏感性及其在保护它的责任。
12.1.1 至少每年检查安全策略和更新策略时的环境变化。	**12.1.1 确认为需要反映对业务目标或危险环境中的信息安全政策至少每年审查和更新。**	安全威胁和保护方法迅速发展。如果没有更新的安全策略，以反映有关的改变，新的保护措施，以防止这些威胁得不到解决战斗。
12.2 实施风险评估过程： • 在每年至少并且在环境变化显著（例如，获取，合并，重新定位等）被执行， • 识别关键资产，威胁和漏洞， • 结果在风险的一个正式的，成文的分析。 *风险评估方法的例子包括但不限于OCTAVE，ISO 27005和NIST SP 800-30。*	**12.2.a 验证的年度风险评估过程有文件证明：** • 标识的关键资产，威胁和漏洞 • 结果在风险的一个正式的，成文分析 **12.2.b 审查风险评估文档，以确认风险评估过程是在每年至少并在环境显著的变化进行的。**	风险评估使组织能够识别威胁和相关漏洞有潜力的业务产生负面影响。不同的风险因素的例子包括网络犯罪，网络攻击和恶意软件的POS机。资源就可以得到有效的分配来实现减少没有实现的可能性和/或威胁的潜在影响控制。 在进行风险评估每年至少一次并在显著的变化允许保持最新与组织变化和不断变化的威胁，趋势和技术的组织。

PCI DSS要求	测试程序	指导
12.3 制定关键技术的使用策略，并确定正确使用这些技术。 ***注意：关键技术的例子包括，但不限于，远程访问和无线技术，笔记本电脑，平板电脑，移动电子媒体，电子邮件使用率和互联网的使用。*** 确保这些使用政策要求如下：	**12.3 审查关键技术的使用策略，并采访负责人员核实以下政策落实如下：**	人才使用政策可以禁止使用某些设备和其他技术的，如果这是公司政策，或对人员，以正确的使用和实施提供指导。如果使用政策不到位，工作人员可使用的技术中违反公司政策，从而使恶意用户能够访问关键系统和持卡人数据。
12.3.1 明确批准，授权方	**12.3.1 验证使用政策包括从授权方明确授权使用的技术工艺。**	而不需要实施这些技术的适当的批准，个别人员可能无意实施解决方案，以感知业务需求，同时也打开科目关键系统和数据的恶意个人一个大洞。
12.3.2 验证使用的技术	**12.3.2 验证使用策略包括进程的所有技术使用与用户ID和密码或其他认证项目（例如，令牌）进行认证。**	如果技术没有适当认证（用户ID和密码，令牌，虚拟专用网等）实现，恶意个人可能很容易地使用此未受保护的技术来访问关键系统和持卡人的数据。
12.3.3 所有这些设备和人员访问的列表	**12.3.3 验证使用策略定义：** • 所有关键设备的列表，并 • 人员名单授权使用的设备。	恶意个人可能破坏物理安全性，并把网络作为自己的设备“后门”人事也可能绕过程序和安装设备。准确的清单以适当的设备标签可以快速识别未经批准的安装。

PCI DSS要求	测试程序	指导
12.3.4 的方法准确且容易地确定所有者，联系信息，和目的（例如， 标记，编码，和/或设备的盘点）	**12.3.4** 验证使用策略定义一个方法以准确和容易地确定所有者，联系信息，和目的（例如，标记，编码，和/或设备的盘点）。	恶意个人可能破坏物理安全性，并把网络作为自己的设备“后门”人事也可能绕过程序和安装设备。准确的清单以适当的设备标签可以快速识别未经批准的安装。考虑为设备建立一个正式的命名规则，并记录既定库存控制的所有设备。逻辑标记可以与信息可以采用例如，可以在设备到它的拥有者，联系信息，和目的相关代码。
12.3.5 该技术可允许的用途	**12.3.5** 验证使用策略定义的技术可允许的用途。	通过定义公司批准的设备和技术的可接受的商业用途和位置，该公司能够更好地配置和操作控制来管理和控制缺口，确保了“后门”恶意个人访问关键不打开系统和持卡人数据。
12.3.6 对于技术可接受的网络位置	**12.3.6** 验证使用策略定义了技术可接受的网络位置。	
12.3.7 公司批准的产品名单	**12.3.7** 验证使用策略包括公司批准的产品清单。	
12.3.8 活动的具体时间后进行远程访问技术的会话自动断开连接	**12.3.8.a** 验证使用政策要求不活动一定时间后进行远程访问技术的会话自动断开。	远程接入技术是频繁的“后门”对关键资源和持卡人数据。通过断开不使用时（例如，那些使用您的POS厂商，其他厂商，或业务伙伴来支持你的系统）远程访问技术，接入和风险网络被最小化。
	12.3.8.b 检查配置的远程访问技术来验证远程访问会话将闲置一定时间后自动断开。	
12.3.9 需要供应商和业务合作伙伴的远程接入技术的激活只有当供应商和商业合作伙伴，使用后立即停用	**12.3.9** 验证需要通过供应商和业务合作伙伴时，才使用后立即停用使用政策需要由供应商和业务合作伙伴使用远程访问技术的激活。	

PCI DSS要求	测试程序	指导
12.3.10 对于人员通过远程访问技术访问持卡人数据，禁止复制，移动，和持卡人数据的存储到本地硬盘驱动器和可移动电子媒介，除非明确授权规定的业务需求。哪里有授权的业务需求，使用政策必须要求数据符合所有适用的PCI DSS要求予以保护。	**12.3.10.a** 验证使用策略禁止复制，移动，或通过远程访问技术访问这样的数据时，持卡人数据存储到本地硬盘驱动器和可移动电子介质。	为了确保所有人员都意识到自己的责任不要保存或复制持卡人的数据到其本地个人电脑或其他媒体，你的政策应该明确禁止除已明确授权这样做人员这样的活动。存储或复制持卡人的数据到本地硬盘或其他介质必须符合所有适用的PCI DSS要求。
	12.3.10.b 对于经过适当授权的人员，确认使用政策要求持卡人数据的保护，按照PCI DSS要求。	
12.4 确保安全政策和程序明确定义了所有人员的信息安全责任。	**12.4.a** 确认信息安全政策明确界定的所有人员的信息安全责任。	如果没有明确定义的安全角色和职责分配，有可能是与安全组不一致的相互作用，从而导致不安全的实现技术或使用过时的或不安全的技术。
	12.4.b 面试责任人员的样本，以验证他们了解安全策略。	
12.4.1 ***只有服务提供商附加要求：*** **执行管理层应建立持卡人**数据的保护和一个PCI DSS合规计划，包括责任： • 维护PCI DSS合规性总体问责 • 定义包机的PCI DSS合规程序和通信执行管理	**12.4.1.a** 检查文档，以确认高级管理层已指派的总体责任维护实体的PCI DSS合规性。	***注意：此要求仅适用于被评估的实体是服务提供商。*** 的PCI DSS合规责任执行管理任务，确保长官级可视性PCI DSS合规计划，并允许有机会提出适当的问题，以确定该计划的有效性和影响力的战略重点。对于PCI DSS合规计划的总负责，可以分配给各个角色和/或组织内的业务单位。执行管理可以包括C级位置，董事会，或等同物。具体的标题将取决于特定的组织结构。细节提供给执行管理水平应适合于特定组织与目标受众。
	12.4.1.b 检查公司的PCI DSS包机，以验证它概括了其PCI DSS合规计划的组织和传递到执行管理的条件。	

PCI DSS要求	测试程序	指导
12.5 分配给个人或小组执行下列信息安全管理责任：	**12.5** 检查信息安全政策和程序来验证： • 信息安全的正式分配给首席安全官或管理的其它安全知识的成员。 • 下面的信息安全责任明确并正式分配：	每个人或团队与信息安全管理责任，应该清楚地知道自己的职责和相关的任务，通过具体的政策。如果没有这种问责制，在工艺的差距可能会打开访问到关键资源或持卡人数据。实体也应该考虑转变和/或继任计划的关键人员，以避免安全作业潜在的差距，这可能导致不分配，因此没有履行职责。
12.5.1 建立，记录和分发安全策略和程序。	**12.5.1** 验证建立，记录和分发安全策略和程序正式分配的责任。	
12.5.2 监控和分析安全警报和信息，并分发到合适的人员。	**12.5.2** 验证监测和分析安全警报，并正式入驻分发信息，以适当的信息安全和业务部门管理人员的责任。	
12.5.3 建立，记录和分发安全事件响应和升级程序，以确保所有情况下及时和有效的处理。	**12.5.3** 验证建立，记录和分发安全事件响应和升级程序被正式分配的责任。	
12.5.4 管理用户账户，包括添加，删除和修改。	**12.5.4** 验证管理（添加，删除和修改）的用户帐户和认证管理正式分配的责任。	
12.5.5 监视和控制所有的数据访问。	**12.5.5** 验证用于监测和控制所有对数据的访问正式入驻这一责任。	
12.6 实施正式的安全意识计划，使所有相关人员知道持卡人的数据安全策略和程序。	**12.6.a** 查看安全意识计划，以验证它提供意识有关持卡人数据安全策略和程序的所有人员。	如果人员不接受关于他们的安全责任，安全保障和已经实施的有可能成为通过错误或故意行为无效程序。
	12.6.b 检查安全意识计划的程序和文件，并执行以下操作：	

PCI DSS要求	测试程序	指导
12.6.1 教育人员在租赁和至少每年一次。 ***注意：*** *方法可以根据人员的角色和他们的访问持卡人数据的水平而变化。*	**12.6.1.a** 确认安全意识计划提供沟通的意识和教育人员（例如，海报，信函，备忘录，基于网络的培训，会议和促销）的多种方法。	如果安全意识计划不包括定期进修课程，关键的安全流程和程序可以被遗忘或忽略，导致暴露的关键资源和持卡人数据。
	12.6.1.b 验证人员参加在雇用和至少每年一次安全意识培训。	
	12.6.1.c 面试人员的样本，以验证他们已经完成了意识培训，并了解持卡人数据安全的重要性。	
12.6.2 要求工作人员每年至少他们已经阅读并理解安全策略和程序的承认。	**12.6.2** 确认安全意识计划要求的人员承认，以书面或电子方式，每年至少一次，他们已阅读并理解信息安全策略。	需要通过人员的书面确认或电子有助于确保他们已阅读并理解安全政策/程序，他们已经并将继续为遵守这些政策的承诺。
12.7 筛选潜在的人员聘用前，以尽量减少来自内部人士透露攻击的风险。（背景调查的例子包括以前的工作经历，犯罪记录，信用记录，并参考检查。） ***注意：*** *对于要聘请这些潜在的人才，为某些职务，如商店收银员在时间上进行交易时，谁只能访问一个卡号，这个要求仅仅是一个建议。*	**12.7** 与人力资源管理部门查询，并验证背景调查进行到聘请谁可以访问持卡人数据或持卡人数据环境中潜在的人员之前（的地方性法规的限制范围内）。	招聘预计将获准进入持卡人数据的潜在谁人员之前进行全面的背景调查使与可疑或犯罪背景的人擅自使用的PAN和其他持卡人数据的风险。
12.8 维护和实施的政策和程序来管理与谁持卡人数据的共享服务提供商，或可能影响持卡人数据的安全性，如下所示：	**12.8** 通过观察，政策和程序，以及支持文件审查，审查确认流程实现管理与谁持卡人数据的共享服务提供商，或可能影响持卡人数据的安全性，如下所示：	如果与服务供应商商户或服务提供商共享持卡人数据，有一定的要求适用于确保该数据的持续保护将通过这样的服务提供商来执行。 不同类型的服务提供商的一些例子包括备份的磁带存储设备，管理服务供应商，如Web托管公司或安全服务提供商，实体收到欺诈建模的目的等数据

PCI DSS要求	测试程序	指导
12.8.1 维护服务提供商，其中包括所提供的服务的描述的列表。	**12.8.1** 验证服务提供商的列表被维持，并且包括所提供的服务的描述。	保持所有服务提供商的轨道识别其中潜在的风险延伸到组织之外。
12.8.2 保持一个书面协议包括确认该服务商负责对持卡人数据的安全服务提供商拥有或以其他方式存储，处理或代表客户的传输，或者在某种程度上，它们可能会影响客户的安全持卡人数据环境。 ***注意：*** *确认将取决于双方之间的协议的确切措辞，所提供的服务的细节，并分配给每一方的责任。在确认没有包括在此要求提供的确切措辞。*	**12.8.2** 遵守书面协议，并确认它们包括服务提供商，他们负责持卡人数据的安全服务提供商拥有或以其他方式存储，处理或传输代表客户的，或在某种程度上，他们可能会影响安全性的确认客户的持卡人数据环境。	服务供应商的确认能证明其维护持卡人数据的适当的安全性，它从客户获得的承诺。在多大程度上服务提供商负责持卡人数据的安全性将取决于特定服务和供应商，并评估实体之间的协议。 在与要求12.9结合，这一要求的目的是促进他们适用的PCI DSS的责任方之间的谅解一致的水平。例如，该协议可以包括适用PCI DSS要求保持为所提供的服务的一部分。
12.8.3 确保有用于接合服务提供商包括接合之前适当的尽职调查已建立的过程。	**12.8.3** 验证政策和程序记录并实施包括让任何服务提供商之前，适当的尽职调查。	该过程确保了服务提供商的任何啮合彻底的组织，其中应包括之前建立与服务供应商的正式关系的风险分析，内部审核。具体的尽职调查流程和目标会为每个组织变化。考虑的例子可能包括供应商的报告的做法，违反通知和事件响应程序，PCI DSS的责任是如何的每一方，供应商如何验证自己的PCI DSS合规性，他们会提供什么样的证据，等等之间的分配细节

PCI DSS要求	测试程序	指导
12.8.4 维护程序每年至少监测服务提供商的PCI DSS合规性状态。	**12.8.4** 验证实体维护计划每年至少监督其服务提供商的PCI DSS合规性状态。	了解你的服务提供商的PCI DSS合规性状态提供有关它们是否符合您的组织受到同样的要求保证和意识。如果服务提供商提供的各种服务，这个要求应该适用于交付给客户的服务，并且这些服务范围为客户的PCI DSS评估。一个实体维护的具体信息将取决于与他们的供应商，特定协议，服务类型等。这样做的目的是评估的实体理解哪些PCI DSS要求它们的供应商已经同意会面。
12.8.5 哪些PCI DSS要求由各个服务提供商管理，以及维护信息由实体管理。	**12.8.5** 验证实体保存有关PCI DSS要求由各个服务提供商管理，并且由实体来管理信息。	
12.9 ***只有服务提供商附加要求：*** 服务供应商以书面形式确认到，他们有责任为服务提供商拥有持卡人数据或以其他方式存储，处理的安全性的客户，或代客户发送，或者在某种程度上，它们可能会影响客户的持卡人数据的安全性环境。 ***注意：*** *确认将取决于双方之间的协议的确切措辞，所提供的服务的细节，并分配给每一方的责任。在确认没有包括在此要求提供的确切措辞。*	**12.9** ***只有服务供应商的评估进一步的测试过程：*** 评论服务提供商的政策和程序，并遵守用于书面协议模板，以确认服务供应商以书面形式承认对客户的服务供应商将保持所有适用的PCI DSS要求服务提供商拥有或以其他方式存储，处理的范围内，或传输持卡人代表客户的，或者他们可能会影响客户的持卡人数据环境的安全程度的数据。	***注意：*** *此要求仅适用于被评估的实体是服务提供商。* 在与要求12.8.2结合，这个要求是为了促进服务提供商和他们对自己适用的PCI DSS责任客户之间的理解一致的水平。服务供应商的确认能证明其维护持卡人数据的适当的安全性，它从客户获得的承诺。用于书面协议的服务提供商的内部政策和与他们的客户互动过程的程序和任何模板应当包括适用的PCI DSS确认为他们的客户。由服务提供商提供书面确认的方法应该提供者和客户之间的约定。

PCI DSS要求	测试程序	指导
12.10 实施事件响应计划。准备立即响应系统漏洞。	**12.10 检查事件响应计划和相关程序来验证实体准备通过执行以下立即响应系统漏洞：**	如果没有正确地传播，阅读，并理解由当事人负责，混乱，缺乏统一的反应可能会给企业进一步宕机，不必要的公共媒体曝光，以及新的法律责任进行彻底安全事故应急预案。
12.10.1 创建事件响应计划，以在系统破坏的情况下实现。确保规划提出以下，至少包括： • 角色，责任和在包括支付品牌的通知妥协的情况下的沟通和联系的战略，至少 • 具体的事件响应程序 • 业务恢复和连续性程序 • 数据备份流程 • 对于报告妥协的法律要求分析 • 覆盖所有关键系统组件的响应 • 参考或列入从支付品牌的事故响应程序。	**12.10.1.a 验证事件响应计划包括：** • 角色，职责和沟通策略中包括的支付品牌的通知妥协的情况下，至少 • 具体的事件响应程序 • 业务恢复和连续性程序 • 数据备份流程 • 对于报告妥协的法律要求分析（例如，加利福尼亚州比尔1386，这需要在他们的数据库中的实际或怀疑的妥协与加州居民任何业务的情况下，受影响的用户的通知） • 覆盖和响应所有关键系统组件 • 参考或列入从支付品牌的事故响应程序。 **12.10.1.b我 nterview人员和从先前报告的事件或警报的抽样审查文件，以验证记录事故应急预案和程序如下。**	事件响应计划应是全面的，包含所有的关键元素，让你的公司在违约可能影响持卡人数据的情况下，有效的反应。
12.10.2 检查和测试计划，其中包括要求上市12.10.1所有元素，至少每年一次。	**12.10.2我 从测试nterview人员和审查文档，以验证该计划至少每年进行测试，而测试包括要求上市12.10.1所有元素。**	如果没有适当的测试，关键的步骤可能会错过，这可能导致在事故发生时增加曝光量。

PCI DSS要求	测试程序	指导
12.10.3 指定特定的人员提供24/7的基础上，以响应警报。	**12.10.3** 通过观察，政策审查，并负责人员的采访时表示，指定的人员可为24/7事件响应和监控覆盖未经授权的活动，未授权的检测无线接入点，关键IDS警报的证据确认，和/或报告未经授权的关键系统或内容文件的变化。	没有受过训练的和容易获得的事件响应团队，可能发生在网络扩展的伤害，关键数据和系统可以通过有针对性的系统的处理不当成为“污染”。这会妨碍事故后调查的成功。
12.10.4 提供适当的培训与安全漏洞响应责任人员。	**12.10.4** 通过观察确认，政策审查，并负责人员与安全事件响应职责，工作人员定期培训的采访。	
12.10.5 包括安防监控系统发出警报，包括但不限于入侵检测，入侵防护，防火墙，和文件完整性监控系统。	**12.10.5** 通过观察和监视和响应来自安全监控系统警报涵盖了事件响应计划过程审核验证。	这些监控系统的设计专注于潜在危险的数据，在采取快速行动，以防止破坏至关重要，必须包含在事件响应过程。
12.10.6 制定过程中修改，并根据教训进化事件响应计划，并纳入行业发展。	**12.10.6** 通过观察，政策审查，并负责人员的面谈确认是否有修改和发展，根据经验的事件响应计划过程中了解到，并纳入行业发展。	结合“经验教训”到事件响应计划的事件发生后，有助于保持当前的计划，并能够对新出现的威胁和安全趋势做出反应。
12.11 ***只有服务提供商附加要求：*** **执行审查至少每季度进行确**认的人员以下的安全政策和操作程序。评论必须包括以下过程： • 每天的日志评论 • 防火墙规则集评论 • 配置应用标准，以新系统 • 响应安全警报 • 变更管理流程	**12.11.a 检查政策和程序，以验证工艺审查和确认的人员以下的安全政策和操作程序，以及评论盖定义：** • 每天的日志评论 • 防火墙规则集评论 • 配置应用标准，以新系统 • 响应安全警报 • 变更管理流程	***注意：此要求仅适用于被评估的实体是服务提供商。*** 定期确认安全政策和程序遵循提供保证预期的控制是积极的和预期的工作。这些审查的目的是不是要重新执行其它PCI DSS的要求，但要确认是否被遵循的程序符合市场预期。
	12.11.b 面试责任人员，并检查审查的记录，验证评审至少每季度进行。	

PCI DSS要求	测试程序	指导
12.11.1 ***只有服务提供商附加要求：*** **保持每季审查程序的**文档，包括： • 记录的审查结果 • 审查和分配责任的PCI DSS合规计划的人员注销结果	**12.11.1** 检查从季度审查文档，以确认它们包括： • 记录的审查结果 • 审查和分配责任的PCI DSS合规计划的人员注销结果	***注意：此要求仅适用于被评估的实体是服务提供商。*** 这些独立检查的目的是确认是否安全的活动正在持续的基础上进行的。这些评论也可以用于验证适当的证据正在维护，例如，审计日志，漏洞扫描报告，防火墙评论等，以帮助实体的下届PCI DSS评估的准备。

附录A：其他PCI DSS要求

本附录包含不同类型的实体的额外PCI DSS要求。本附录中的部分包括：

- 附录A1： 对于共享主机提供商附加PCI DSS要求
- 附录A2： 使用SSL / TLS的早期用于实卡POS POI终端连接用于实体额外PCI DSS要求
- 附录A3： 指定的单位补充验证

指导和适用性信息每个部分内。

附录A1：对共享主机提供商其他PCI DSS要求

如要求12.8和12.9引用，以访问持卡人数据（包括共享主机提供商）所有的服务提供商必须遵守PCI DSS。此外，要求2.6指出共享主机提供商必须保护每个实体的托管环境和数据。因此，共享主机提供商另外还必须遵守本附录的要求。

A1的要求	测试程序	指导
A1 保护每个实体（即商户，服务提供商或其他实体）托管环境和数据，每A1.1 A1.4通过： 一个托管服务提供商必须满足这些要求以及PCI DSS的所有其他相关章节。 ***注意：** 即使一个托管服务提供商可满足这些要求，该实体的使用托管服务提供商的合规性无法得到保证。每个实体必须遵守PCI DSS并验证其是否遵守适用的。*	**A1** 特别是对于共享托管服务提供商的PCI DSS评估，以确认共享托管提供商保护实体（商家和服务提供商）的托管环境和数据，跨越的代表性样本选择服务器（Microsoft Windows和Unix / Linux操作系统）的一个样本托管商户和服务提供商，并通过以下A1.4执行A1.1：	*附录A* 的PCI DSS适用于谁愿意提供他们的商户和/或服务提供商客户提供符合PCI DSS的托管环境的共享托管服务提供商。
A1.1 确保每个实体只运行访问该实体的持卡人数据环境的过程。	**A1.1** 如果共享主机提供商允许实体（例如，商家或服务提供商）运行自己的应用程序，验证使用实体的唯一ID运行这些应用程序。例如： • 在系统上没有实体可以使用共享网络服务器的用户ID。 • 由实体使用的所有CGI脚本必须创建并运行作为实体的唯一用户ID。	如果商家或服务提供者被允许在共享服务器上运行自己的应用程序，这些应与商户或服务提供商的用户ID运行，而不是作为特权用户。

A1的要求	测试程序	指导
A1.2 限制 每个实体的访问和特权只有自己的持卡人数据环境。	**A1.2.a 验证任何应用进程的用户ID不是特权用户（根/管理员）。**	为了确保访问和权限进行了限制，即每个商户或服务提供商只向自己的环境准入，考虑以下因素： 1.商户或服务提供商的Web服务器的用户ID的权限; 2.权限授予读，写和执行文件; 3.权限授予写入系统二进制文件; 4.权限授予商户和服务提供商的日志文件; 和 5.控制，以确保一个商户或服务提供商不能独占系统资源。
	A1.2.b 验证每个实体（商户，服务提供商）有读，写，或者只对文件，它拥有目录或必要的系统文件（通过文件系统权限，访问控制列表，chroot环境，jailshell等限制）执行权限 **重要： 实体的文件可能不按组共享。**	
	A1.2.c 验证一个实体的用户不必共享系统二进制文件的写权限。	
	A1.2.d 验证日志条目不能观看仅限于拥有实体。	
	A1.2.e 为了确保每个实体不能独占服务器资源利用的漏洞（例如，错误的比赛，并重新启动造成的条件，例如缓冲区溢出），验证限制都将在使用这些系统资源： • 磁盘空间 • 带宽 • 记忆 • 中央处理器	
A1.3 确保日志和审计跟踪启用和独特的每个实体的持卡人数据环境，并符合PCI DSS要求 10。	**A1.3 验证共享的托管服务提供商已经启用了日志记录如下，供每个销售商和服务供**应商环境： • 日志对于常见的第三方应用程序启用。 • 日志默认活跃。 • 日志可用于由所拥有的实体审查。 • 登录位置清晰地传达给所属单位。	日志应该在共享宿主环境使商家和服务提供商可以访问，并可以查看可用的，记录具体到他们的持卡人数据环境。
A1.4 进程可以提供在妥协于任何托管商户或服务提供商的情况下，及时取证调查。	**A1.4 验证共享的托管服务提供商写，提供的一种妥协的情况下，相关服务器的及时取**证调查的政策。	共享主机提供商必须有流程，以提供所需要的妥协取证调查事件快速和容易响应，下至具体的适当水平，使个体商户或服务提供商的详细信息是可用的。

附录A2：使用SSL / TLS早期的实卡POS POI终端连接实体其他PCI DSS要求

使用SSL和TLS早期用于POS终端的POI实体的连接必须朝向尽快升级到一个强密码协议工作。此外，SSL和/或TLS早期不能被引入，其中这些协议已经不存在的环境。本标准出版时，已知的漏洞很难在POS POI支付终端利用。然而，新的漏洞可能出现在任何时候，它是由组织来保持最新与脆弱性趋势，并确定它们是否是易受任何已知漏洞。直接受影响的PCI DSS要求是：

2.2.3要求	实施额外的安全功能对于任何需要的服务，协议，或者被认为是不安全的守护进程。
2.3要求	加密使用强大的加密所有非控制台管理访问。
4.1要求	使用强大的加密和安全协议传输在开放的公共网络中，以保护敏感的持卡人数据。

SSL和TLS早期不能用作安全控制，以满足这些要求，除非在如本附录中详述POS终端POI连接的情况下。为了支持工作从SSL / TLS早期迁移走在POS终端POI实体，以下规定包括：

- 新的POS终端POI实现必须不能使用SSL或TLS早在安全控制。
- 所有POS终端POI服务供应商必须提供安全的服务产品。
- 服务供应商支持使用SSL和/或TLS早现有的POS终端POI的实现必须建立一个正式的风险缓解和迁移计划。
- **POS终端POI在卡存在的环境，可以被验证为不易感于SSL和TLS早期任何已知漏洞， 而SSL / TLS终结点，它们所连接， 可以继续使用SSL / TLS初作为安全控制。**

本附录仅适用于使用SSL / TLS初作为安全控制，以保护POS终端POI，包括服务供应商提供谁进入连接POS终端POI实体。

A2要求	测试程序	指导
A2.1 其中POS终端POI（在商家或支付接受位置）使用SSL和/或TLS早期，该实体必须确认设备不易于对那些协议的任何已知漏洞。 ***注意：*** *这个要求是旨在适用于该实体与所述POS终端的POI，例如商家。这一要求不适用于服务提供商谁充当终端或连接点的POS终端POI。要求A2.2和A2.3适用于POS POI服务提供商。*	**A2.1** *对于使用SSL和/或TLS早期POS POI终端，* 确认实体具有用于验证的设备不易于用于SSL / TLS早期任何已知漏洞的文档（例如，供应商的文档，系统/网络配置的详细信息，等等）。	在卡本环境中使用的POS终端的POI可以继续使用SSL / TLS初时可以示出认为POS终端POI不易目前已知的漏洞。 然而，SSL是一种过时的技术，可能会受到在今后进行更多的安全漏洞; 因此，强烈建议POS终端POI被尽快升级到一个安全的协议。如果环境中不需要SSL / TLS初期，使用和回退到这些版本应该被禁用。指当前PCI SSC信息补充在SSL / TLS早期为进一步指导。 ***注意：*** *对于POS终端POI目前不容易受到攻击的补贴是基于目前，已知风险。如果引入了新的漏洞，其POS终端POI容易，在POS终端POI需要立即更新。*

A2要求	测试程序	指导
A2.2 *要求服务提供商，只有：* 与现有的连接点在A2.1称POS终端POI使用SSL和/或TLS早期所有服务供应商必须制定正式的风险缓解和迁移计划。	**A2.2** 查看记录的风险缓解和迁移计划，以验证它包括： • 用法的描述，包括正在发送哪些数据，类型和使用和/或系统数量支持SSL / TLS的早期，类型环境; • 风险评估结果和降低风险的控制措施; • 的过程监视与SSL / TLS早相关新漏洞描述; • 被执行，以确保SSL / TLS早期未执行到新环境的变更控制流程的说明; • 移民项目计划的概述，以在未来某一日期取代SSL / TLS初。	POS POI终止点，包括但不限于服务提供商，如收单方或单方处理器，可以继续使用SSL /早期TLS时可以示出它的是，服务提供者在地方，减轻支持用于这些连接的风险控制服务提供商环境。风险缓解和迁移计划是，详细的计划迁移到一个安全协议，并且还介绍了在地方，以减少与SSL / TLS早期的风险，直到迁移完成控制实体拥有的实体准备的文件。服务提供者应传达给使用SSL / TLS早期关于其使用相关的风险所有客户需要迁移到一个安全的协议。
A2.3 *要求服务提供商，只有：* 所有服务供应商必须提供安全的服务产品。	**A2.3** 检查系统配置和支持文档验证服务供应商提供他们的服务安全协议选项。	服务提供商配套POS终端POI SSL / TLS早期连接也应该提供一个安全的协议选项。指当前PCI SSC信息补充在SSL / TLS早期为进一步指导。

附录A3：指定的单位补充验证（DESV）

本附录仅适用于由支付品牌（S）或作为收购方需要对现有的PCI DSS要求额外的验证指定的单位。实体的例子，这个附录 *可以* 适用于包括：

- 那些存储，处理和/或传送大量持卡人数据，
- 那些持卡人数据提供聚集点，或
- 那些遭受显著或屡次违反持卡人数据。

这些补充验证步骤是为了提供更大的保证，即PCI DSS控制是通过业务照常（BAU）过程的验证有效，在连续基础上保持，并且增加了验证和范围界定的考虑。本文档中的额外的验证步骤分为以下控制区：

***A3.1** 实现PCI DSS合规计划。*

***A3.2** 文件和验证PCI DSS范围。*

***A3.3** 验证PCI DSS被纳入业务照常（BAU）的活动。*

***A3.4** 控制和管理对持卡人数据环境的逻辑访问。*

***A3.5** 识别和可疑事件作出回应。*

***注意：** 一些要求定义的时间表（例如，至少每季度或每半年）将被执行在其内的某些活动。对于初步评估，而这个文件，它不要求的活动已经为每一个这样的时间表在过去的一年被执行，如果评估验证：*

1）的活性按照最近的时间范围内（也就是，最近的四分之一或六个月期间）适用的要求进行的，和

2）实体具有记录的政策和程序继续到所定义的时间范围内执行的活动。对于初始评估后随后的几年中，必须已经为它要求（例如，必须已经为每个前一年的四个季度进行季度性）每个时间内进行的活动。

***注意：** 实体必须根据本附录接受评估 只有当指示由收单机构或支付品牌这样做。*

A3要求	测试程序	指导
A3.1实现一个PCI DSS合规计划		
A3.1.1 执行管理层应建立持卡人数据的保护和一个PCI DSS合规计划，包括责任： • 维护PCI DSS合规性总体问责 • 定义包机的PCI DSS合规计划 • 提供了对PCI DSS合规举措和问题，包括整治活动的最新执行管理层和董事会，每年至少一次 ***PCI DSS参考：要求12***	**A3.1.1.a 检查文档，以确认高级管理层已指派的总体责任维护实体的PCI DSS合规性。** **A3.1.1.b 检查公司的PCI DSS包机，以验证它概括了其PCI DSS合规计划的组织的条件。** **A3.1.1.c 检查的董事会会议纪要和/或演示执行管理层和董事会，以确保PCI DSS合规计划和整治活动至少每年沟通。**	的PCI DSS合规责任执行管理任务，确保长官级可视性PCI DSS合规计划，并允许有机会提出适当的问题，以确定该计划的有效性和影响力的战略重点。对于PCI DSS合规计划的总负责，可以分配给各个角色和/或组织内的业务单位。
A3.1.2 正式的PCI DSS合规程序必须到位，包括： • 维护和监视整个PCI DSS合规性，包括业务照常活动的活动定义 • 年度PCI DSS评估过程 • 过程为PCI DSS要求的不断验证（例如：每天，每周，每季度等作为适用每要求） • 一种用于执行业务影响分析过程，以确定战略业务决策的潜在PCI DSS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，以验证工艺专为以下定义：** • 维护和监控整个PCI DSS合规性，包括业务照常活动 • 年度PCI DSS评估（S） • 的PCI DSS要求的不断验证 • 业务影响分析，以确定战略业务决策的潜在PCI DSS影响	一个正式的合规计划使企业能够监控其安全控制的健康，是在将控制失败的情况下主动，有效地在整个组织交流活动，合规性状态。在PCI DSS合规程序可以是一个涵盖范围广泛的合规性和/或管理程序的专用程序或部分，并应包括一个明确的方法，演示了一致和有效的评价。实例的方法包括：计划 - 执行 - 检查 - 行动（PDCA）的戴明循环，ISO 27001，COBIT，DMAIC和六西格玛。 *（接下页）*

A3要求	测试程序	指导
	A3.1.2.b 面试人员和观察达标活动，以验证定义的过程以下实现的： • 维护和监控整个PCI DSS合规性，包括业务照常活动 • 年度PCI DSS评估（S） • 的PCI DSS要求的不断验证 • 业务影响分析，以确定战略业务决策的潜在PCI DSS影响	维护和监控一个组织的总体PCI DSS合规包括识别活动，每天执行，每周，每月，每季或每年，并确保被相应地进行这些活动（例如，使用安全自我评估或PDCA方法）。应该针对潜在PCI DSS的影响进行分析的战略业务决策实例可以包括兼并和收购，新技术的采购，或者新的费付款，承兑渠道。
A3.1.3 PCI DSS合规性角色和责任必须明确界定，并正式分配给一个或更多的人员，至少包括以下内容： • 管理PCI DSS业务照常活动 • 每年的管理PCI DSS评估 • 管理连续的验证PCI DSS要求（例如：每天，每周，每季度等作为适用每要求） • 管理业务影响分析，以确定战略业务决策的潜在PCI DSS影响 ***PCI DSS参考：要求12***	**A3.1.3.a 检查信息安全政策和程序，面试人员核实的角色和责任都有明**确的规定和职责分配给至少包括以下内容： • 管理PCI DSS业务照常活动 • 每年的管理PCI DSS评估 • 管理连续的验证PCI DSS要求（例如：每天，每周，每季度等作为适用每要求） • 管理业务影响分析，以确定战略业务决策的潜在PCI DSS影响	具体PCI DSS合规性的角色和职责的正式定义有助于确保问责和持续的PCI DSS合规工作的监督。这些角色可以被分配到一个单一的所有者或多个所有者的不同方面。所有权应分配给个体能够基于风险 - 决策权，并在其中的责任在于为特定的功能。职责应正式定义和业主应该能够证明自己的责任和义务的理解。
	A3.1.3.b 面试责任人员，并确认他们熟悉并执行其指定的PCI DSS合规责任。	

A3要求	测试程序	指导
A3.1.4 每年至少提供了最新的PCI DSS和/或信息安全培训与PCI DSS合规责任人员（如在A3.1.3标识）。 ***PCI DSS参考：*** *要求12*	**A3.1.4.a** 检查信息安全政策和程序，以验证PCI DSS和/或信息安全培训至少需要每年进行PCI DSS合规责任的每个角色。 **A3.1.4.b** 面试人员检查出勤或其他记录的证书，以确认符合PCI DSS合规责任人员每年至少接受了最新的PCI DSS和/或类似的信息安全培训。	负责PCI DSS合规人员有具体的培训需求超过了通常由一般的安全意识培训提供。与PCI DSS合规责任人应接受专门的培训，除了对信息安全的总体认识，着眼于特定的安全议题，技能，过程或方法所必须遵循的那些个人有效履行合规责任。培训可以由第三方来提供方，例如，SANS或PCI SSC（PCI意识，PCIP和ISA），支付品牌，以及acquirers-或培训可能是内部的。培训内容应该是适用于特定的工作职能，并成为当前包括PCI DSS的最新安全威胁和/或版本。 ***最佳实践实现一个安全意识计划。***

A3要求	测试程序	指导
A3.2文献和验证PCI DSS范围		
A3.2.1 文件并确认的PCI DSS范围的准确性至少每季度以及在该调查范围内的环境显著的变化。至少，每季作用域验证应包括： • 确定所有调查范围内的网络和系统组件 • 识别用于网络被淘汰的范围，包括实现的所有分割控制的说明所有外的范围的网络和理由 • 确定所有连接的实体 - 例如，第三方实体访问持卡人数据环境（CDE） ***PCI DSS参考：PCI DSS要求的范围***	**A3.2.1.a 检查的范围审查和面试人员核实，审查执行记录的结果**： • 至少每季度一次 • **在调查范围内的环境显著变化后** **A3.2.1.b 每季度检查范围的记录结果审查核实之后执行**： • 所有调查范围内的网络和系统部件的鉴定 • 外的范围内的所有网络的识别和理由网络被淘汰的范围，包括实现的所有分割控制的说明 • 所有连接的实体 - 例如，第三方实体的身份与访问CDE	的PCI DSS范围确认应尽可能频繁地进行尽可能确保PCI DSS范围保持最新且不断变化的业务目标保持一致。
A3.2.2 确定所有变更系统或网络，包括新的系统和新的网络连接添加PCI DSS范围的影响。过程必须包括： • 执行一个正式的PCI DSS评 • 确定适用的PCI DSS要求，系统或网络 • 更新PCI DSS范围适当 • 负责人事的影响评估结果的文件签核（如A3.1.3定义） ***PCI DSS参考：PCI DSS要求的范围; 要求1-12***	**A3.2.2 检查 改变文件和面试人员核实，对于每次更改系统或网络**： • 进行了正式的PCI DSS影响评估。 • 对系统或网络的变化适用PCI DSS要求进行鉴定。 • PCI DSS范围进行了更新以适合变化。 • 签退由负责人员（如在A3.1.3定义）获得和记录。	更改系统或网络可以有PCI DSS范围显著的影响。例如，防火墙规则的变化能带动整个网络段成范围，或新的系统可以被添加到CDE必须被适当地保护。处理，以确定应当知道，在系统和网络可以具有对一个实体的PCI DSS范围可以作为专用的PCI DSS合规性项目的一部分来执行，或一个实体的过拱顺应性和/或治方案下可以落入的潜在影响。

A3要求	测试程序	指导
A3.2.2.1 一旦改变完成，所有相关 PCI DSS要求，必须对所有新的或更改系统和网络来验证和文档必须更新适用。那应验证包括但不限于PCI DSS要求的例子： • 网络图被更新，以反映更改。 • 系统是每个配置的标准配置，所有的默认口令更改和不必要的服务禁用。 • 系统保护与所需的控制，例如，文件完整性监控（FIM），防病毒，补丁，审计日志记录。 • 验证敏感认证数据（SAD）不被存储，并且所有持卡人数据（CHD）存储记录并掺入DATA-保留策略和程序 • 新系统包括在季度漏洞扫描过程。 ***PCI DSS参考：** PCI DSS要求的范围; 要求1-12*	**A3.2.2.1 对于系统和网络变化的样品，检查变更记录，采访人员和观察受**影响系统/网络，以验证适用PCI DSS要求得到落实，文档更新变化的一部分。	有过程来分析，以确保所有的适当的PCI DSS控制被施加到加入到在范围内环境中的任何系统或网络由于改变的所有变化是很重要的。建立此验证到变更管理流程帮助确保设备库存和配置标准的不断更新和安全控制应用需要的地方。变更管理流程应包括配套的证据表明，PCI DSS要求实施或通过迭代过程保存下来。

A3要求	测试程序	指导
A3.2.3 改变组织结构 - 例如公司合并或收购，改变或在冲击到PCI DSS范围和控制应用的正式（内部）审查安全控制，结果责任人员的重新分配。 ***PCI DSS参考：要求12***	**A3.2.3 检查政策和程序来验证的变化在影响到PCI DSS范围和控制应用正**式审查组织结构的结果。	一个组织的结构和管理定义了高效，安全运行的要求和协议。改变这种结构可以有通过重新分配或移除，一旦支持PCI DSS控制或继承，可能不到位建立控制新职责的资源，以现有的控件和框架的负面影响。因此，如果有改变，以确保控制措施和积极的，重要的是重新审视PCI DSS范围和控制。
A3.2.4 如果使用了分割，确认PCI DSS范围由上分割控制进行渗透测试，至少每6个月进行任何更改后分割控制/方法。 ***PCI DSS参考：要求11***	**A3.2.4 检查从最近的渗透测试，以验证结果**： • 进行渗透测试，以验证分段控制至少每6个月进行任何更改后分割控制/方法。 • 渗透测试涵盖了所有在用分段控制/方法。 • 渗透测试验证分割控制/方法的操作和有效的，并且从在CDE系统隔离所有外的范围的系统。	如果分割用于在范围内的网络从外的范围网络隔离，这些分割控制必须使用渗透测试，以确认他们继续按计划和有效地操作进行验证。Penetration-测试技术应该遵循现有的渗透方法，如PCI DSS要求11有关的有效渗透测试的更多信息规定，是指在PCI SSC的信息补上 ***渗透测试指南。***

A3要求	测试程序	指导
A3.2.5 实现数据发现的方法来确认PCI DSS范围和定位所有源和明文PAN的位置至少每季度以及在持卡人环境或流程显著的变化。 数据发现方法必须考虑到对明文PAN的潜力，驻留在当前定义的CDE的外部系统和网络。 ***PCI DSS参考：*** *PCI DSS要求的范围*	**A3.2.5.a 检查记载的数据发现的方法来验证以下内容**： • 数据发现方法包括用于识别所有源和明文PAN的位置的过程。 • 方法考虑到了潜在的明文PAN驻留在当前定义的CDE的外部系统和网络。 **A3.2.5.b 最近数据发现工作检查结果，并采访负责人员，以验证数据发现**，至少进行季度和在持卡人环境或流程显著的变化。	PCI DSS要求，作为范围界定工作的一部分，评估机构必须识别并记录在他们的环境中的所有明文PAN的存在。实现识别所有来源和明文PAN的位置，并考虑到了潜在的明文PAN驻留在当前定义的CDE的外部或内部的定义意想不到的地方系统和网络数据 - 一个方法论的发现CDE-例如，在错误日志文件或内存转储文件 - 有助于确保检测明文PAN的以前未知的地点和适当的保护。可以通过各种方法来执行的数据发现过程，包括但不限于：（1）可商购的数据发现软件，（2）的内部开发的数据发现程序，或（3）一个手动搜索。无论使用何种方法的，
A3.2.5.1 确保用于数据发现方法的有效性 - 例如，方法必须能够发现在所有类型的系统组件的明文PAN（例如，每个操作系统或平台），并在使用的文件格式。数据发现方法的有效性，必须至少每年予以确认。 ***PCI DSS参考：*** *PCI DSS要求的范围*	**A3.2.5.1.a 面试人员和审查文档，以确认**： • 该实体具有到位以测试用于数据发现方法的效力的方法。 • 该过程包括验证方法能够发现在所有类型的系统组件和文件格式中使用明文PAN。 **A3.2.5.1.b 检查的有效性最近测试的结果来验证的用于数据发现方法的**有效性至少每年予以确认。	的方法来测试的用于数据发现方法的效力可确保完整性和持卡人数据检测的准确度。为了完整性，至少一个在两个系统部件的采样中，范围和外的范围网络应被包括在数据发现过程。精度可通过放置在系统部件和文件格式的使用中的样品测试的PAN，并确认数据 - 发现方法检测的测试的PAN进行测试。

A3要求	测试程序	指导
A3.2.5.2 于CDE包括外面的检测明文PAN的要启动实施应急程序： • 程序确定，要怎么做，如果明文PAN是CDE以外发现的，包括它的检索，安全缺失和/或迁移到当前定义CDE适用 • 确定如何将数据程序结束了CDE的外部 • 程序补救数据泄漏或处理间隙，导致数据作为CDE的外部 • 程序用于识别数据的源 • 程序识别任何轨道数据是否存储与所述的PAN	**A3.2.5.2.a 检查文档化反应步骤，以检验用于响应于检测到明文PAN的CDE的外部程序的定义，并包括：** • 程序确定，要怎么做，如果clear-文本PAN是CDE以外发现的，包括它的检索，安全缺失和/或迁移到当前定义CDE适用 • 确定如何将数据程序结束了CDE外 • 程序补救数据泄漏或处理间隙，导致数据作为CDE的外部 • 程序用于识别数据的源 • 程序识别任何轨道数据是否存储与所述的PAN **A3.2.5.2.b 面试人员，并检查响应行动的记录，以验证时，CDE的外部检测明文PAN所执行的整治活动。**	具有遵循在事件明文记载PAN响应程序被发现CDE的外部帮助，以确定必要的补救措施，防止将来泄漏。例如，如果PAN被发现CDE的外部，分析应该被执行以（1）确定它是否被保存独立于其他数据（或者是它的完整轨道的一部分？），（2）识别的源数据，以及（3）确定导致数据作为CDE外侧的控制间隙。
A3.2.6 实施用于检测和防止明文PAN从经由未授权信道，方法或过程，包括生成审计日志和警报离开CDE机制。 ***PCI DSS参考：*** *PCI DSS要求的范围*	**A3.2.6.a 检查文档和观察实施机制，以验证机制是：** • 实施积极运行 • 被配置为检测和防止明文PAN离开CDE通过未经授权的信道，方法，或过程 • 经由非授权信道，方法，或过程产生在检测clear-文本PAN离开CDE的日志和警报 **A3.2.6.b 检查审计日志和警报，并采访负责人员，以确认警报进行了研究。**	机制来检测和防止明文PAN的未经授权的损失可以包括适当的工具，如防止数据丢失（DLP）的解决方案，和/或手动流程和程序。该机制的覆盖范围应包括，但不限于，电子邮件，下载到可移动介质，并输出到打印机。这些机制的使用允许一个组织来检测和防止可能导致数据丢失的情况。

A3要求	测试程序	指导
A3.2.6.1 在检测的尝试经由非授权信道，方法或工艺，以去除从CDE明文PAN的要发起实现响应程序。响应程序必须包括： • 程序由负责人员提醒及时调查 • 程序补救数据泄漏或处理间隙，根据需要，以防止任何数据丢失	**A3.2.6.1.a** 检查文档化反应步骤，以检验用于经由非授权信道，方法，或过程响应于尝试移走从CDE明文PAN的程序包括： • 程序由负责人员提醒及时调查 • 程序补救数据泄漏或处理间隙，根据需要，以防止任何数据丢失	试图通过未授权渠道，方法或工艺去除明文PAN可能表明恶意窃取数据，也可以授权雇员是谁不知道或根本就没有遵循正确的方法的动作。这些事件的及时调查可以查明修复需要被应用，并提供有价值的信息，以帮助了解其中的威胁来自何方。
	A3.2.6.1.b 进行面试的人员，并检查的检测明文PAN时通过未经授权的渠道，方法或过程留下CDE采取的行动记录，并验证整治活动。	
A3.3验证PCI DSS被纳入业务照常（BAU）活动		
A3.3.1 实现关键的安全控制失效的过程可以立即检测和警报。关键的安全控制的例子包括，但不限于： • 防火墙 • IDS / IPS • FIM • 反病毒 • 物理访问控制 • 逻辑访问控制 • 审计日志机制 • 分割控制（如果使用） ***PCI DSS参考：要求1-12***	**A3.3.1.a** 检查文件的政策和程序，以验证过程被定义为立即检测和对关键安全控制故障警报。	对于没有及时正规流程（尽快）检测和关键安全控制故障报警，故障可能未被发现长时间，并为攻击者提供充足的时间来从持卡人数据环境破坏系统，窃取敏感数据。
	A3.3.1.b 检查检测和报警流程及面试人员确认过程为所有关键安全控制来实现，并在警报产生严重的安全控制结果失败。	

A3要求	测试程序	指导
A3.3.1.1 应对任何关键的安全控制的故障及时。为应对故障的安全控制必须包括流程： • 恢复安全功能 • 确定和记录安全故障时间（日期和时间开始到结束） • 确定和记录失败的原因（S），包括根本原因，和记录补救，以解决根本原因需要 • 识别和解决故障期间出现的任何安全问题 • 执行风险评估，以确定进一步的行动是否需要为安全故障导致 • 实施控制，以防止故障原因再次发生 • 安全控制的恢复监测 ***PCI DSS参考：要求1-12***	**A3.3.1.1.a 检查记录的政策和程序，面试人员核实过程定义和实现对安全控制的故障响应，包括：** • 恢复安全功能 • 确定和记录安全故障时间（日期和时间开始到结束） • 确定和记录失败的原因（S），包括根本原因，和记录补救，以解决根本原因需要 • 识别和解决故障期间出现的任何安全问题 • 执行风险评估，以确定进一步的行动是否需要为安全故障导致 • 实施控制，以防止故障原因再次发生 • 安全控制的恢复监测 **A3.3.1.1.b 检查记录，验证安全控制失效都记录包括：** • 失败的原因（一个或多个）的鉴定，包括根本原因 • 持续安全故障（日期和时间开始和结束） • 整治的细节需要解决的根本原因	书面证据（例如，问题管理系统中记录）应支持流程和程序到位，以安全故障响应。此外，工作人员应在发生故障时意识到自己的责任。操作和响应故障应在书面证据被捕获。

A3要求	测试程序	指导
A3.3.2 查看硬件和每年至少软件技术，以确认他们是否能继续满足组织的PCI DSS要求。（例如，由供应商和/或不再不再支持的技术审查符合组织的安全需求。）	**A3.3.2.a** 他们是否能继续满足组织的PCI DSS要求检查记录的政策和程序，面试人员核实过程定义和实施审查的硬件和软件技术进行确认。	硬件和软件技术在不断地发展和组织需要意识到改变他们所使用的技术，以及这些技术不断发展的威胁。企业还需要了解由技术供应商作出他们的产品或支持流程，了解这些变化如何影响组织使用该技术的变化。这种影响或影响PCI DSS控制可以帮助采购，使用和部署策略，并确保依靠这些技术的控制仍然有效的技术定期审查。
	A3.3.2.b 回顾最近的审查结果来验证评审至少每年进行一次。	
该过程包括补救不再满足组织的PCI DSS要求，达到技术和包括更换技术的适当计划。 ***PCI DSS参考：要求2,6***	**A3.3.2.c** 对于已确定不再满足组织的PCI DSS要求任何技术，验证计划到位，以修复技术。	

A3要求	测试程序	指导
A3.3.3 执行审查至少每季度一次验证BAU活动被人跟踪。评论必须分配给PCI DSS合规性计划（如A3.1.3标识）的人员进行，并包括以下内容： • 所有BAU活动（如，A3.2.2，A3.2.6和A3.3.1）正在执行确认 • 这些人员在下面的安全政策和操作程序（例如，每天的日志评论，防火墙规则集的评论，配置标准的新系统等）确认 • 在介绍如何审查已经完成，包括所有BAU活动是如何被确认为是到位。 • 按要求年度PCI DSS评估的记录证据收集 • 审查和注销通过分配给PCI DSS合规计划的责任人员的结果（如A3.1.3识别） • 记录和文档至少12个月，覆盖所有BAU活动保留 ***PCI DSS参考：要求1-12***	**A3.3.3.a 检查政策和程序，以验证工艺审查和验证BAU活动定义。验证程序包括：** • 确认所有BAU活动（如，A3.2.2，A3.2.6和A3.3.1）正在执行 • 确认人员以下的安全政策和操作程序（例如，每天的日志评论，防火墙规则集的评论，配置标准的新系统，等等） • 在介绍如何审查已经完成，包括所有BAU活动是如何被确认为是到位 • 收集书面证据的要求年度PCI DSS评估 • 审查并通过PCI DSS治理执行管理指派专人负责注销结果 • 保留记录和文档至少12个月，涵盖了所有BAU活动 **A3.3.3.b 采访专人负责检查审查核实的记录：** • 评论被分配给PCI DSS合规程序的专业人员进行。 • 回顾至少每季度进行。	实现PCI DSS控制到一切照旧活动，是保证安全的有效方法是作为一个持续的基础上正常业务运作的一部分。因此，重要的是，进行独立的检查，以确保BAU控制是活性和如预期工作。这些独立检查的目的是审查确认正在执行一切照旧活动的证据。这些评论也可以用于验证适当的证据正在维护，例如，审计日志，漏洞扫描报告，防火墙评论等，以帮助实体的下届PCI DSS评估的准备。

A3要求	测试程序	指导
A3.4控制和管理对持卡人数据环境的逻辑访问		
A3.4.1 回顾用户帐户和访问权限，调查范围内的系统组件，至少每半年要确保用户帐户和访问基于工作职能保持适当的，并授权。 ***PCI DSS参考：要求7***	**A3.4.1 采访专人负责检查证明文件，以确认：** • 用户帐户和访问权限进行审查，至少每半年一次。 • 点评确认接入是适当根据工作职能，所有的访问被授权。	访问要求随着时间的推移个人改变角色或者离开公司，并作为工作职能发生变化。管理层需要定期复查，重新验证，并更新用户访问，在必要时，以反映人事变动，包括第三方和用户的工作职能。
A3.5识别和可疑事件作出回应		
A3.5.1 实施的攻击模式，及时识别和不良行为跨系统的方法，例如，在使用协同人工审查和/或集中管理或自动化的对数相关性分析工具，至少包括以下内容： • 异常或可疑活动的识别，因为它发生时 • 在检测到可疑活动或异常相关责任人及时警示发行 • 响应于根据警报文件化反应程序 ***PCI DSS参考：要求10，12***	**A3.5.1.a 审查文件和面试人员核实的方法是定义和实现，以确定及时跨系统的攻击模式和不良行为，并包括以下内容：** • 异常或可疑活动的识别，因为它发生时 • 及时提醒相关责任人的发行 • 响应于根据警报文件化反应程序 **A3.5.1.b 检查事件响应程序和面试负责人员确认：** • 随叫随到的人员得到及时的提醒。 • 警报回应每个文件响应程序。	来识别跨系统的攻击模式和不希望的行为的能力是在预防，检测，或最小化数据妥协的影响是至关重要的。日志在所有环境中的存在使深入跟踪，警报和分析出问题的时候。确定折衷的原因是非常困难的，如果不是不可能的，没有过程来证实从关键的系统组件的信息，并执行安全功能，诸如防火墙，IDS / IPS，和文件级完整性监控（FIM）系统的系统。因此，对于所有的关键系统部件和执行安全功能的系统日志应收集，相关，和维护。这可能包括使用的软件产品和服务的方法来提供实时分析，报警，

附录B：补偿性控制

补偿控制可被视为对于大多数PCI DSS要求当一个实体不能明确符合要求的规定，由于合法的技术或记录业务上的限制，但已充分平缓通过实施等，或补偿，控制与需求相关联的风险。

补偿控制必须满足以下标准：

1.符合原来的PCI DSS要求的目的性和严密性。

2.提供防御作为原始PCI DSS的要求，使得补偿控制足够抵消原来的PCI DSS要求的目的是抵御风险的水平相近。（看到 *指导专栏* 的每个PCI DSS要求的目的。）

3.要"超越"其他PCI DSS要求。（只要符合其他PCI DSS要求是不是一个补偿的控制。）

当评估"超越"为补偿控件，请考虑以下几点：

注意：在项目a）至c）中的旨在仅作为示例。所有补偿性控制必须审查和通过谁进行的PCI DSS审查评估员验证的充分性。补偿控制的有效性依赖于在其中控制被实现环境，周围的安全控制，并且所述控制的配置的细节。公司应该知道，一个特定的补偿控制不会有效于各种环境。

a）现有的PCI DSS要求，不能被看作是如果他们已经要求在审查项目补偿控制。例如，对于非控制台管理访问密码必须发送加密，以缓解拦截明文管理密码的风险。实体不能使用其它PCI DSS密码要求（入侵者锁定，复杂密码等），以弥补缺乏加密后的口令，因为这些其他的密码要求不能减轻明文密码截取的风险。此外，其他的密码控制已经在审查（密码）项PCI DSS要求。

b）现有的PCI DSS要求可被视为如果他们需要另一个领域补偿性控制，但不要求在审查项目。

c）中存在的PCI DSS要求可以用新的控制进行组合成为一个补偿控制。例如，如果一个公司无法呈现每要求3.4（例如，通过加密），补偿控制可以由一个或多个设备，应用程序，以及解决所有以下的控制的组合的不可读持卡人数据：（1）内部网络分段;（2）的IP地址或MAC地址过滤; 和（3）一次性密码。

4.要与不遵守PCI DSS的要求，评估员需要每个年度PCI DSS评估期间全面评估补偿控制，以验证各补偿控制充分解决原有PCI DSS要求旨在风险造成的额外风险相称地址，每上述项目1-4。为了保持合规性，程序和控制必须到位，以确保补偿性控制仍然有效的评估完成之后。

附录C：补偿性控制工作表

使用此工作表定义，其中补偿控制用于满足PCI DSS要求任何要求补偿控制。需要注意的是补偿控制措施也应在报告中记录在相应PCI DSS要求部分合规。

注意：只有已经开展了风险分析，并有合法的技术或书面业务限制的公司可以考虑使用补偿性控制来实现合规性。

需求人数和定义：

	所需资料	说明
1.限制	清单约束排除符合原来的要求。	
目的	定义原始控制的目标; 标识由补偿控制达到了目标。	
3。 已识别的风险	确定由缺乏原有的控制造成的任何额外的风险。	
4.补偿性控制的定义	定义补偿性控制并解释它们是如何解决原控制和风险增加的目标，如果有的话。	
5.验证补偿性控制的	定义补偿性控制是如何验证和测试。	
6.保养	定义流程和控制措施，以维护补偿性控制。	

补偿性控制工作表 - 已完成实施例

使用此工作的任何要求标注为通过补偿性控制"到位"被定义补偿性控制。

需求人数： ***8.1.1 - 是否允许他们访问系统组件或持卡人数据之前，唯一的用户ID标识的所有用户？***

	所需资料	说明
1.限制	清单约束排除符合原来的要求。	*XYZ公司采用单机UNIX服务器没有LDAP。因此，它们各自需要一个"根"登录。这是不可能的XYZ公司管理的"根"登录，也不是可行的，每个用户登录所有的"根"的活动。*
目的	定义原始控制的目标; 标识由补偿控制达到了目标。	*唯一需要登录的目标是双重的。首先，它没有考虑从安全角度来看可以接受的共享登录凭据。其次，具有共享登录使得不可能明确陈述一个人负责的特定动作。*
3。 已识别的风险	确定由缺乏原有的控制造成的任何额外的风险。	*附加险是不能确保所有用户都具有一个唯一的ID，并能够被追踪引入到门禁系统。*
4.补偿性控制的定义	定义补偿性控制并解释它们是如何解决原控制和风险增加的目标，如果有的话。	*XYZ公司将要求所有用户登录到使用他们的普通用户帐户的服务器，然后使用"命令"命令来运行任何管理命令。这允许使用的"根"帐户权限来运行由须藤在安全日志中记录预先定义的命令。通过这种方式，每个用户的行为可以追溯到单个用户帐户，没有"根"的密码被与用户共享。*
5.验证补偿性控制的	定义补偿性控制是如何验证和测试。	*XYZ公司演示了评审员认为sudo命令被配置正确使用"sudoers文件"的文件，只有预先定义的命令可以被特定的用户运行，并通过使用sudo的个人进行的所有活动都记录，以确定执行行动的个人使用"root"特权。*
6.保养	定义流程和控制措施，以维护补偿性控制。	*XYZ公司文档的流程和程序，以确保须藤配置没有改变，修改，或移除，以允许个别用户没有被单独地识别，跟踪和记录执行根命令。*

附录d：分割和商务设施的取样/系统组件