支付卡行业（PCI）数据安全标准

安全审计程序

版本：V1.1

发布时间：2006年9月

目录

前言

支付卡行业（PCI）安全审计程序的目标用户是执行现场审查的评估机构，在商家和服务提供商的要求下，评估机构根据支付卡行业数据安全标准（以下简称PCI DSS）要求进行合规审核。
本文档中阐述的要求和审计程序基于PCI DSS。

本文档包括以下内容:

- **前言**
- **PCI DSS适用性信息**
- **PCI DSS要求合规评估范围**
- **合规报告的指导和内容**
- **公开事项再评估**
- **安全审计程序**

附录

- **附录 A：PCI DSS对于主机服务商的适用性（及测试程序）**
- **附录 B：补偿控制**
- **附录 C：补偿控制备忘录/完整示例**

PCI DSS 适用性信息

下表介绍了通常会使用到的持卡人数据和敏感认证数据、它们是否允许**被保存**以及**各数据元素**是否必须受到**保护**。本表格没有列举出所有的数据元素，只阐明了应用于各类数据元素的不同类型的要求。

	数据元素	存储许可	保护要求	PCI DSS 要求 3.4
持卡人数据	主账号（PAN）	YES	YES	YES
	持卡卡人姓名*	YES	YES*	NO
	服务代码*	YES	YES*	NO
	有效期*	YES	YES*	NO
敏感认证数据**	全部磁条信息	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

*当这些数据元素与PAN一起存储时，它们必须受到保护。保护措施必须符合PCI DSS的相关要求。另外，基于某种原因（比如，顾客个人信息保护、隐私保护、防止身份盗窃或保护数据安全），其他法律可能对这些数据会提出特别的保护要求，或者要求在经营活动中收集了顾客的个人信息的公司适当地公开其某些活动，以符合法律的要求。在PAN没有被存储、处理或传输的情况下，PCI DSS不适用。

**认证结束后，禁止存储敏感认证数据（即使已加密）。

PCI DSS 要求合规评估范围

PCI DSS 安全要求适用于所有“系统组件”。系统组件可以是持卡人数据环境中或与之相连的任何网络组件、服务器和应用等。持卡人数据环境是处理持卡人数据或敏感认证信息的网络部分。网络组件包括（但不限于）防火墙、交换机、路由器、无线接入点、网络设备和其他安全设备等。服务器类型包含但不仅限于：Web、数据库、认证、邮件、代理、网络时间协议（NTP）和域名服务（DNS）等服务器。应用是指所有购买的和定制的应用，包括内部和外部（例如，互联网）应用。

通过适当的网络划分，将存储、处理或传输持卡人数据的系统与其他系统分离，可以缩小持卡人数据环境的范围。评估机构必须检查网络划分是否充分而且缩小了审计范围。

服务商或商家可以使用第三方服务提供商来管理路由器、防火墙、数据库、物理安全设备和/或服务器等组件。如果是这样，持卡人数据环境的安全性可能受到影响。必须根据 1) 第三方服务提供商的客户的PCI审计程序；或者 2)第三方服务提供商自己的PCI 审计程序对第三方服务商提供的相关服务进行审查。

对于需要接受年度现场审查的服务提供商，必须对存储、处理或传输持卡人数据的所有系统组件进行合规审查。

对于需要接受年度现场审查的商家，合规审查范围的重点是与授权和结算相关的任何系统或系统组件，这些系统/系统组件存储、处理或传输持卡人数据，它们包括：

- 商家网络中的所有外部连接（例如，员工远程访问、执行处理和维护任务的支付卡公司和第三方的访问）
- 授权和结算环境的入站或出站连接（例如，员工访问连接或防火墙和路由器等设备的连接）
- 任何位于授权和结算环境之外且存付的账号超过50万的数据仓库。注：即使一些数据仓库或系统不要求进行审计，但是商家仍然有责任确保所有存储、处理或传输持卡人数据的系统符合PCI DSS要求
- POS 环境 – 它是商家场所（如零商店、餐馆、酒店、加油站、超市或其他POS场所）中接受交易的位置
- 如果商家场所没有外部访问（通过互联网、无线、虚拟专用网（VPN）、拨号、宽带或公用设备（如自动售货机）访问），可以排除对POS环境的审计

无线

如果使用无线技术存储、处理和传输持卡人数据（例如，POS 交易数据和“line-busting”），或者部分持卡人数据环境与无线局域网相连（例如，未使用防火墙明确地隔离），必须采用并执行针对无线环境的要求和测试程序。无线安全目前还不成熟，这些要求规定了提供最低限度的保护所需要实现的基本无线安全特性。由于无线技术安全性还得不到保障，因此在采用无线技术之前，组织应认真考虑无线技术的必要性，以防范风险。可以考虑仅将无线技术应用于非敏感性数据传输，或者等待部署更安全的技术。

外包

对于那些将持卡人数据的存储、处理和传输外包给第三方服务提供商的实体，*合规报告*必须记录每个服务提供商承担的任务。此外，服务提供商还有责任审查他们自己的 PCI DSS 要求合规情况，这与客户的合规审计无关。另外，商家和服务提供商必须签署合约，要求所有相关的第三方访问持卡人数据时必须遵守 PCI DSS 的规定。*有关详细介绍请参阅本文档中的要求 12.8*

取样

评估机构可以选择一个具有代表性的系统组件进行测试。样本必须是从所有类型的系统组件中选择的具有代表性的组件，而且应覆盖受审查区域的各种操作系统、功能和应用。例如，审查者可以选择运行 Apache 的 Sun 服务器、WWW 服务器、运行 Oracle 的 NT 服务器、运行传统支付卡处理应用的大型主机系统、运行 HP-UX 的数据传输服务器和运行 MYSQL 的 Linux 服务器。如果所有应用都运行在一个OS（例如NT或Sun）上，样本仍然应该覆盖各种应用（例如、数据库服务器、Web 服务器和数据传输服务器）。

选择商家的商店或连锁店样本时，评估机构应考虑以下事项：

- 如果制定了相关的标准，而且每家商店都遵循了所要求的PCI DSS流程，取样范围可以小于所要求的范围，如果没有标准流程，应确保每家商店都根据标准流程进行配置。
- 如果实施了多种类型的标准流程（例如，不同类型的商店实施不同的流程），取样范围应足够大，以确保覆盖实施了不同类型流程的各类商店。
- 如果未实施标准PCI DSS流程而且每家商店都实施他们自己的流程，取样范围应较大，以确保每家商店都理解并正确地实现PCI DSS要求。

补偿控制

评估机构必须书面记录补偿控制措施，而且随同合规报告一起呈递，请参阅附录C – 补偿控制备忘录/完整示例

有关“补偿控制”的定义，请参阅PCI DSS术语和缩略语。

合规报告的指导和内容

评估机构可以将此文档作为模板来创建《合规报告》。接受审计的实体应遵守支付卡公司的相关报告要求，以确保每家支付卡公司都认可实体的合规地位。联系各家支付卡公司，以确定各公司的报告要求和指导说明。编写《合规报告》时，所有评估机构都必须参照报告的内容和格式指导说明：

1. 联系信息和报告日期

- 包括商家或服务提供商和评估机构的联系信息
- 报告的编写日期

2. 执行摘要

包括以下内容：

- 业务说明
- 与公司共享持卡人数据的服务提供商和其他实体
- 执行人关系
- 说明实体是否直接连接到支付卡公司
- 对于商家，列出所使用的POS产品
- 任何必须遵守PCI DSS规定的全资附属实体
- 任何需要遵守PCI DSS规定的国际实体
- 任何连接到持卡人数据环境的无线 LAN 和/或无线 POS 终端

3. 工作范围和采用的方法说明

- 执行评估所使用的安全审计程序文档的版本
- 评估时间安排
- 进行重点评估的环境（例如，客户的互联网接入点、公司内部网、支付卡公司的处理点）
- 任何未接受审查的区域
- 网络拓扑和控制的简要说明和概要图
- 访谈人员列表
- 审查的文档列表

- 所使用的硬件和关键软件（如数据库或加密软件）列表
- 对于托管服务提供商（MSP）审查，明确地说明本文档中的哪些要求适用于 MSP（并需要进行审查），以及哪些要求不需要接受审查，而是由MSP的客户进行审查。说明进行MSP季度弱点扫描时必须对 MSP 的哪些IP地址进行扫描，以及哪些IP地址由 MSP 的客户执行他们的季度扫描任务时进行扫描。

4. 季度扫描结果

- 在“要求 11.2”的备注中对最近的季度扫描结果进行总结
- 扫描必须覆盖实体中所有的外部可访问（互联网接口）IP 地址

5. 结果和报告

- 所有评估机构都必须使下面的模板提供每项要求和子要求的评估结果详细报告
- 可行的情况下，应记录为了实施控制而采用的所有补偿控制。
- 有关补偿控制的定义，请参阅PCI DSS术语和缩略语。

公开事项再评估

需要提供“已实施的控制措施”报告，以确保合规性。如果审计员/评估机构编写的原始报告包含“公开事项”，商家/服务提供商必须提出这些事项，然后才能进行验证。评估机构/审计员将进行重新评估，以确定是否发生了变更，以及所有要求是否都得到了满足。重新验证之后，评估机构将发布新的《合规报告》，说明系统完全合规，然后按照指导说明呈递报告（参阅前面的内容）

构建和维护安全网络

要求 1: 安装并且维护防火墙以保护持卡人数据

防火墙是一种计算机设备，它控制着出入组织网络或出入组织内部敏感网络的通信。防火墙检查所有的网络通信并阻止不符合特定安全要求的通信。

所有系统必须受到保护，以防止来自互联网的非授权访问，这些非授权访问可能伪装成一次电子商务交易、员工通过桌面电脑进行互联网浏览或员工的电子邮件访问。通常，看似平常的互联网通路可以成为进入关键系统的途径。所以，防火墙是计算机网络的一个关键保护机制。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
1.1 建立防火墙配置标准，包括：	**1.1** 获得并查看防火墙配置标准和下面指出的其他文档，以检查标准是否完备。必须检查本节中规定的所有项目。			
1.1.1一个正式的流程，用以对所有的外部网络连接和防火墙配置变更进行批准和测试	**1.1.1** 检查防火墙配置标准是否包含一个正式的流程，这个流程应规定了如果如何对外部连接和防火墙配置的所有更改进行测试和审批。			
1.1.2 当前的网络图中必须标明所有连接到持卡人数据的所有连接（包括所有无线网络连接）	**1.1.2.a** 检查是否存在当前网络图，并检查这个网络图是否记录了连接到持卡人数据的所有连接（包括所有无线网络连接）			
	1.1.2.b.检查这个网络图是否为最新的网络图。			
1.1.3 要求在所有互联网连接点以及隔离区（DMZ）与内部网络区域之间配置防火墙	**1.1.3** 检查防火墙配置标准是否要求在每个互联网连接点以及在隔离区（DMZ）与内联网之间配置防火墙。检查当前网络图是否与防火墙配置标准相一致。			
1.1.4网络组件逻辑管理的组、角色和职责描述	**1.1.4** 检查防火墙配置标准是否包括了网络组件逻辑管理的组、角色和职责描述。			
1.1.5 业务必需的服务和端口清单文件	**1.1.5** 检查防火墙配置标准是否包括一个业务必需的服务和端口清单文件			
1.1.6任何采用的传输协议都必须经过审批和记录。传输协议不仅限于超文本传输协议（HTTP）、安全套接字层（SSL）、安全 Shell（SSH）和虚拟专用网络（VPN）协议	**1.1.6** 检查防火墙配置标准是否包括任何可用协议（不仅限于 HTTP、SSL、SSH 和 VPN）的审批和记录规定。			
1.1.7 对采用的任何风险较高的协议（比如FTP）进行审批和记录。内容包括，使用此协议的原因和已采取的安全措施	**1.1.7.a** 检查防火墙配置标准是否包括任何风险性协议（如 FTP）的审批和记录规定，并且必须说明使用此类协议的原因以及已采取的安全措施			
	1.1.7.b 检查每项运行中的服务的文档和设置，以获得能够证明服务的必要性和安全性的证据。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
1.1.8 每季度复审防火墙和路由器的规则设置	**1.1.8.a** 检查防火墙配置标准是否要求每季度复审防火墙和路由器的规则设置			
	1.1.8.b 检查是否每季度都复审了这些规则设置			
1.1.9 路由器的标准配置	**1.1.9** 检查防火墙配置标准是否应用于防火墙和路由器			
1.2 建立一个防火墙配置用以拒绝来自不可信网络和主机的所有通信，持卡人数据环境所必需的协议除外。	**1.2** 选择一个样本防火墙/路由器，它位于 1)互联网与 DMZ 之间，2）DMZ与内部网络之间。这个样本应包括互联网上的扼制点路由器、DMZ 路由器和防火墙、DMZ 持卡人区域、边界路由器和内部持卡人数据网络区域。检查防火墙和路由器配置，以确定是否只允许持卡人数据环境所必需要的协议的入站和出站流量。			
1.3 任何存储有持卡人数据的系统（及其组成部分）与公共服务器之间的任何连接（包括无线连接），都需建立一个防火墙配置加以限制。这个防火墙配置应包含：	**1.3** 检查防火墙/路由器配置，以确定公用服务器与存储有持卡人数据的组件之间的连接是否受到限制，方法如下：			
1.3.1 限制互联网输入流量到达隔离区内的互联网协议（IP）地址（进入过滤）	**1.3.1** 检查是否仅允许互联网流量到达DMZ内的IP地址			
1.3.2 不允许内部地址经由互联网 访问 DMZ	**1.3.2** 检查是否允许内部地址经由互联网进入DMZ。			
1.3.3 实施状态检测－也称为动态包过滤－只允许通过“已建立”的连接进入网络。	**1.3.3** 检查防火墙是否执行状态检查（动态包过滤）。[只允许通过已建立的连接进入，而且这些连接必须与预先建立的会话相关联（使用“syn reset”或“syn ack”位组对所有 TCP 端口运行 NMAP – 如果收到响应，表示允许数据包通过，即使它们不是预先建立的会话中的一部分）]。			
1.3.4 将数据库放置于内部网络区域，且必须与 DMZ 隔离	**1.3.4** 检查数据库是否位于与DMZ相隔离的内部网络区域。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
1.3.5 限制持卡人数据环境的入站和出站流量，仅允许必需的流量出入	**1.3.5** 检查是否仅允许持卡人数据环境所必需的入站和出站流量，以及是否使用文档记录了这些限制规定。			
1.3.6 保护并同步路由器配置文件。例如，运行配置文件（路由器在正常工作状态下使用的配置文件）和初始化配置文件（当路由器重新启动时会使用）应具有相同的安全配置。	**1.3.6** 检查路由器配置文件的安全性和同步性[例如，运行配置文件（路由器在正常工作状态下使用的配置文件）和初始化配置文件（当路由器重新启动时会使用）应具有相同的安全配置]。			
1.3.7 拒绝所有未被明确允许入站和出站的流量	**1.3.7** 检查是否拒绝 1.2 和 1.3 中未述及的所有其他入站和出站流量。			
1.3.8 在任何无线网络和持卡人数据环境之间安装边界防火墙，并且将这些防火墙配置为拒绝所有来自无线环境的流量或控制业务必需的流量	**1.3.8** 检查无线网络与存储了持卡人数据的系统之间是否安装了防火墙，以及这些防火墙是否拒绝或控制任何从无线环境进入持卡人数据存储系统的流量。			
1.3.9 任何与互联网直接相连、又被用于访问组织（内部）网络的移动电脑和员工所有的电脑（比如，员工使用的笔记本电脑）应安装个人防火墙软件	**1.3.9** 检查任何与互联网直接相连、又被用于访问组织（内部）网络的移动电脑和员工所有的电脑（比如，员工使用的笔记本电脑）上是否安装并启用个人防火墙系统，以及是否按照组织规定的标准对防火墙进行了配置而且员工无法修改配置。			
1.4 禁止任何存储持卡人数据的内部网络和系统组件（比如，数据库，日志，跟踪文件） 被外部网络间接/直接地公开访问。	**1.4** 检查是否禁止了外部公用网络与存储持卡人数据的系统组件之间的直接访问，按照以下方法进行检查，并且重点检查 DMZ 与内部网络之间的防火墙/路由器配置：			
1.4.1 建立一个DMZ以过滤和屏蔽所有流量，禁止为互联网流量提供直接的入站和出站路由	**1.4.1** 检查防火墙/路由器配置，并检查是否存在互联网流量的直接入站或出站路由			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
1.4.2 限制源自支付卡应用、目的地为DMZ区IP地址的出站流量	**1.4.2** 检查防火墙/路由器配置，并检查是否仅允许持卡人应用的内部出站流量到达 DMZ内的IP地址。			
1.5 实施IP伪装以防止内部地址被识别并被暴露在互联网上。 使用私人地址空间（参考 RFC 1918）并利用端口地址转换（PAT）或网络地址转换（NAT）。	**1.5** 对于上面的样本防火墙/路由器组件，检查是否采用了 NAT 或其他使用 RFC 1918 地址空间的技术，以限制将IP地址从内部网络广播到互联网（IP 伪装）。			

要求 2：避免使用供应商提供的默认系统口令和其他安全参数

（组织内部或外部的）攻击者经常使用供应商默认口令和其他供应商默认设置来攻击系统。这些默认口令和其他一些默认设置在黑客团体中广为知晓，而极易根据公开的信息推定。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
2.1 将系统安装到网络上**之前**，应修改供应商提供的默认设置（比如，口令、SNMP（社区字符串），并删除不必要的账户）。	**2.1** 选择一个样本系统组件、关键服务器和无线接入点，（在系统管理的帮助下）尝试使用供应商提供的默认账户和口令登录设备，以检查是否已经更改了默认的账户和口令。（通过供应商手册和网上资源获取供应商提供的默认账户/口令）			
2.1.1对于无线环境，修改无线设备的供应商默认设置，包括但不仅限于 WEP 口令、SSID、口令和 SNMP 社区字符串。禁止SSID广播。在WPA可用的情况下，启用 WiFi 访问保护（WPA 和 WPA2）技术提供加密和身份认证。	**2.1.1** 对于无线环境，检查下列相关的供应商默认设置： • 安装时是否更改了WEP密钥，知晓密钥的员工离开组织或转换工作岗位时否更改了WEP 密钥。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
	• 是否更改了默认SSID • 是否禁止了SSID广播 • 是否更改了接入点的默认SNMP社区字符串 • 是否更改了接入点的默认口令 • 如果无线系统支持WPA，是否启用了WPA或WPA2 技术 • 是否更改了其他与安全相关的无线供应商默认设置（如果适用）			
2.2 为所有的系统组件开发配置标准。保证这些标准考虑了所有已知的安全弱点，并与行业认可的系统加固标准相一致，例如，由SANS、NIST和CIS定义的相关标准。	2.2.a 检查组织为网络组件、关键服务器、无线接入点制定的系统配置标准，并检查系统配置标准是否与行业认可的系统加固标准相一致，例如，由SANS、NIST和CIS定义的相关标准			
	2.2.b 检查系统配置标准是否包括后面的项目（2.2.1 – 2.2.4）			
	2.2.c 检查是否遵照系统配置标准配置新系统			
2.2.1每一台服务器只承担一项主要功能（例如，Web服务器、数据库服务器和DNS 应该被分别部署在不同的服务器上）	**2.2.1**对于样本系统组件、关键服务器和无线接入点，检查是否每台服务器只承担一项主要功能			
2.2.2禁用所有不必要的、不安全的服务和协议（指某设备完成它特定的任务不直接需要的服务和协议）	**2.2.2**对于样本系统组件、关键服务器和无线接入点，检查启用的系统服务、守护程序（daemon）和协议。检查是否禁用了不必要或不安全的服务，以及是否对使用的服务进行审批和记录（例如，不使用FTP，或者通过SSH或其他技术对FTP进行加密）。			
2.2.3 设定系统安全参数以防止误用/滥用	**2.2.3.a** 与系统管理员和/或安全负责人面谈，以确认他们是否知晓操作系统、数据库服务器、Web服务器和无线系统的常用安全参数设置。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
	2.2.3.b 检查系统配置标准中是否包括了常用安全参数设置			
	2.2.3.c 对于样本系统组件、关键服务器和无线接入点，检查常用安全参数的设置是否正确。			
2.2.4 移除所有不必要的功能，例如，脚本、驱动、特性、子系统、文件系统和不必要的Web服务器。	**2.2.4** 对于样本系统组件、关键服务器和无线接入点，检查是否移除了所有不必要的功能（例如、脚本、驱动、特性、子系统和文件系统等）。检查是否记录了启用的功能、这些功能是否支持安全配置，以及样本设备上是否只存在经过记录的功能。			
2.3 对所有非控制台管理连接进行加密。利用SSH、VPN或SSL/TLS等技术保护基于Web的管理和其他非控制台管理访问。	**2.3** 对于样本系统组件、关键服务器和无线接入点，通过下面的方法检查是否对非控制台管理访问进行了加密： • 监测登录到各个系统的管理员，以检查要求输入管理员口令之前是否调用了 SSH（或其他加密方法）。 • 复查系统上的服务和参数文件，以确定禁止内部使用Telnet和其他远程登录命令。 • 检查是否使用SSL/TLS技术对无线管理界面的管理 员访问进行了加密。另外，还可以检查管理员是否能够远程连接到无线管理界面（所有无线环境的管理都只能在控制台上进行）			
2.4 主机服务商必须保护各实体的主机环境和数据。这些服务商必须满足一些特定的要求（详见 附录A ： “PCI DSS对于主机服务商的适用性”）	**2.4** 执行“附录 A：PCI DSS对于主机服务商的适用性（及测试程序）”A.1.1 – A.1.4 中介绍的测试程序，完成针对**共享主机服务商**的PCI审计，检查**共享主机服务商**是否为实体（商家和服务提供商）的主机环境和数据提供了保护。			

保护持卡人数据

要求 3：保护存储的持卡人数据

加密是持卡人数据保护的一项关键组成部分。如果入侵者绕过其它网络安全控制措施，但没有正确的密钥，即使能获得经过加密的数据，这些数据对他也是毫无意义的。其它一些被认为是降低潜在风险的措施也可以有效的保护存储数据的安全。例如，除非绝对必要，否则不保存持卡人数据；在不需要完整PAN的情况下，保存时截去部分持卡人数据；不使用未加密的电子邮件传送PAN。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
3.1 保留最少的持卡人数据。开发一个数据保留和处理策略，限制数据存储量和保留时间，达到恰好能满足业务，法律和管理规定需要的程度。上述策略应文档化。	**3.1** 获得并检查公司的数据保留和处理策略和程序，执行以下检查步骤： • 检查策略和程序是否包括针对数据保留的法律、法规和业务要求，包括持卡人数据的具体保留要求（例如，根据业务原因确定持卡人数据的保留时间） • 检查策略和程序是否要求法律、法规或业务不需要保留数据时立即销毁数据，包括销毁持卡人数据 • 检查策略和程序是否覆盖所有的持卡人数据存 储，包括数据库服务器、大型主机、传输目录、用于在服务器之间传输数据的批量数据复制目录和用于协调服务器流量的目录等 • 检查策略和程序是否包含一个程序化（自动）流程，用于每季度移除超过业务或审计所需要的保留期限的持卡人数据，以确保存储的持卡人数据未超过业务所要求的保留期限。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
3.2 禁止在身份认证结束后存储敏感认证数据(即使经过加密) 敏感认证数据包括要求3.2.1 至 3.2.3 中引用的数据：	**3.2** 如果需要接收和删除机密认证数据，获得并检查数据删除流程，以确定被数据是否不可恢复。对于下面的机密认证数据项目，执行以下检查步骤：			
3.2.1 禁止存储磁条中任一磁道的全部内容。(磁条可能位于卡的背面、在一个芯片中或其他位置)这项数据可以被称为全部磁道、磁道、磁道 1、磁道2和磁条数据 *在常见的业务过程中，可能需要保留磁条中的一些数据字段，如持卡人姓名，主账号，有效日期和服务代码。为了将风险降至最低，只存储业务必须的数据字 段。切勿存储卡验证码或个人标识代码（PIN）。* *注：其他信息请参阅术语表。*	**3.2.1** 对于样本系统组件、关键服务器和无线接入点，检查以下项目，并确定在任何情况下都禁止存储卡背面的磁条中任一磁道的全部内容： • 输入的事务处理数据 • 事务处理日志 • 历史文件 • 追查文件 • 调试日志 • 若干数据库结构 • 数据库内容			
3.2.2 不允许存储卡验证码或/验证值（打印在支付卡的正面或背面3或4位阿拉伯数字）。*注：其他信息请参阅术语表。*	**3.2.2** 对于样本系统组件、关键服务器和无线接入点，检查下列项目，并确定在任何情况下都不存储印刷在卡背面或签名条上的三位或四位卡验证码（CVV2、CVC2、CID、CAV2）数据： • 输入的事务处理数据 • 事务处理日志 • 历史文件 • 追查文件 • 调试日志			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
	• 若干数据库结构 • 数据库内容			
3.2.3不允许以明文或密文的形式存储个人标识代码（PIN）	**3.2.3** 对于样本系统组件、关键服务器和无线接入点，检查以下项目，并确定在任何情况下都不允许以明文或密文存储个人标识码（PIN）： • 输入的事务处理数据 • 事务处理日志 • 历史文件 • 追查文件 • 调试日志 • 若干数据库结构 • 数据库内容			
3.3 显示 PAN 时采用隐蔽措施（最多只显示最前6位和最后4位数字）。 *注：在员工和其他组织因特殊原因需要看到完整 PAN 的情况下，本要求不适用；同时，本要求也不能代替其他更为严格的关于持卡人数据显示的要求（例如，对于 POS 收条的要求）。*	**3.3** 获得并检查书面的策略，检查信用卡数据的联机显示，以确定显示持卡人数据时是否采用了隐蔽措施，除非需要看到完整的信用卡卡号。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
3.4 存储于任何位置（包括 PDA，存储介质，日志和由无线网络获得/存储的数据）的 PAN， 在呈递时，通过采用下列任一途径，使 PAN 至少不可读： • 强壮的单向散列函数（散列索引） • 截断（删除或省略字符串的头部或尾部） • 口令本（口令本必须被安全保存） • 强壮的加密机制，并结合相应密钥管理流程和管理程序 提交/呈现账户信息时，至少保证 PAN 不可读（经过散列函数/截断/加密等处理）。 *如组织由于某些原因不能对持卡人数据进行加密,则需参考附录 B：“补偿控制”。*	**3.4.a** 获得并检查已存储数据保护系统的文档内容，包括供应商、系统/流程的类型和加密算法（如果适用）。检查是否使用了以下其中一种方法对数据进行了处理，使之不可读： • 单向散列（散列索引）算法，如 SHA-1 • 截断或隐藏 • 口令本（口令本必须被安全保存） • 强壮的加密机制，并结合相应密钥管理流程和管理程序			
	3.4.b 检查样本数据库服务器中的若干个表，以确认数据是否经过了处理而不可读（即，不以纯文本形式存储数据）			
	3.4.c 检查可移动介质（例如备份磁带）样本，以确认持卡人数据是否经过了处理而不可读			
	3.4.d 检查样本审计日志，以确认持人数据是否经过了处理或被清除出日志			
	3.4.e 检查从无线网络接收到的持卡人数据是否经过了处理并且无法在其存储位置中解读数据。			
3.4.1 如采用了磁盘加密（它优于文件加密或数据库列级加密），逻辑访问必须独立于本地操作系统的访问控制机制（例如，避免使用本地系统账号或活动目录账号）。解密密钥不能和用户帐号绑定或关联。	**3.4.1.a** 如果采用磁盘加密，检查是否通过与本地操作系统机制不同的机制实现对加密文件系统的逻辑访问（例如，不使用本地账号或活动目录账号）。			
	3.4.1.b 检查解密密钥是否不存储在本地系统上（例如，将密钥存储在软盘、CD-ROM 上，以确保其安全并且仅在需要时取回）			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
	3.4.1.c 检查是否对移动介质上存储的持卡人数据进行了加密（磁盘加密方法通常不能对移动介质进行加密）			
3.5 保护持卡人数据的加密密钥，防止泄露和滥用。	**3.5** 检查加密密钥保护流程（加密密钥用于对持卡人数据进行加密以防止泄露和滥用），执行以下步骤：			
3.5.1只允许最少的保管人接触密钥	**3.5.1** 检查用户访问列表，以确定是否仅允许少数保管人接触密钥			
3.5.2密钥应安全保存在尽量少的场所和表单中	**3.5.2**检查系统配置文件，以确定密钥是否以加密格式存储，并且密钥加密密钥与数据加密密钥分开存储			
3.6 对于所有用以加密持卡人数据的密钥，应制定并实施全面的密钥管理流程和程序，包括：	**3.6.a** 检查是否制定了密钥管理程序并且应用该流程管理持卡人数据加密密钥			
	3.6.b 本检查步骤仅针对服务提供商。如果服务提供商与他们的客户共享密钥，以进行持卡人数据传输，检查服务提供商是否为客户提供了相关文档，文档中应包括如何安全存储和更改客户的加密密钥（用于在客户与服务提供商之间传输数据）等指导内容。			
	3.6.c 检查密钥管理流程并执行以下步骤：			
3.6.1 强壮密钥的生成	**3.6.1** 检查密钥管理流程是否要求生成强壮的密钥			
3.6.2 密钥安全分发	**3.6.2** 检查密钥管理流程是否要求确保密钥分发的安全。			
3.6.3 密钥安全存储	**3.6.3** 检查密钥管理流程是否要求确保密钥存储的安全			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
3.6.4 密钥定期更换 • 根据自身认为必要和应用推荐的方式来进行（例如，重设密钥）； • 至少每年一次	**3.6.4** 检查密钥管理流程是否要求定期更换密钥。检查密钥更换流程是否至少每年执行一次。			
3.6.5 过期密钥的销毁	**3.6.5** 检查密钥管理流程是否要求销毁过期密钥。			
3.6.6 知识分割并建立密钥的双重控制（两人或三人分别掌握部分密钥片断，必须聚齐所有片断才能重建整个密钥）	**3.6.6** 检查密钥管流程是否要求知识分割和密钥的双重控制（两人或三人分别掌握部分密钥片断，必须聚齐所有片断才能重建整个密钥）			
3.6.7 防止非授权的密钥更换	**3.6.7** 检查密钥管理流程是否要求禁止非授权的密钥更改			
3.6.8 更换已被知晓或可能被泄漏的密钥	**3.6.8** 检查密钥管理程序是否要求更换已被知晓或可能被泄漏的密钥。			
3.6.9 收回过期或失效的密钥	**3.6.9** 检查密钥管理程序是否要求收回过期或失效的密钥（主要针对 RSA 密钥）			
3.6.10 要求密钥保管人签署一份文件，申明他（她）理解并接受密钥保管责任	**3.6.10** 检查密钥管理流程是否要求保管人签署一份文件以申明他/她理解并接受密钥保管责任			

要求 4：加密开放/公共网络上的持卡人数据传输.

在易被攻击者截获、篡改和重定向的网络上传输敏感信息时必须加密。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
4.1 使用强壮的加密算法和安全协议，例如安全套接字层（SSL）/传输层安全（TLS）和IP 安全协议（IPSEC）来保护敏感持卡人数据在开放/公共网络上的传输。 *在PCI DSS中，开放/公共网络的例子包括互联网、WiFi（IEEE 802.11x）、全球移动通信系统（GSM）和通用分组无线业务（GPRS）*	**4.1.a** 检查在开放/公共网络上传输或接收持卡人数据时是否使用了加密技术（例如，SSL/TLS或IPSEC） • 检查数据传输期间是否使用了强壮的加密方法 • 对于SSL实现，检查浏览器统一资源定位符（URL）中是否有HTTPS，URL中没有HTTPS时，不能有持卡人数据。 • 选择一个样本交易，观察交易发生过程，确定传输期间是否对持卡人数据进行了加密。 • 检查是否仅接受可信任的SSL/TLS密钥/证书。 • 检查是否为所使用的加密算法实现了适合的加密强度 （查看供应商建议/最佳实践）			
4.1.1 通过无线网络传输持卡人数据时，使用WiFi保护访问（WPA 或 WPA2）技术，IPSEC VPN 或SSL/TLS进行传输加密。不要仅仅依赖WEP保护无线网络的机密性和访问权限。	**4.1.1.a** 对于传输持卡人数据或连接到持卡人数据环境的无线网络，检查是否使用了适当的加密算法进行无线传输加密，例如：Wi-Fi保护访问（WPA 或 WPA2）、IPSEC VPN或SSL/TLS			

]

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
如果使用了WEP，应进行以下设置： •使用不低于104 位的加密密钥和 2 位的初始值 •必须与WAP/WAP2、VPN或SSL/TLS 配合使用 •每季度更换WEP共享密钥（或在技术条件允许的情况下采用自动更换的方式） •掌握密钥的人员一旦发生变更，密钥也必须立即更换 •根据MAC地址进行访问限制	**4.1.1.b** 如果使用了WEP，应检查： • WEP是否使用不低于104位的加密密钥和24位的初始值 • WEP是否与则WAP/WAP2、VPN 或SSL/TLS配合使用 • 是否至少每季度更换一次共享的 WEP 密钥（或在技术条件允许的情况下采用自动更换的方式） • 是否在掌握密钥的人员发生变更时立即更换密钥 • 是否根据MAC地址对访问进行限制			
4.2 从不使用电子邮件发送未经加密的PAN。	4.2.a 检查通过电子邮件发送持卡人数据时是否使用了电子邮件加密方法			
	4.2.b 检查是否制定了相应的策略，以声明禁止通过电子邮件发送未加密的PAN			
	4.2.c 与3-5名员工面谈，检查是否要求使用电子邮件加密软件对包含PAN的电子邮件进行加密			

维护一个弱点管理程序

要求 5：使用定期升级的防病毒软件或计算机程序

许多漏洞和恶意病毒经常通过员工的电子邮件进入网络。必须在所有容易受感染的系统上使用防病毒软件。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
5.1 在所有容易感染病毒的系统上部署防病毒软件（尤其是个人电脑和服务器） *注：通常受病毒感染的系统不包括基于 UNIX 的操作系统或大型主机系统。*	**5.1** 对于样本系统组件、关键服务器和无线接入点，检查是否安装了防病毒软件			
5.1.1 确保防病毒电脑程序具有检测，移除其它形式恶意软件的功能，包括间谍软件或广告软件	**5.1.1** 对于样本系统组件、关键服务器和无线接入点，检查防病毒程序能否检测、清除和防御其他恶意软件，包括间谍软件和广告软件			
5.2 确保所有的防病毒措施及时更新和正常运行，并能生成审计日志。	**5.2** 检查防病毒软件是否为最新版本并且运行正常，而且能够生成日志 • 获得并检查相关策略，核实策略是否要求及时更新防病毒软件和病毒库。 • 检查防病软件的宿主系统是否支持自动更新和定期扫描，以及样本系统组件、关键服务器和无线接入点是否启用了这些功能 • 检查是否支持日志生成以及是否根据组织的信息保留策略对日志进行了保留			

要求 6：开发并维护安全的系统和应用

不道德的个人会利用安全弱点获得系统访问特权。许多安全弱点可以使用供应商提供的补丁加以弥补。所有的系统必须安装最新的、适当的补丁，以防内部员工，外部攻击者和病毒的侵害。注：适当的补丁指那些已经过充分的评估和测试、被确定不会与现有的安全配置相冲突的补丁。对于内部开发的应用，采用标准的系统开发流程和安全编码技术可以减少大量的弱点。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
6.1 确保所有的系统组件和软件都安装了最新的、供应商提供的安全补丁。相关补丁应 在发布后的一个月之内被安装。	**6.1.a** 对于样系统组件、关键服务器、无线接入点和相关的软件，将每个系统上安装的安全补丁列表与最新的供应商安全列表进行比较，以检查是否安装了供应商最新提供的补丁			
	6.1.b 检查与安全补丁安装相关的安全策略，以确定这些安全策略是否要求在30天之内安装所有相关的新安全补丁			
6.2 建立一个流程以识别最新发现的安全弱点（例如，从互联网上订阅一个免费的预警服务）。根据新的弱点进行相应的升级。	**6.2.a** 与负责人员面谈，以确定是否实施了这些用于识别最新安全弱点的流程。			
	6.2.b 发现新的弱点公告后，对这个流程进行验证，确定其是否能够识别新的安全弱点，包括使用外部安全弱点信息源和更新要求 2 中所述的系统配置。			
6.3 在业界最佳实践的基础上开发软件应用，并将信息安全与整个软件开发生命周期相结合。	**6.3** 获取并检查书面的软件开发流程，以检查它们是否基于业界标准，以及是否整个生命周期都考虑了安全性。通过检查软件开发流程、与软件开发人员面谈和检查相关数据（网络配置文档、生产和测试数据等），核实以下事项：			
6.3.1 所有的安全补丁以及对系统和软件的配置变更经过测试后，才能部署	**6.3.1** 在部署到实际生产环境之前，确保所有变更（包括补丁）都经过了测试			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
6.3.2将开发，测试和生产环境分离	**6.3.2** 测试/开发环境与生产环境分离，并使用访问控制确保分离			
6.3.3 对开发，测试和生产环境进行职责分离	**6.3.3** 开发/测试环境和生产环境负责人员承担各自的职责。			
6.3.4 生产数据（实际有效的PAN）不允许被用于测试或开发	**6.3.4** 生产数据（实际有效的PAN）不允许被用于测试、开发或者在使用之前对它进行审核。			
6.3.5生产系统正式上线之前，移除所有测试数据和测试账号	**6.3.5** 生产系统正式上线之前，移除测试数据和测试账号			
6.3.6 应用正式上线或向消费者发布前，移除应用中自定义的账号、用户名和口令	**6.3.6** 系统投入生产或向消费者发布之前，移除自定义的应用账户、用户名和/或口令			
6.3.7 在正式上线或向消费者发布前，对定制代码进行复审，检查可能存在的编码弱点	**6.3.7.a** 获取并检查所有书面或其他形式的策略，以检查策略是否要求由非原编码人员复审代码			
	6.3.7.b 检查是否对新代码和修改后的代码进行了复查。 *注：此要求适用于定制软件开发（作为系统开发生命周期（SDLC）的一部分）的代码复查 – 可由内部人员进行复查。从2008年6月30日开始，Web界面应用的自主编码需要经过其他的控制 – 详情请参阅PCI DSS要求6.6。*			
6.4 对所有系统和软件配置的修改，都必须按照变更控制过程进行。变更控制过程包括：	**6.4.a** 获得并检查与安全补丁安装和软件修改相关的公司变更控制程序，检查此程序是否要求按照下面的6.4.1 – 6.4.4进行：			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
	6.4.b 对于样本系统组件、关键服务器、无线接入点，检查每个系统组件的变更情况和安全补丁，并根据变更控制文档记录规定记载这些变更情况。对于所检查的变更情况，确定是否按照变更控制程序进行了记录：			
6.4.1 记录所受到的影响	**6.4.1** 检查变更控制文档记录规定是否要求记录每个取样变更对客户造成的影响			
6.4.2 有关部门管理层审批	**6.4.2** 检查是否每项取样变更都经过了管理层的审批			
6.4.3 测试操作功能	**6.4.3** 检查是否对每个取样变更执行操作功能测试			
6.4.4 恢复程序	**6.4.4** 检查是否为每个取样变更准备了恢复程序			
6.5 所有的Web应用开发基于安全编码指南。 例如，开放Web应用安全项目（OWASP）指南。 复审定制的应用代码以识别编码弱点。 软件开发流程中通常会出现的编码弱点包括：	**6.5.a** 获得并审查所有基于Web的应用的软件开发流程，检查开发流程是否要求为开发人员提供编码技术培训，并检查流程是否基于OWASP指南（http://www.owasp.org）等安全编码指南。			
	6.5.b 对于基于Web的应用，检查是否制定相应的流程以确保Web 应用能够有效地防御：			
6.5.1 无效输入	**6.5.1** 无效输入			
6.5.2 失效访问控制（例如，用户ID的恶意使用）	**6.5.2** 用户ID的恶意使用			
6.5.3 失效的身份认证和会话管理（对于账户凭据和会话Cookie的使用）	**6.5.3** 账户凭据和会话cookie的恶意使用			
6.5.4 跨站脚本攻击（XSS 或CSS）	**6.5.4** 跨站脚本攻击			
6.5.5 缓存溢出	**6.5.5** 由于无效输出和其他原因造成的缓存溢出			
6.5.6 注入缺陷（例如，SQL注入缺陷）	**6.5.6** SQL注入和其他命令注入缺陷			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
6.5.7 不适当的错误处理	**6.5.7** 错误处理缺陷			
6.5.8 不安全的存储	**6.5.8** 不安全的存储			
6.5.9 拒绝服务器攻击（DOS）	**6.5.9** 拒绝服务器攻击（DOS）			
6.5.10 不安全的配置管理	**6.5.10** 不安全的配置管理			
6.6 通过以下方法，确保所有的Web界面应用能抵御已知的攻击： • 由应用安全专业组织，对所有定制的应用代码进行复审，以发现编码弱点 • 在Web界面应用前端，安装应用层防火墙 *注：这些方法在2008 年6月30日之后将成为标准的一项要求，此前被认为是一项最佳实践。*	**6.6** 对于基于Web的应用，确保实现以下其中一项测试方法： • 检查定制应用代码是否定期由应用安全组织进行复查，是否更正了所有的编码弱点，以及在进行更正之后是否对应用进行了重新评估 • 检查是否在Web界面应用之前安装了应用防火墙，以侦测和防止基于Web的攻击			

实施强有力的访问控制措施

要求7：根据业务需要限制对持卡人数据的访问

这项要求是为了保证关键数据仅供授权用户访问。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
7.1 只允许有工作需要的个人访问计算资源和持卡人数据。	**7.1** 获得并检查书面的数据控制策略，检查策略是否要求： • 仅为授权用户ID分配履行工作职责所必需的最低权限 • 根据人员的岗位类别和职能分配权限 • 授权需要负责规定必要权限的管理层的签名 • 实施一个自动访问控制系统			
7.2 为多用户系统建立一套机制：按照“因需知晓”的原则进行访问控制，除非获得特别许可，“拒绝所有”访问。	**7.2** 检查系统设置和供应商文档，检查是否实施了访问控制系统以及该系统是否符合以下要求： • 覆盖所有系统组件 • 根据人员的岗位类别和职能分配权限 • 默认设置为“全部拒绝”（有些访问控制系统默认设置为“全部允许”，因而允许所有访问，除非使用规则明确地拒绝访问）			

要求 8：为每一个具有计算机访问权限的用户分配唯一的ID

为每一个具有访问权限的用户分配唯一的ID，以保证对于关键数据和系统的操作能够被追溯到已知的、被授权的用户。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
8.1 使用唯一的用户名来鉴别用户，此后才允许他们访问系统组件或持卡人数据	**8.1** 对于样例用户ID，复查用户ID列表，并检查是否所有用户都使用唯一的用户名访问系统组件或持卡人数据			
8.2 除了分配唯一的ID，至少采用下列方式的其中一种方法以鉴别所有用户： • 口令 • 令牌设备（例如，SecureID，证书或公开密钥） • 生物特征	**8.2** 检查是否使用唯一ID和附加认证（如口令）鉴别访问持卡人环境的用户，方法如下： • 获得并检查认证方法说明文档 • 对于所使用的各种类型的认证方法和各种类型的系统组件，审核认证方法，以确定认证方法的运行是否与文档中的认证方法说明相一致。			
8.3 针对员工，管理员和第三方的远程网络访问，采用双因素身份认证机制。 例如，使用远程接入拨号用户服务（RADIUS）或终端访问控制器访问控制系统（TACACS）等技术； 在支持个人数字证书的VPN（基于SSL/TLS 或IPSEC）。	**8.3** 检查是否实现了作用于所有远程网络访问的双因素认证机制，方法是：监测一个远程连接到网络的员工（例如管理员），检查是否要求使用附加认证项目（智能卡、令牌PIN）			
8.4 加密所有口令，无论是在传输过程中或存储在任何系统组件中。	**8.4.a** 对于样本系统组件、关键服务器和无线接入点，检查口令文件，确定是否无法获得口令。			
	8.4.b 检查口令文件，确定客户口令是否经过了加密，这一检测步骤仅针对**服务提供商**			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
8.5 对于所有系统中的非消费者用户和管理员，进行适当的用户身份认证和口令管理：	**8.5** 复查认证程序，并与相关人员面谈，确定是否实施了用户身份认证和口令管理程序，方法如下：			
8.5.1 控制用户ID、凭据以及其它鉴别对象的增加，删除和修改	**8.5.1.a** 选择一个样本用户ID，这个样本应包括管理员和普通用户。通过执下步骤，检查是否根据公司策略对使用系统的用户进行认证： • 获得并检查每个ID认证表 • 通过认证表中的信息，检查是否根根据认证表（和分配的权限及获得的所有签名）对样本用户ID进行认证			
	8.5.1.b 检查是否仅允许管理员访问无线网络管理控制台			
8.5.2 在执行口令重置前认证用户身份	**8.5.2** 检查口令程序并观察安全人员，以确定：如果用户通过电话、电子邮件、网页或其他非面晤方式请求重设口令时，是否在重设口令之前对用户的身份进行验证			
8.5.3 为每个用户设置唯一的初始口令，并在初次使用后立即更改	**8.5.3** 检查口令程序并观察安全人员，以确定是否为每个新用户设置唯一的初始口令并且在初次使用后立即更改			
8.5.4 立即收回被解聘的用户的访问权限	**8.5.4** 选择在过去六个月内被解聘的若干员工样本，审查当前用户访问列表，确定他们的ID是否已经被禁用或移除			
8.5.5 至少每九十天清理并移除一次非活动的用户账户	**8.5.5** 对于样本用户ID，检查是否不存在未使用时间超过九十天的账户			
8.5.6 供应商远程维护账户仅在需要时才被启用	**8.5.6** 检查是否禁用了供应商支持和维护系统所使用的账户，仅在需要时才启用此账户，并对此账户的使用情况进行监控			
8.5.7 向所有具有持卡人数据访问权限的用户通告口令管理程序和策略	**8.5.7** 拜访样本用户ID的所有者，确定他们是否熟悉口令程序和策略			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
8.5.8 避免使用共享账户和共享口令	**8.5.8.a** 对于样本系统组件、关键服务器和无线接入点，检查用户 ID 列表，以确定： • 禁用或移用了公用用户ID和账户 • 不存在可执行系统管理活动和其他关键功能的共享用户 ID • 禁用使用共享和公用的用户ID管理无线LAN和设备			
	8.5.8.b 检查口令策略/程序，以核实是否明确地禁止共享口令			
	8.5.8.c 与系统管理员面谈，核实是否禁止发送共享口令，即使接收到请求时也禁止。			
8.5.9 至少每九十天修改一次用户口令	**8.5.9** 对于样本系统组件、关键服务器和无线接入点、获得并查看系统配置设置，以检查系统配置是否被设置为要求用户至少每九十天修改一次口令。 对于**服务提供商**，复查内部流程和客户/用户文档，以检查是否要求定期修改客户口令，以及是否为客户提供了口令修改指导，这些指导说明了在何时以及哪些情况必须修改口令。			
8.5.10 口令最小长度不低于七个字符	**8.5.10** 对于样本系统组件、关键服务器和无线接入点，获得并查看系统配置设置，以检查系统口令的长度是否被设置为不低于七个字符。 对于**服务提供商**，复查内部流程和客户/用户文档，以检查是否要求客户口令必须符合最低口令长度规定			
8.5.11 使用包含数字和字母的口令	**8.5.11** 对于样本系统组件、关键服务器和无线接入点，获得并查看系统配置设置，以检查口令参数是否被设置为要求口令必须同时包含数字和字母字符。 对于**服务供应商**，复查内部流程和客户/用户文档，以检查是否要求了客户口令必须同时包含数字和字母字符。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
8.5.12 不允许任何个人提交的新口令与其最近使用的四个口令相同。	**8.5.12** 对于样本系统组件、关键服务器和无线接入点，获得并检查系统配置设置，以确定口令参数是否被设置为禁止新口令与最近使用的口令相同。 对于**服务提供商**，审查内部流程和客户/用户文档，以确定是否禁止新的客户口令与最近使用的四个口令相同。			
8.5.13 通过锁定用户ID的方式限制连续的访问企图（最多不允许超过六次）	**8.5.13** 对于样本系统组件、关键服务器和无线接入点，获得并检查系统配置设置，以确定口令参数是否被设置为连续输入六次无效的口令后锁定用户的账户。 对于**服务提供商，**查看内部流程和客户/用户文档，以检查是否通过临时锁定客户账户的方限制连续的访问企图（最多不允许超过六次）			
8.5.14（用户ID）锁定持续时间设定为三十分钟或直至管理员为其解锁	**8.5.14** 对于 样本系统组件、关键服务器和无线接入点，获得并查看系统配置设置，以检查口令参数是否被设置为要求用户账户的锁定持续时间为三十分钟或直至管理员为其解锁			
8.5.15 如果一个会话空闲的时间超过十五分钟,要求用户再次输入口令以重新激活终端	**8.5.15** 对于样本系统组件、关键服务器和无线接入点，获得并查看系统配置设置，以检查系统/会话空闲超时被设置为15分钟或更短			
8.5.16 针对任何含有持卡人数据的数据库的访问都须经过身份认证.这些访问包括由应用、管理员和所有其他用户发起的	**8.5.16.a** 查看样本数据库的数据库配置，以检查访问是否需要经过认证，包括单个用户、应用程序或管理员进行的访问。			
	8.5.16.b 查看数据库配置设置和数据库账户，以确定是否禁止直接 SQL 查询（数据库登录账户应尽可能少，并且应只允许数据库管理员执行直接 SQL 查询）			

要求 9：限制对于持卡人数据的物理访问

任何针对含有持卡人数据的数据或系统的物理访问都应受到适当的限制， 以防止数据和设备被移除或硬拷贝。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
9.1 针对存储、处理或传输持卡人数据的系统，采用适当的场所进入控制措施，以限制和监测对上述系统的物理访问。	**9.1** 对于持卡人数据存储系统所在的计算机室、数据中心和其他物理区域，检查是否有物理安全控制措施。 • 检查是否使用了证件识读器和其他设备（包括授权证和锁钥）对访问进行控制 • 系统管理员尝试登录持卡人数据环境中三个随机选定的系统，对这个尝试操作进行监控，以确定这些系统是否被“锁定”，从而禁止未获权的使用			
9.1.1使用摄像机监视敏感区域。审计收集到的数据，并与其他入口（的数据）相关联。(数据）至少保存三个月，除非法律另作限制	**9.1.1**检验是否使用了摄像机监视存储了持卡人数据的数据中心和入口和出口。摄像机应位于数据中心内部或者采取了保护措施以避免被损坏或禁用。检查是否摄像机是否受到监控以及摄像数据是否至少保存三个月。			
9.1.2 限制对于公用网络接口的物理访问	**9.1.2** 通过与网络管理员面谈和观察，检查是否只有在授权员工需要时才启用网络接口。例如，用于招待访客的会议室不应具有支持 DHCP 的网络端口。 此外，检查访客在具有可用网络接口的区域活动时，是否全程有专人陪同。			
9.1.3限制对于无线接入点，网关和手持设备的物理访问	**9.1.3** 检查对无线接入点、网关和手持设备的物理访问是否受到了适当的限制			
9.2 开发一套流程，使得所有人员都能容易地区别员工和访客。 在可以接触到持卡人数据的区域，这一点尤为重要。 *“员工”指全职和兼职的雇员，临时雇员和常驻在该场所的顾问。*	• **9.2.a** 对流程和员工、合同商和访问客户证件分配程序进行复查，检查这些流程是否包括：新证件授予、访问更改规定和停职员工证件和到期访问证件收回等程序 • 证件系统访问限制			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
“访客”是指供应商，员工的客人，服务人员或任何需要进入该场所、并作短期（通常不超过一天）逗留的人。	**9.2.b** 观察场所内的人员，检查是否容易区分员工和访客。			
9.3 确保对所有访客按照以下方式处理：	**9.3** 检查是否实施了员工/访客控制：			
9.3.1获得授权后，方可进入处理或保存持卡人数据的区域	**9.3.1** 观察访客，以检查他们是否使用访问ID证件。尝试进入数据中心，以检查访客ID证件是否禁止在无陪同的情况下进入存储了持卡人数据的物理区域			
9.3.2 授予一个物理凭据（例如，证件或通行设备）用以区分访客和员工。 一旦超过有效期限该物理凭据即失效	**9.3.2** 检查员工和访客证件，以审核ID证件是否明确区分了员工的身份与访客/外来人士的身份以及是否标明了访客证件的有效期			
9.3.3 在离开该场所或有效期期满时被要求归还物理凭据。	**9.3.3** 观察离开场所的访客，以检查访客离开或证件到期时是否被要求归还他们的 ID 证件			
9.4 使用一个访客日志，使得访客的物理活动可审计。此记录至少保留三个月，除非法律另作限制。	**9.4.a** 检查是否使用了访客日志记录对存储或传输持卡人数据的场所、计算机室和数据中心的物理访问			
	9.4.b 检查该日志是否包含访问姓名、所代表的公司和授权物理访问的员工姓名，以及日志是否至少保留三个月。			
9.5 在一个安全的位置（最好是离场设施，比如备份站点或商业存储设施）保存备份介质。	**9.5** 检查备份介质的存储位置是否安全。检查离场存储是否受到定期检查以确定备份介质存储的物理安全性和防火性。			
9.6 对于任何含有持卡人数据的纸质和电子介质（包括计算机，电子介质，网络，硬件通信设备，通信线路，纸质收据，纸质报告和传真）进行物理安全保护。	**9.6** 检查持卡人数据保护程序是否包括计算机室和数据中心的纸质和电子介质（包括纸质收据、纸质报告、传真、CD和员工办公桌内和开放办公区的磁盘、PC硬盘驱动器等）物理安全控制。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
9.7 应严格控制任何含有持卡人数据的介质在内部或外部分发：	**9.7** 检查是否制定了相应的策略，以控制分发包含了持卡人数据的介质，并检查该策略是否覆盖所有分发的介质（包括分发给个人的介质）			
9.7.1 对这些介质进行分类，并标识为机密	**9.7.1** 检查所有介质是否被分类以便被标识为“机密”			
9.7.2 通过安全的渠道或可以被准确追查的发送方法发送介质	**9.7.2** 检查是否记录了从机构发送出去的所有介质、这些介质发送是否获得了管理层的授权以及是否通过安全的渠道或可以追查的发送方法进行发送			
9.8 确保所有介质离开安全区域前，都经过管理层批准（尤其当分发对象为个人时）	**9.8** 选择一个近期若干日的离站介质追查日志样本，检查日志内是否有追查详细记录和相应的管理层授权			
9.9 对于含有持卡人数据的介质的存储和访问，维护严格的控制。	**9.9** 获得并检查存储控制硬拷贝和电子介质维护策略，检查此策略是否要求定期库存介质。			
9.9.1 正确库存所有介质并确保存储安全性	**9.9.1.a** 获得并查看介质库存日志，以检查是否执行了定期介质库存 **9.9.1.b** 对流程进行复查，以检查介质存储是否安全			
9.10 含有持卡人数据的介质，当业务不再需要或法律不再要求时，按照以下方式进行销毁：	**9.10** 获得并检查定期介质销毁策略，以检查它是否覆盖所有存储持卡人数据的介质并确认以下事项：			
9.10.1 粉碎，焚毁或送纸浆厂销毁	**9.10.1.a** 检查是否根据ISO 9564-1或ISO 11568-3e标准对硬拷贝材料进行了粉碎、焚毁或送纸浆厂销毁			
	9.10.1.b 检查将要被销毁的信息存储容器，确定容器的安全性。例如，检查是否禁止查看“将要被粉碎”的容器中的内容			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
9.10.2 清除、消磁、粉碎或以其他方式销毁磁介质，使得持卡人数据无法被重建	**9.10.2** 检查是否使用军用销毁程序销毁了电子介质或通过消磁或其他物理方式销毁了介质，使数据无法被重建			

定期监控和测试网络

要求 10：追踪并监控对网络资源和持卡人数据的所有访问

日志机制和追踪用户活动的能力至关重要。在所有环境中使用日志机制， 以追踪和分析可能出现的不正常情况或错误。离开了系统活动日志，很难确定有害事件的原因。

PCI DSS 要求	测试程序	现场	未实施	目标日期/备注
10.1 建立一个流程，将针对所有系统组件的访问与每个用户个体联系起来。尤其是具有管理员权限的访问，例如，root。	**10.1** 通过观察和面晤系统管理员，确定审计跟踪功能是否已启用并且运行正常，包括针对连接的无线网络的审计跟踪			
10.2 对所有系统组件实施自动的审计跟踪，以记录下列事件：	**10.2** 通过访谈和检查审计日志及审计日志设置，确定是否在系统活动日志中记录了以下事件			
10.2.1 所有用户个体对持卡人数据的访问	**10.2.1** 所有用户个体对持卡人数据的访问			
10.2.2 以root或管理员权限进行的所有操作	**10.2.2** 以root或管理员权限进行的所有操作			
10.2.3 对任何审计记录的访问	**10.2.3** 对任何审计记录的访问			
10.2.4 无效的逻辑访问尝试	**10.2.4** 无效的逻辑访问尝试			
10.2 5（身份）鉴别和认证机制的使用	**10.2 5**（身份）鉴别和认证机制的使用			
10.2.6 对审计日志的初始化操作	**10.2.6** 对审计日志的初始化操作			
10.2.7 系统层对象的创建和删除操作	**10.2.7** 系统层对象的创建和删除操作			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
10.3 针对所有系统组件的所有事件，至少保存以下审计记录条目：	**10.3** 通过访谈和观察，对于每个可审计事件（10.2 中的事件），检查审计记录是否包括以下条目：			
10.3.1 用户ID	**10.3.1** 用户ID			
10.3.2 事件类型	**10.3.2** 事件类型			
10.3.3 日期和时间	**10.3.3** 日期和时间戳			
10.3.4 成功或失败标记	**10.3.4** 成功或失败标记，包括无线连接成功或失败标记			
10.3.5 事件源	**10.3.5** 事件源			
10.3.6 受影响的数据，系统组件或资源的 ID 或名称	**10.3.6** 受影响的数据，系统组件或资源的ID或名称			
10.4 同步所有关键系统的时钟	**10.4** 获得并检查组织内的正确时间捕获和发送流程以及样本系统组件、关键服务器和无线接入点的时间相关系统参数设置。检查流程中是否包含并且实施了时间同步过程：			
	10.4.a 检查是否使用了NTP或类似技术进行时间同步			
	10.4.b 检查内部服务器是否始终接收外部时间源的时间信号。[组织内的两个或三个中央时间服务器接收外部时间信号[直接从专用无线电、GPS卫星或其他基于国际原子时间和 UTC（以前的 GMT）的时间源接收时间信号]，它们相互协调以保持时间的准确性，并且与其他内部服务器共享时间。]			
	10.4.c 检查运行的网络时间协议（NTP）是否为最新版本			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
	10.4.d 检查是否指定了专用的外部主机 – 时间服务器将这个主机接收最新的时间（以防止攻击者更改时间）。此外，还可以使用对称密钥对时间更新进行加密。另外，还可以创建一个访问控制列表，这个列表指定了将获得NTP 服务的客户端设备的IP地址（以防止在未获授权的情况下使用内部时间服务器）。有关详细信息，请访问 www.ntp.org。			
10.5 保护审计追踪记录，以防被更改	**10.5** 与系统管理员面谈，并检查审计追踪记录，以确定审计追踪记录是安全的，而且无法被修改，方法如下：			
10.5.1 只允许具有工作需要的人员查看审计追踪记录	**10.5.1** 检查是否仅允许有工作需要的人员查看审计追踪记录			
10.5.2 保护审计追踪记录以防被非授权更改	**10.5.2** 检查是否通过访问控制机制、物理隔离和/或网络隔离对审计记录进行保护，以防目未经授权的修改			
10.5.3 将审计追踪记录即时备份到到集中的日志服务器上或难以更改的介质上.	**10.5.3** 检查当前的审计追踪记录是否被即时备份到到集中的日志服务器上或难以更改的介质上			
10.5.4 将无线网络的日志复制到一台位于内部局域网的日志服务器上	**10.5.4** 检查是否将无线网络的日志复制到了一台位于内部局域网的日志服务器上			
10.5.5 使用文件完整性监视和变更检测软件保护日志，确保已有的日志被改变时产生报警（当然，在已有的日志中添加数据，不应触发报警）	**10.5.5** 检查是否使用了文件完整性监视和变更检测软件保护日志，确保已有的日志被改变时产生报警			
10.6 至少每天复审所有系统的日志。日志复审必须包含那些执行安全功能的服务器，类如入侵检测（IDS）、身份验证、授权和记账协议（AAA）服务器（例如，RADIUS）。 注：日志采集，分析和报警工具可以被用来实现遵从“要求10.6”	**10.6.a** 检查是否至少每天复审所有系统的日志。日志复审必须覆盖那些执行安全功能的服务器。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
	10.6.b 通过观察和访问相关人员，检查是否对所有系统组件进行了定期日志审查			
10.7 至少保持一年的审计追踪记录，其中至少三个月的内容可被联机访问。	**10.7.a** 获得并检查安全策略和程序，确定它们是否包含审计日志保留策略并要求审计日志至少保留一年			
	10.7.b 检查是否可以联机访问审计日志或者至少在磁带上存储一年			

要求 11：定期测试安全系统和流程

新的弱点正不断地被黑客和研究者发现，并随着新的软件被引入。
系统、流程和定制软件应接受经常性的测试，以保证安全性不会因时间或软件变更的原因受到削弱。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
11.1 每年对安全控制措施、网络连接和限制措施进行测试，以确保具备充分的识别和阻止非授权访问的能力。 至少每季度使用无线分析工具识别所有使用中的无线设备。	**11.1.a** 通过与安全人员面谈和检查相关代码、文档和流程，确认是否对设备进行了安全测试，以确保控制方法能够识别并阻止持卡人环境内的非授权访问企图。			
	11.1.b 检查是否每季度使用一次无线分析工具识别所有无线设备。			
11.2 内部和外部网络弱点扫描至少每季度一次，在网络发生重大变更（例如，安装了新的系统组件，网络拓扑发生变化，防火墙配置变更，产品升级）后亦需执行。	**11.2.a** 检查最近四个季度的网络、主机和应用弱点扫描输出结果，以确认是否对持卡人环境中的设备进行了定期的安全性测试。 检查扫描过程是否包含重扫描以获得“干净”的结果。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
注：每季度的外部弱点扫描必须交由经过支付卡行业资格认定的扫描服务商执行。网络变更后的扫描可由组织内部人员执行。	**11.2.b** 检查是否根据PCI安全扫描程序以每季度一次的频率进行了外部扫描，查看最近四个季度的外部弱点扫描结果，以检查： • 最近的12个月是否每季度进行了一次扫描 • 每次扫描的结果是否符合PCI安全扫描程序的要求（例如，未发现紧迫、关键和重大的弱点） • 扫描是否由获准执行PCI安全扫描程序的扫描服务商完成			
11.3 渗透测试至少每年执行一次，基础设施或应用完成重大的升级或调整（例如，操作系统升级，环境中增加了一个子网或增加了一台Web服务器）后亦需执行。 渗透测试必须包含以下内容：	**11.3** 获得并检查最近的渗透测试结果，以确认渗透测试是否至少每年执行一次而且在环境重大调整后也进行了测试。检查是否修正了已发现的弱点。检查渗透测试是否包含以下内容：			
11.3.1 网络层渗透测试	**11.3.1** 网络层渗透测试			
11.3.2 应用层渗透测试	**11.3.2** 应用层渗透测试			
11.4 采用网络入侵检测系统、主机入侵检测系统和入侵防护系统监视所有网络通信，并向相关人员发出可疑事件警报。所有入侵检测和防护引擎应及时更新。	**11.4.a** 检查网络入侵检测系统和/或入侵防护系统在网络上的使用情况。确认持卡人数据环境中的所有关键网络流量是否都受到了监控。			
	11.4.b 确认是否部署了IDS 和/或IPS以监控可疑事件和向相关人员发送可疑事件警。			
	11.4.c 检查IDS/IPS配置并确认是否根据供应商的指导对IDS/IPS设备进行了配置、维护和更新以确保最佳的防护效果。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
11.5 部署文件完整性监控软件，一旦关键系统或文件被非授权更改，及时通知相关人员；并配置该软件至少每周对关键文件进行比较。 *关键文件不仅限于那些含有持卡人数据的文件。根据文件完整性监控目的，关键文件通常指那些不经常变化，它的变化可能意味着系统安全面临被破坏的危险。* *文件完整性监控产品的初始配置通常根据相关的操作系统类型设定关键文件。其他关键文件，例如定制应用的关键文件，必须由组织（此处特指商家或服务提供商）进行评估和定义。*	**11.5** 通过查看系统设置、受监控的文件和监控活动的输出结果，检查持卡人数据环境内的文件完整性监控产品的使用情况。			

维护一个信息安全策略

要求 12：维护一个策略用以向员工和合同商传达信息安全

强有力的安全策略为整个组织设定了重视安全的氛围，并向员工传达了组织对他们的期望。所有员工都应洞悉数据的敏感性和他们承担的保护责任。

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
12.1 建立、发布、维护和宣传一个安全策略以实现以下目的：	**12.1** 检查信息安全策略，确保此策略已经发布并且被呈送给所有相关的系统用户（包括供应商、合同商和商业合作伙伴）			
12.1.1 阐述本规约中的所有要求	**12.1.1** 检查策略是否阐述了本规约中的所有要求。			
12.1.2 包含一个每年执行的流程，以鉴别风险和弱点并据此进行正式风险评估	**12.1.2** 检查信息安全策略是否包含一个用于鉴别风险和弱点并据此进行正式风险评估的信息安全策略 。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
12.1.3 安全策略至少每年评审一次，并根据环境变化而更新	**12.1.3** 检查信息安全策略是否至少每年评审一次并且更根据业务目标和环境变化而更新			
12.2 开发与本规约要求相一致的日常操作安全程序（例如，用户账号维护程序，日志审核程序）。	**12.2.a** 检查日常操作安全程序。确定它们是否与本规约相一致，而且针对每条要求制定了相应的管理和技术程序。			
12.3 开发面向员工的关键技术（例如，调制解调器和无线网络）使用策略。策略定义了所有员工和签约方对此类技术的适当使用。确保使用策略包含以下内容：	**12.3** 获得并检查面向员工的关键技术，确定策略是否包含以下内容：			
12.3.1 管理层的明确批准	**12.3.1** 检查使用策略是否要求必须获得管理层的明确批准才能使用设备。			
12.3.2 此类技术的使用身份认证	**12.3.2** 检查使用策略是否要求使用任何设备都必须通过用户名和口令或其他认证方法（如令牌） 进行身份认证			
12.3.3 此类设备和具有使用权限的人员列表	**12.3.3** 检查使用策略是否要求提供一个所有设备和具有权限的人员列表。			
12.3.4 设备贴上标签规则，据此标示所有人、联系信息和用途	**12.3.4** 检查使用策略是否要求对设备贴标，以标示所有人、联系信息和用途。			
12.3.5 此类技术的可接受用途	**12.3.5** 检查使用策略是否要求技术仅用于可接受的用途。			
12.3.6 此类技术可接受的网络位置	**12.3.6** 检查使用策略是否要求只能在可接受的网络位置使用技术。			
12.3.7 受组织认可的产品列表	**12.3.7** 检查使用策略是否要求提供一个受组织认可的产品列表。			
12.3.8 调制解调器会话超过特定的空闲状态时间后，自动断开连接	**12.3.8** 检查使用策略是否要求在调制解调器会话超过特定的空闲状态时间后自动断开连接。			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
12.3.9 仅在供应商需要时为供应商激活调制解调器，使用完毕后立即断开	**12.3.9** 检查是否仅在供应商需要时为供应商激活调制解调器并且在使用完毕后立即断开			
12.3.10 通过调制解调器远程访问持卡人数据时，禁止在本地硬盘、软盘或其它外部介质上存储持卡人数据。禁止在远程访问中使用剪切、粘贴和打印功能	**12.3.10** 检查使用策略是否禁止在本地硬盘、软盘或其它外部介质上存储持卡人数据。检查使用策略是否禁止在远程访问中使用剪切、粘贴和打印功能			
12.4 确保安全策略和程序明确定义了所有员工和合同商的信息安全责任。	**12.4** 检查信息安全策略是否明确定义了所有员工和合同商的信息安全责任。			
12.5 将下列信息安全管理责任分配给一名个人或一个团队：	**12.5** 检查首席安全官或其他安全管理人员的信息安全职责。获得并检查信息安全策略和程序，确定是否正式规定了以下信息安全职责：			
12.5.1 建立、文档化并分发安全策略和程序	**12.5.1** 检查是否正式规定了安全策略和程序创建和分发职责			
12.5.2 监控并分析安全报警和信息，并分发至适当的人员	**12.5.2** 检查是否正式规定了安全报警分析和信息监控职责			
12.5.3 建立、文档化并分发安全事件响应和升级程序，以保证及时、有效地处理各种情况	**12.5.3** 检查是否正式规定了建立、文档化并分发安全事件响应和升级程序			
12.5.4 添加、删除和修改管理员账户	**12.5.4** 检查是否正式规定了用户账户的管理和身份认证管理职责			

PCI DSS 要求	测试程序	未实施	已实施	目标日期/备注
12.5.5 监控对数据的所有访问	**12.5.5** 检查是否正式规定了所有数据访问监控责任			
12.6 实施一套安全意识宣传程序以使所有员工洞悉保护持卡人数据安全的重要性：	12.6.a 检查是否制定了正式的安全意识宣传计划			
	12.6.b 获得并检查安全意识宣传计划和文档，并执行以下检查			
12.6.1 雇用员工时为其提供培训，并且至少每年一次。	**12.6.1.a** 检查是否通过多种方法进行安全意识宣传和员工培训（例如，海报、信函和会议等）			
	12.6.1.b 检查员工上岗前是否接受了安全意识会培训，并且至每年接受一次培训			
12.6.2 要求员工提交签字确认（书）以表明他已经阅读并理解了组织的安全策略和流程	**12.6.2** 检查是否要求员工提交签字确认（书）以表明他已经阅读并理解了组织的安全策略和流程			
12.7 对待聘员工进行筛选，将内部攻击的风险降至最低。 *对于像商店出纳员一类只有在处理业务时才能查看到卡号的员工，要求他们必须有推荐信。*	**12.7** 询问人力资源部门管理人员，检查是否对待聘员工进行背景考虑，如果这些待聘员工上岗后可以接触持卡人数据或持卡人数据环境。（背景考察的例子包括聘前犯罪记录、信用历史记录和参考材料检查）			
12.8 如果与服务提供商共享持卡人数据，则必须在合约中注明以下要求：	**12.8** 如果接受审计的实体与其他组织共享持卡人数据，获得并检查组织与处理持卡人数据的第三方（例如，备份磁带存储机构、受管服务提供商（如 Web 主机服务商或安全服务商）或使用持卡人数据进行欺诈建模的机构）之间签署的合约。执行以下检查步骤：			
12.8.1 服务提供商必须遵守PCI DSS的要求规定	**12.8.1** 检查合约是否要求第三方必须遵守PCI DSS的要求规定			

PCI DSS 要求	测试程序	已实施	未实施	目标日期/备注
12.8.2 提供商应在协议中承诺对其所处理的持卡人数据的安全负有责任	**12.8.2** 检查合约是否要求第三方承诺对其所处理的持卡人数据的安全负有责任。			
12.9 实施执行一套事件响应计划。随时准备对系统破坏作出快速响应。	**12.9** 获得并检查突发事件响应计划和相关程序，检查步骤如下：			
12.9.1 创建事件响应计划，当系统破坏情况发生时遵照执行确保此计划至少阐明：明确的事件响应流程，业务恢复和连续性流程，数据备份流程，角色和职责，通讯和联系策略（例如，通知收单行和信用卡组织）	**12.9.1** 检查突发事件响应计划和相关程序是否包含以下内容： □明确的角色和职责划分和通讯策略，以应对破坏事件 □ 覆盖和响应所有的关键系统组件 □ 通知方案，至少应通知信用卡组织和收单行 □ 确保避免受到破坏事件影响的业务连续性策略 □ 引用和包含信用卡组织的事件响应程序 □ 破坏事件报告法律要求分析（例如，根据加州法案1386的规定，对于为加州居民提供的任何业务，如果实际发生或可能发生破坏事件，必须通知受影响的消费者。			
12.9.2 至少每年测试此计划一次	**12.9.2** 检查计划是否至少每年测试一次			
12.9.3 指派具体的人员提供24*7 小时报警响应	**12.9.3** 通过查看和评审查策略，检查是否制定了覆盖任何未授权活动证据、关键IDS报警和/或未授权关键系统或文件内容变化的24*7事件响应和监控机制。			
12.9.4 为负责响应安全违规事件的人员提供适当的培训	**12.9.4** 通过查看和评审策略，检查安全违规事件责任人员是否定期接受了培训。			

PCI DSS 要求	测试程序	现场	未实施	目标日期/备注
12.9.5 覆盖入侵检测系统、入侵防护系统和文件完整性监控系统发出的报警	**12.9.5** 通过查看和评审策略，检查事件响应计划中是否包含了安全系统报警监控和响应机制。			
12.9.6 结合已有的教训和行业的发展，开发事件响应计划变更和优化流程	**12.9.6** 通过查看和评审策略，检查是否制定了一个流程，以结合已有的教训和行业的发展修改和升级事件响应计划			
12.10 所有的处理机构和服务提供商必须维护并贯彻策略和流程以管理已连接的实体，包括下列内容：	**12.10** 通过查看和评审策略、流程和支持文档，检查是否制定了一个流程来管理已连接的实体，检查步骤如下：			
12.10.1 维护一个已建立连接的实体列表	**12.10.1** 检查是否维护了一个已连接的实体列表			
12.10.2 确保连接一个实体之前进行了例行审查	**12.10.2** 确保连接一个实体之前进行了例行审查			
12.10.3 确保实体符合PCI DSS要求	**12.10.3** 检查该流程是否确保实体符合PCI DSS要求。			
12.10.4 应按照已建立的流程建立和断开与一个实体之间的连接	**12.10.4** 检查是否按照已制定的流程建立或断开与一个实体之间的连接			

附录 A：PCI DSS 对于主机服务商的适用性（及测试程序）

要求 A1: 主机服务商保护持卡人数据环境

如“要求 12.8”中的引用所述，所有具有持卡人数据访问权限的服务提供商（包括主机服商）必须遵守 PCI DSS 要求规定。
另外，“要求2.4”规定主机服务商必须保护每一个组织的主机环境和数据。
因此，主机服务商必须对下列内容予以特别的考虑：

要求	测试程序	已实施	未实施	目标日期/备注
A.1 按照A.1.1 至A.1.4 的要求，保护各实体（指商家，服务提供商或其它实体）的主机环境和数据：除上述要求外，主机服务商也必须满足 PCI DSS 其它章节的要求。 *注：即使主机服务商满足合规性要求，也不能保证接受其主机服务的实体同样具有合规性。任何标准适用范围内的组织都必须符合PCI DSS，并验证其合规性。*	A.1 对于针对**共享主机服务商**的PCI审计，检查**共享主机服务商**是否为实体（商家和服务提供商）的主机环境和数据提供了保护，从具有代性的使用主机服务的商家和服务提供商样本中，选择一个样本服务器（Microsoft Windows 和 Unix/Linux），检查 **A.1.1 – A.1.4**，如下所述：			
A.1.1 确保各组织只能访问自身的持卡人数据环境。	**A.1.1** 如果共享主机服务商允许实体（例如，商家或服务提供商）运行它们自己的应用，使用实体的唯一ID检查这些应用流程的运行情况。例如检查： • 是否禁止系统上的任何实体使用共享的Web服务器用户ID • 是否必须通过实体的唯一用户ID创建和运行实体所使用的所有CGI脚本			
A.1.2 限制每个实体的访问和权限，使之仅能访问自有的持卡人数据	**A.1.2.a** 确认应用流程的用户ID不是特权用户（root/admin）。			

要求	测试程序	已实施	未实施	目标日期/备注
	A.1.2.b 检查是否仅允许实体（商家、服务提供商）写入、读取或执行它自己的文件和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、jailshell 等进行限制）。重要需知：不允许共享实体的文件			
	A.1.2.c 检查实体的用户是否无权对共享的系统二进制文件执行写入操作。			
	A.1.2.d 检查是否仅允许实体查看自己的日志			
	A.1.2.e 为了确保禁止一个实体独占服务器资源而利用弱点（错误、记录、重启条件和产生的缓存溢出），检查是否对以下系统资源的使用进行了限制： • 磁盘空间 • 宽带 • 内存 • CPU			
A.1.3 确保每个组织的持卡人数据环境的日志和审计追踪功能是独立的、已被激活的，并与PCI DSS“要求10”保持一致。	**A.1.3.a** 检查共享主机服务商是否为每个商家和服务提供商启用了日志功能，包括： • 是否支持通用第三方应用的日志功能 • 默认情况下是否激活了日志功能 • 是否允许实体查看它们的日志 • 是否明确地向实体通告了它们的日志所在的位置			
A.1.4 当任何接受主机服务的商家或服务提供商受到危害时，及时启动相应的取证**调查流程。**	**A.1.4** 检查共享主机服务商是否制定了相关的策略，并在发生破坏事件时及时地提供对相关服务器进行调查取证。			

附录 B – 补偿控制

补偿控制 – 概要

对于大多数PCI DSS要求，当组织无法满足某要求的技术规范时，通常可以考虑补偿措施，但是补偿措施也带来相关的风险。有关补偿措施的完整定义，请参阅PCI DSS术语。

补偿措施的有效性依赖于它的实施环境、周边安全控制和本身配置的具体情况。各组织应意识到特定的补偿措施无法在各种环境中都具有效力。每个补偿措施在实施后必须经过彻底的评估以确保其有效性。组织无法采用不可读的形式呈递持卡人数据时，可根据以下指导实施补偿措施以对应“要求 3.4”的控制要求。

要求3.4 的补偿措施

于因技术性约束或业务限制而无法采用不可读方式（例如，采用加密）呈递持卡人数据的组织，可以考虑补偿措施。*组织只有在进行了风险分析并采用合理的技术或文档化的业务限制，方可考虑借助于补偿措施实现符合性。*

考虑采用补偿措施呈递持卡人数据的组织必须理解以可读形式保存的持卡人数据所带来的风险。通常，补偿措施必须提供附加的保护，以降低持卡人数据以可读形式保存所带来的额外风险。补偿措施必须是PCI DSS要求以外的、符合满足PCI DSS术语表中关于“补偿措施”的定义。补偿措施可由一个或多个设备/应用/控制措施组合而成，这些设备/应用/控制措施**必须满足以下所有条件：**

1. 提供附加的分割/抽象（例如，在网络层）。
2. 提供基于以下条件对持卡人数据或数据库进行访问控制的能力：
   - IP地址/MAC地址
   - 应用/服务
   - 用户账号/组
   - 数据类型（包过滤）
3. 限制对于数据库的逻辑访问
   - 对数据库逻辑访问的控制，独立于活动目录（微软Active Directory）或轻量目录访问协议（LDAP）
4. 预防/检测针对通用应用软件或数据库攻击（例如，SQL注入攻击）。

附录 C：补偿控制备忘录/完整示例

示例

1. 限制情况：列出原始要求合规受限情况

公司XYZ部署了无LDAP的独立Unix服务器。公司的每个员工都要以‘root’权限登录。公司XYZ无法管理‘root’登录，也不能记录每个用户的所有‘root’活动

2. 目的：说明原始控制措施的目的；阐明补偿措施可以达到哪些目的

原始控制要求使用唯一的用户名登录，这具有双重目的。首先，从安全角度来看，共享登录凭据是不可接受的。其次，共享登录凭据使我们无法确定哪个人员应对一项具体的操作负责。

3. 已发现的风险：说明未执行原始控制而可能带来的其他风险

由于不能确保所有用户都具有唯一的ID，而且无法对用户进行追查，因此可能给访问控制系统带来额外的风险。

4. 补偿措施定义：定义补偿措施并阐述它们如何达到与原始控制措施相同的目的，以及带来的风险（如果有）。

公司XYZ计划要求所有员工在他们的计算机上使用SU命令登录服务器。SU 允许用户以‘root’账户登录并在‘root’账户下执行操作，而且能够在su-log子目录下记录用户的操作。这样，就可以通过SU账户追查每个用户的操作。