一、 PCI DSS 标准介绍

支付卡行业(Payment Card Industry (PCI))数据安全标准 （Data Security Standard (DSS)） 是一组全面的要求，旨在确保持卡人的信用卡和借记卡信息保持安全，而不管这些信息是在何处以何种方法收集、处理、传输和存储。

PCI DSS 由 PCI 安全标准委员会的创始成员（包括 American Express、Discover Financial Services、JCB、MasterCard Worldwide 和 Visa International）制定，旨在鼓励国际上采用一致的数据安全措施。

PCI DSS 中的要求是针对在日常运营期间需要处理持卡人数据的公司和机构提出的。具体而言，PCI DSS 对在整个营业日中处理持卡人数据的金融机构、贸易商和服务提供商提出了要求。PCI DSS 包括有关安全管理、策略、过程、网络体系结构、软件设计的要求的列表，以及用来保护持卡人数据的其他措施。

二、 PCI-DSS 要求范围

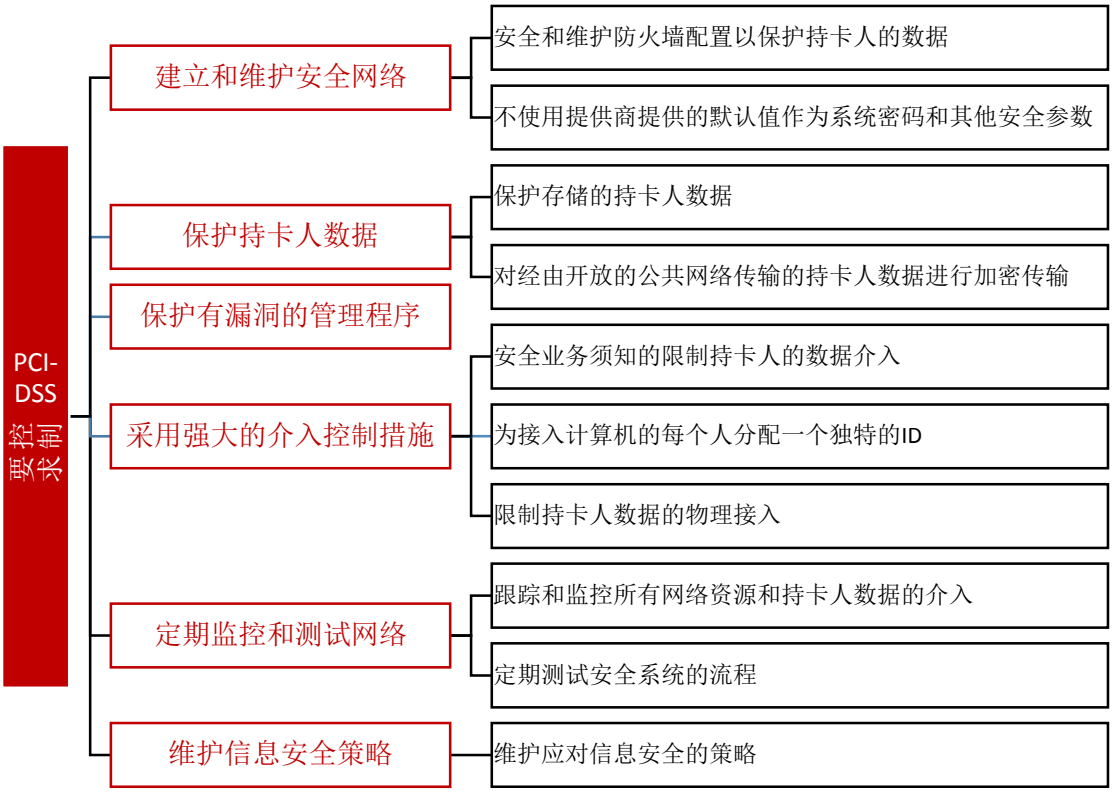
PCI-DSS 安全要求适用于持卡人数据环境中包含或与之连接的所有系统组件。持卡人数据环境（CDE）包含存储、处理或传输持卡人数据或敏感验证数据的人员、流程和技术。系统组件包括网络设备、服务器、计算设备和应用程序，系统组件包括但不限于：

- 提供安全服务、方便分段或可能影响 CDE 安全性的系统；
- 虚拟化组件，例如虚拟机、虚拟交换机/路由器、虚拟设备、虚拟应用该程序/桌面和虚拟机监控程序。
- 网络组件，包括但不限于防火墙、交换机、路由器、无线接入点、网络设备和其他安全设备；
- 服务器类型，包括但不限于 WEB、应用程序、数据库、验证、邮件、代理、网络事件协议（NTP）和域名系统（DNS）；
- 应用程序，包括所有购买和自定义的应用程序以及内部和外部应用程序；
- 位于 CDE 内或连接到 CDE 的任何其他组件或设备；

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

三、 PCI-DSS 控制要求

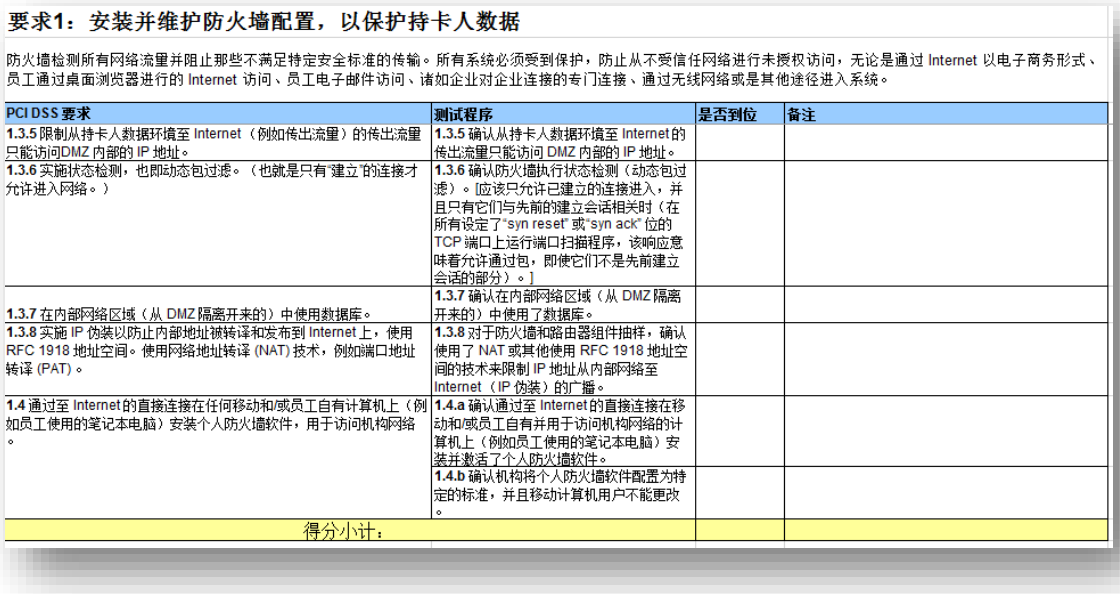
PCI DSS 包括 6 个控制域，12 个控制目标，对支付卡行业中持卡人数据的存储、处理、传输等过程进行严格控制，以保护持卡人数据信息不被泄露：



四、PCI-DSS 实施方法

安言咨询为企业根据 PCI-DSS 标准要求，在管理制度方面，主要通过审查 PCI-DSS 制度的形式进行，调阅了企业相关的制度文件度，审核信息安全方针策略、网络和系统的安全、物理与环境安全、信息安全组织和人员等方面的制度的内容，并通过内审等活动对制度的执行情况进行了检查和验证。在技术层面，为企业定位在业务的应用，根据网络和业务系统的具体安全运行维护技术工作执行和有效性层面进行的技术测试和评估。

五、 PCI-DSS 实施工具示例



要求1：安装并维护防火墙配置，以保护持卡人数据

防火墙检测所有网络流量并阻止那些不满足特定安全标准的传输。所有系统必须受到保护，防止从不受信任网络进行未授权访问，无论是通过 Internet 以电子商务形式、员工通过桌面浏览器进行的 Internet 访问、员工电子邮件访问、诸如企业对企业连接的专门连接、通过无线网络或是其他途径进入系统。

PCI DSS 要求	测试程序	是否到位	备注
1.3.5 限制从持卡人数据环境至 Internet（例如传出流量）的传出流量只能访问DMZ 内部的 IP 地址。	**1.3.5** 确认从持卡人数据环境至 Internet 的传出流量只能访问 DMZ 内部的 IP 地址。		
1.3.6 实施状态检测，也即动态包过滤。（也就是只有"建立"的连接才允许进入网络。）	**1.3.6** 确认防火墙执行状态检测（动态包过滤）。[应该只允许已建立的连接进入，并且只有它们与先前的建立会话相关时（在所有设定了"syn reset"或"syn ack"位的 TCP 端口上运行端口扫描程序，该响应意味着允许通过包，即使它们不是先前建立会话的部分）。]		
1.3.7 在内部网络区域（从 DMZ 隔离开来的）中使用数据库。	**1.3.7** 确认在内部网络区域（从 DMZ 隔离开来的）中使用了数据库。		
1.3.8 实施 IP 伪装以防止内部地址被转译和发布到 Internet 上，使用 RFC 1918 地址空间。使用网络地址转译 (NAT) 技术，例如端口地址转译 (PAT)。	**1.3.8** 对于防火墙和路由器组件抽样，确认使用了 NAT 或其他使用 RFC 1918 地址空间的技术来限制 IP 地址从内部网络至 Internet（IP 伪装）的广播。		
1.4 通过至 Internet 的直接连接在任何移动和/或员工自有计算机上（例如员工使用的笔记本电脑）安装个人防火墙软件，用于访问机构网络。	**1.4.a** 确认通过至 Internet 的直接连接在移动和/或员工自有并用于访问机构网络的计算机上（例如员工使用的笔记本电脑）安装并激活了个人防火墙软件。		
	1.4.b 确认机构将个人防火墙软件配置为特定的标准，并且移动计算机用户不能更改。		
得分小计：			

PCI-DSS 安全评估工具-防火墙管理评估