支付卡行业 **(PCI)**

数据安全标准

适用于商户的自我评估调查问卷 D
和遵从性证明书

其他所有符合 SAQ 适用条件的商户

适用于 PCI DSS 3.2 版

修订版 1.1

2017 年 1 月

文档变更记录

日期	PCI DSS 版本	SAQ 修订版	描述
2008 年 10 月	1.2		根据新的 PCI DSS 1.2 版调整内容并实施原始 1.1 版中标出的微小变更。
2010 年 10 月	2.0		根据新的 PCI DSS 2.0 版要求与测试程序调整内容。
2014 年 2 月	3.0		根据 PCI DSS 3.0 版要求与测试程序调整内容并纳入了其他应对方案。
2015 年 4 月	3.1		更新以符合 PCI DSS 3.1 版。有关 PCI DSS 变更的详细信息，请参阅*"PCI DSS – PCI DSS 3.0 版到 3.1 版的变更汇总"*。
2015 年 7 月	3.1	1.1	更新以在 2015 年 6 月 30 日前将参考部分移至"最优方法"，并针对要求 11.3 移除 PCI DSS 2 版报告选项。
2016 年 4 月	3.2	1.0	更新以符合 PCI DSS 3.2 版。有关 PCI DSS 变更的详细信息，请参阅*"PCI DSS – PCI DSS 3.1 版到 3.2 版的变更汇总"*。
2017 年 1 月	3.2	1.1	已更新版本编号，以便与其他 SAQ 保持一致

确认通知：

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

目录

开始之前

适用于商户的 SAQ D 适用于符合 SAQ 条件且不满足其他任何类型 SAQ 标准的商户。可使用 SAQ D 的商户环境可能包括但不限于：

- 在自己网站上接受持卡人数据的电子商务商户
- 以电子方式存储持卡人数据的商户
- 未以电子方式存储持卡人数据但不满足其他类型 SAQ 标准的商户
- 其环境可能满足其他类型 SAQ 标准但受到其他 PCI DSS 要求限制的商户

由于许多完成 SAQ D 的组织需要认证其对于每项 PCI DSS 要求的遵从性，因此一些具有特定业务模式的组织可能会发现某些要求不适用。有关要排除的某些特定要求，请参见下面的相关指南。

PCI DSS 自我评估实施步骤

1. 识别适用于您所在环境的 SAQ – 有关详情，请参见 PCI SSC 网站上的*自我评估调查问卷说明和指南*文档。
2. 确认您所在环境范围适当且满足您所使用的 SAQ 的适用标准。
3. 评估您所在环境是否遵从 PCI DSS 要求。
4. 实施此文档的所有章节：
   - 第 1 节（AOC 的第 1、2 部分）– 评估信息和实施概要。
   - 第 2 节 – PCI DSS 自我评估调查问卷 (SAQ D)
   - 第 3 节（AOC 的第 3、4 部分）– 认证和证明书详情以及针对未遵从要求的行动计划（如果适用）
5. 向收单机构、支付品牌或其他申请机构提交 SAQ、遵从性证明书 (AOC) 以及其他任何要求的文档（例如 ASV 扫描报告）。

了解自我评估调查问卷

此自我评估调查问卷中“PCI DSS 问题”列所包含的问题基于 PCI DSS 中的要求。

为帮助完成评估流程，已提供了就 PCI DSS 要求和如何完成自我评估调查问卷予以指导的其他资源。下面概述了其中的一些资源：

文档	内容：
PCI DSS *（PCI 数据安全标准要求和安全评估程序）*	• 有关范围界定的指导 • 有关所有 PCI DSS 要求意图的指导 • 测试程序详情 • 有关补偿性控制的指导
SAQ 说明和指南文档	• 所有 SAQ 及其适用标准的相关信息 • 如何确定哪项 SAQ 适用于您所在组织
PCI DSS 和 PA-DSS 术语、缩略词和首字母缩略词词汇表	• PCI DSS 和自我评估调查问卷中所使用的术语的说明和定义

上述资源和一些其他资源可在 PCI SSC 网站 *(www.pcisecuritystandards.org)* 上找到。建议组织在开始评估之前先浏览 PCI DSS 和其他支持文档。

预期测试

"预期测试"列中包含的说明基于 PCI DSS 中的测试程序，提供了有关认证已满足要求所必须执行的测试活动类型的高级说明。有关针对各项要求的测试程序的完整详情，请参见 PCI DSS。

完成自我评估调查问卷

对于每个问题，可以选择一个回复选项来表明您所在公司针对该要求的状态。***对于每个问题，只能选择一个回复。***

下表说明了各项回复的含义：

回复	此回复的适用情况：
是	已执行预期测试，且已按照相关说明满足该要求的所有元素。
是，已填写 CCW （补偿性控制工作表）	已执行预期测试，且已采用补偿性控制满足该要求。 如果选择此列中的回复，则必须在 SAQ 附录 B 中填写补偿性控制工作表 (CCW)。 要了解如何使用补偿性控制和填写该工作表，请参见 PCI DSS。
否	该要求的部分或所有元素尚未满足或正处于实施状态，或者需要进一步测试才能确定是否满足。
N/A （不适用）	该要求不适用于相关组织所在环境。（有关示例，参见下面的*某些特定要求的不适用性指南*。） 如果选择此列中的回复，则必须在 SAQ 附录 C 中提供支持说明。
未测试	该要求未包含在本次评估的考虑范围内，且未以任何形式进行测试。（有关此选项的适用情况示例，参见下面的*不适用和未测试之间的区别说明*。） 如果选择此列中的回复，则必须在 SAQ 附录 D 中提供支持说明。

某些特定要求的不适用性指南

由于许多完成 SAQ D 的组织需要认证其对于每项 PCI DSS 要求的遵从性，因此一些具有特定业务模式的组织可能会发现某些要求不适用。举例来说，如果一家公司在任何方面都不使用无线技术，则无需认证对于特定于管理无线技术的 PCI DSS 章节的遵从性。同样地，从未以电子方式存储任何持卡人数据的组织无需认证对有关安全存储持卡人数据的要求的遵从性（有关示例，参见第 3.4 条要求）。

具有特定适用性的要求包括：

- 除非您的网络中使用了无线技术，否则无需回答针对安全无线技术的问题（例如要求 1.2.3、2.1.1 和 4.1.1）。请注意，即使您的网络中未使用无线技术，也仍必须针对要求 11.1（使用流程识别未经授权的无线接入点）提供回复，因为该流程可检测出任何可能在您不知情的情况下添加的欺诈或无授权设备。
- 除非您所在组织开发了专有自定义应用程序，否则无需回答特定于应用程序开发和安全编码的问题（要求 6.3 和 6.5）。

- 除非是对于位于“敏感区域”（定义如下）的设施，否则无需回答针对要求 9.1.1 和 9.3 的问题：“敏感区域”指任何数据中心、服务器室或任何存储、处理或传输持卡人数据的系统所在区域。这不包括仅有销售点终端的区域（例如零售店的收银区），但包括存储持卡人数据的零售店后端办公服务器室以及存储了大量持卡人数据的区域。

如果您认为任何要求不适用于您所在环境，请针对该特定要求选择“N/A”选项，然后在附录 C 为所有“N/A”条目填写“不适用性说明”。

不适用和未测试之间的区别说明

视为不适用于相关环境的要求必须获得相应认证。以上述无线技术为例，如果某个组织想要针对要求 1.2.3、2.1.1 和 4.1.1 选择“N/A”，则必须先确认其 CDE 中未使用或连接到任何无线技术。经过确认后，该组织便可针对这些特定要求选择“N/A”。

如果在审核过程中未经任何考虑便将某项要求完全排除在适用范围之外，则应选择“未测试”选项。此类情况可能包括：

- 某组织的收单机构可能要求其验证是否遵从特定要求部分，例如使用优先方法验证是否达到特定里程碑。
- 某组织可能想要验证仅会影响特定要求部分的新安全控制，例如实施新的加密方法需要针对 PCI DSS 要求 2、3 和 4 进行评估。
- 某服务供应商组织提供的某项服务可能只涉及有限部分的 PCI DSS 要求，例如某物理存储供应商可能只想要针对 PCI DSS 要求 9 为其存储设施进行物理安全控制验证。

在上述情况下，相关组织只想要验证特定 PCI DSS 要求，即使其他要求可能也适用于其所在环境。

法律规定的例外情况

如果您所在组织因受到相关法律限制约束而无法满足 PCI DSS 要求，请针对该要求选择“否”列，然后在第 3 部分填写相关证明书。

第 1 节： 评估信息

提交说明

商户必须填写此文档，以声明其按照*支付卡行业数据安全标准要求和安全评估程序 (PCI DSS) 所做的自我评估的结果*。填写所有章节：商户应负责确保相关方（如果有）填写所有章节。联系收单机构（商户银行）或支付品牌以确定报告和提交程序。

第 1 部分 商户和合格安全性评估商信息

第 1a 部分 商户组织信息

公司名称：			DBA（经营别称）：		
联系人姓名：			职务：		
电话：			电子邮件地址：		
公司地址：			城市：		
州/省：		国家/地区：		邮编：	
网址：					

第 1b 部分 合格安全性评估商公司信息（如果有）

公司名称：					
QSA 主要联系人姓名：			职务：		
电话：			电子邮件地址：		
公司地址：			城市：		
州/省：		国家/地区：		邮编：	
网址：					

第 2 部分 实施概要

第 2a 部分 商户业务类型（选中所有合适选项）

☐ 零售商	☐ 通信	☐ 百货和超市
☐ 石油	☐ 电子商务	☐ 邮件/电话订购 (MOTO)
☐ 其他（请指明）：		

您所在企业提供哪些类型的支付渠道？	此 SAQ 覆盖哪些支付渠道？
☐ 邮件/电话订购 (MOTO)	☐ 邮件/电话订购 (MOTO)
☐ 电子商务	☐ 电子商务
☐ 实卡交易（面对面）	☐ 实卡交易（面对面）

注：如果您所在组织的支付渠道或流程未涵盖在此 SAQ 范围内，请咨询您的收单机构或支付品牌了解如何验证其他渠道。

第 2b 部分 支付卡业务说明

您所在企业如何存储、处理和/或传输持卡人数据，以及支持的容量是多少？	

第 2c 部分 地点

列出 PCI DSS 审核中包含的场所类型（例如，零售店、公司办公室、数据中心、呼叫中心等等）以及所在地点概要。

场所类型	此类场所数量	场所所在地点（城市、国家/地区）
示例：零售店	*3*	*美国马萨诸塞州波士顿*

第 2d 部分 支付应用程序

该组织是否使用一款或多款支付应用程序？ ☐ 是 ☐ 否

提供有关您所在组织使用的支付应用程序的下列信息：

支付应用程序名称	版本号	应用程序供应商	该应用程序是否获得 PA-DSS 认证？	PA-DSS 认证失效日期（如果有）
			☐ 是 ☐ 否	
			☐ 是 ☐ 否	
			☐ 是 ☐ 否	
			☐ 是 ☐ 否	
			☐ 是 ☐ 否	

第 2e 部分 环境说明

提供有关此评估所涵盖的环境的***高级***说明。 *例如：* • *对持卡人数据环境 (CDE) 的输入和输出连接。* • *该 CDE 中的关键系统组件（例如 POS 设备、数据库、网络服务器等）以及其他任何必要的支付组件（如果有）。*	

您所在企业是否使用网络分段来影响 PCI DSS 环境范围？ *（有关网络分段的指南，请参见 PCI DSS 的"网络分段"章节）*	☐ 是 ☐ 否

第 2f 部分 第三方服务提供商

您的公司是否使用合格集成商和经销商 (QIR)？ 如果是的话： QIR 公司名称： QIR 个人名称： QIR 所提供服务的说明：	☐ 是 ☐ 否
您所在公司是否与任何第三方服务提供商（例如，合格集成商和经销商 (QIR)、网关、支付处理商、支付服务提供商 (PSP)、网络托管公司、航班订票代理商、忠诚计划代理商等）共享持卡人数据？	☐ 是 ☐ 否

如果是的话：

服务提供商名称：	**所提供服务的说明：**

注：*要求 12.8 适用于上述列表中的所有条目。*

第 2 节： 适用于商户的自我评估调查问卷 D

注：以下问题的编号与 PCI DSS 要求和安全评估程序文档中说明的 PCI DSS 要求和测试程序顺序相符。

自我评估实施日期：

构建和维护安全网络和系统

要求 1： ***安装和维护防火墙配置以保护数据***

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
1.1	是否已建立和实施了包括以下方面的防火墙和路由器配置：						
1.1.1	是否建立了用于批准和测试所有网络连接以及防火墙和路由器配置变更的正式流程？	▪ 审核已记录的流程 ▪ 与工作人员面谈 ▪ 检查网络配置	☐	☐	☐	☐	☐
1.1.2	(a) 是否已存在当前网络图且该图记录了持卡人数据环境与包括任何无线网络在内的其他网络之间的所有连接？	▪ 审核当前网络图 ▪ 检查网络配置	☐	☐	☐	☐	☐
	(b) 是否有相应流程以确保该图及时更新？	▪ 与负责人面谈	☐	☐	☐	☐	☐
1.1.3	(a) 是否已存在当前图且该图显示了系统和网络间的所有持卡人数据流？	▪ 审核当前数据流图 ▪ 检查网络配置	☐	☐	☐	☐	☐
	(b) 是否有相应流程以确保该图及时更新？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
1.1.4	(a) 各互联网连接以及任何非军事区 (DMZ) 和内部网络区域间是否要求和实施了防火墙？	▪ 审核防火墙配置标准 ▪ 查看网络配置以确认是否部署了防火墙	☐	☐	☐	☐	☐
	(b) 当前网络图是否与防火墙配置标准相符？	▪ 对比防火墙配置标准和当前网络图是否相符	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
1.1.5	防火墙和路由器配置标准中是否分配和记录了网络组件逻辑管理的群组、角色和责任？	▪ 审核防火墙和路由器配置标准 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
1.1.6	(a) 防火墙和路由器配置标准是否包含服务、协议和端口的文档记录列表（包括各自的业务理由和审批）？	▪ 审核防火墙和路由器配置标准	☐	☐	☐	☐	☐
	(b) 是否已识别出所有不安全的服务、协议和端口且已针对识别出的所有服务记录和实施了安全功能？	▪ 审核防火墙和路由器配置标准 ▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
1.1.7	(a) 防火墙和路由器配置标准是否要求至少每半年审核一次防火墙和路由器规则集？	▪ 审核防火墙和路由器配置标准	☐	☐	☐	☐	☐
	(b) 是否至少每半年审核了一次防火墙和路由器规则集？	▪ 检查有关防火墙审核的文档记录	☐	☐	☐	☐	☐
1.2	防火墙和路由器配置是否按照下述要求限制了不可信网络和持卡人数据环境中任何系统间的连接： ***注：****"不可信网络"指受审核实体所属网络之外的任何网络，和/或不受该实体控制或管理的任何网络。*						
1.2.1	(a) 输入和输出流量是否限制在持卡人数据环境所需的范围？	▪ 审核防火墙和路由器配置标准 ▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
	(b) 是否明确拒绝（例如，使用明确的"拒绝所有"或在允许声明后含蓄地表达拒绝之意）其他所有输入和输出流量？	▪ 审核防火墙和路由器配置标准 ▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
1.2.2	路由器配置文件是否禁止未经授权的访问且已同步，例如运行（或活动）配置与启动配置（启动电脑时使用）相匹配？	▪ 审核防火墙和路由器配置标准 ▪ 检查路由器配置文件和路由器配置	☐	☐	☐	☐	☐
1.2.3	是否在所有无线网络和持卡人数据环境间安装了外围防火墙，并将这些防火墙配置为拒绝流量或（如果出于业务目的而需要流量）仅允许无线环境和持卡人数据环境间的授权流量？	▪ 审核防火墙和路由器配置标准 ▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
1.3	是否按照下述要求禁止了互联网与持卡人数据环境中任何系统组件之间的直接公共访问：						
1.3.1	是否已实施了 DMZ 以将输入流量限制为仅支持提供授权公共访问服务、协议和端口的系统组件？	▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
1.3.2	是否已限制为仅向 DMZ 内的 IP 地址输入互联网流量？	▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
1.3.3	是否实施了反欺骗措施以检测并阻止伪造的源 IP 地址进入该网络？ （例如，阻止具有内部地址的互联网流量。）	▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
1.3.4	从持卡人数据环境输出到互联网的流量是否具有明确授权？	▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
1.3.5	是否仅允许已建立的连接进入该网络？	▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
1.3.6	存储持卡人数据的系统组件（例如数据库）是否放置在与 DMZ 和其他不可信网络隔离的内部网络区域中？	▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
1.3.7	(a) 是否已实施相应方法来阻止私有 IP 地址和路由信息泄漏到互联网？ ***注：****掩盖 IP 地址的方法包括但不限于：* • 网络地址转换 (NAT) • 将包含持卡人数据的服务器放置在代理服务器/防火墙中， • 删除或过滤针对采用注册地址的专用网络的路由器广告， • 在内部使用 RFC1918 地址空间而非注册地址。	▪ 检查防火墙和路由器配置	☐	☐	☐	☐	☐
	(b) 面向外部实体的任何私有 IP 地址和路由信息泄漏是否都经过授权？	▪ 检查防火墙和路由器配置 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

1.4	(a) 是否在位于该网络外连接到互联网且可用于访问 CDE 的任意便携式计算设备（包括公司和/或员工所有的便携式计算设备，例如，员工使用的笔记本电脑）上安装和激活了个人防火墙软件（或类似功能）？	▪ 审核相关政策和配置标准 ▪ 检查移动设备和/或员工自有设备	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
	(b) 个人防火墙软件（或类似功能）是否配置为特定配置设置、积极运行且无法由移动设备用户和/或员工自有设备用户更改？	▪ 审核相关政策和配置标准 ▪ 检查移动设备和/或员工自有设备	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
1.5	针对防火墙管理的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 审核安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

要求 2：　不要使用供应商提供的默认系统密码和其他安全参数

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
2.1	(a) 是否始终于在该网络中安装系统之前更改供应商提供的默认值？ *此要求适用于所有默认密码，包括但不限于操作系统、提供安全服务的软件、应用程序和系统帐户、销售点 (POS) 终端、支付应用程序、简单网络管理协议 (SNMP) 社区字符串等使用的默认密码。*	▪ 审核相关政策和程序 ▪ 检查供应商文档 ▪ 查看系统配置和帐户设置 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(b) 是否已于在该网络中安装系统之前删除或禁用不必要的默认帐户？	▪ 审核相关政策和程序 ▪ 审核供应商文档 ▪ 检查系统配置和帐户设置 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
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，是否按照下述要求在安装时更改了所有无线供应商提供的默认值：						
	(a) 是否在安装以及知道密钥的任何人离职或更换岗位时更改了默认的加密密钥？	▪ 审核相关政策和程序 ▪ 审核供应商文档 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(b) 是否在安装时更改了无线设备上的默认 SNMP 社区字符串？	▪ 审核相关政策和程序 ▪ 审核供应商文档 ▪ 与工作人员面谈 ▪ 检查系统配置	☐	☐	☐	☐	☐
	(c) 是否在安装时更改了接入点的默认密码/口令？	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 检查系统配置	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
	(d) 是否已更新无线设备的固件来支持通过无线网络进行的验证和传输的强效加密？	▪ 审核相关政策和程序 ▪ 审核供应商文档 ▪ 检查系统配置	☐	☐	☐	☐	☐
	(e) 是否已更改其他与安全有关的无线供应商默认值（如果适用）？	▪ 审核相关政策和程序 ▪ 审核供应商文档 ▪ 检查系统配置	☐	☐	☐	☐	☐
2.2	(a) 配置标准是否为针对所有系统组件制定的，以及是否与行业认可的系统强化标准一致？ *行业认可的系统强化标准来源包括但不限于：美国系统网络安全协会 (SANS)、国家标准与技术研究所 (NIST)、国际标准化组织 (ISO) 和互联网安全中心 (CIS)。*	▪ 审核系统配置标准 ▪ 审核行业认可的强化标准 ▪ 审核相关政策和程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(b) 是否已按照要求 6.1 在发现新的安全漏洞问题时更新了系统配置标准？	▪ 审核相关政策和程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(c) 是否已在配置新系统时应用了系统配置标准？	▪ 审核相关政策和程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(d) 系统配置标准是否包含以下所有说明： • 更改所有供应商提供的默认值并删除不必要的默认帐户 • 每台服务器仅执行一项主要功能以免需要不同安全级别的功能并存于同一台服务器上 • 仅启用系统功能所需的必要服务、协议、守护进程等 • 对于任何被视为不安全的必要服务、协议或守护进程，均执行附加安全功能 • 配置系统安全参数以防滥用 • 删除所有非必要功能，例如脚本、驱动程序、特性、子系统、文件系统和不必要的网络服务器	▪ 审核系统配置标准	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
2.2.1	(a) 是否仅在每台服务器执行了一项主要功能，以免需要不同安全级别的功能并存于同一台服务器上？ *例如，网络服务器、数据库服务器和 DNS 均应在单独的服务器上执行。*	▪ 检查系统配置	☐	☐	☐	☐	☐
	(b) 如果采用了虚拟化技术，那么每个虚拟系统组件或设备是否仅执行了一项主要功能？	▪ 检查系统配置	☐	☐	☐	☐	☐
2.2.2	(a) 是否仅启用了系统功能所需的必要服务、协议、守护进程等（并非执行设备特定功能所直接需要的服务和协议已禁用）？	▪ 审核配置标准 ▪ 检查系统配置	☐	☐	☐	☐	☐
	(b) 是否已根据书面配置标准判断所有已启用的不安全服务、守护进程或协议是否合理？	▪ 审核配置标准 ▪ 与工作人员面谈 ▪ 检查配置设置 ▪ 对比已启用的服务等和理由记录是否相符	☐	☐	☐	☐	☐
2.2.3	是否已针对任何被视为不安全的必要服务、协议或守护进程记录和执行了附加安全功能？ ***注：****若要使用 SSL/早期 TLS，须完成附录 A2 中的要求。*	▪ 审核配置标准 ▪ 检查配置设置	☐	☐	☐	☐	☐
2.2.4	(a) 系统管理员和/或负责配置系统组件的工作人员是否了解适用于这些系统组件的常用安全参数设置？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(b) 常用系统安全参数设置是否包含在系统配置标准中？	▪ 审核系统配置标准	☐	☐	☐	☐	☐
	(c) 适用于系统组件的安全参数设置是否适当？	▪ 检查系统组件 ▪ 检查安全参数设置 ▪ 对比设置和系统配置标准是否相符	☐	☐	☐	☐	☐
2.2.5	(a) 是否删除了所有非必要功能，例如脚本、驱动程序、特性、子系统、文件系统和不必要的网络服务器？	▪ 检查适用于系统组件的安全参数	☐	☐	☐	☐	☐
	(b) 已启用的功能是否已记录，且是否支持安全配置？	▪ 审核相关文档 ▪ 检查适用于系统组件的安全参数	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
	(c) 系统组件是否只适用具有文档记录的功能？	▪ 审核相关文档 ▪ 检查适用于系统组件的安全参数	☐	☐	☐	☐	☐
2.3	是否按照下述要求对非控制台管理访问进行了加密： ***注：****若要使用 SSL/早期 TLS，须完成附录 A2 中的要求*						
	(a) 是否已对所有非控制台管理访问应用强效加密法，且在要求提供管理员密码前已调用强效加密法？	▪ 检查系统组件 ▪ 检查系统配置 ▪ 查看管理员登录	☐	☐	☐	☐	☐
	(b) 系统服务和参数文件是否已配置为阻止使用 Telnet 和其他不安全的远程登录命令？	▪ 检查系统组件 ▪ 检查服务和文件	☐	☐	☐	☐	☐
	(c) 是否已采用强效加密法对管理员进入基于 web 的管理界面的访问权进行加密？	▪ 检查系统组件 ▪ 查看管理员登录	☐	☐	☐	☐	☐
	(d) 是否已按照行业最优方法和/或供应商建议对所使用的技术实施强效加密？	▪ 检查系统组件 ▪ 审核供应商文档 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
2.4	(a) 是否已保留 PCI DSS 范围内的系统组件清单，其中包含软硬件组件列表以及各自的功能/用途描述？	▪ 检查系统清单	☐	☐	☐	☐	☐
	(b) 书面清单是否及时更新？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
2.5	用于管理供应商默认值和其他安全参数的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 审核安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
2.6	*此要求仅适用于服务提供商。*						

保护持卡人数据

要求 3：　　保护存储的持卡人数据

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
3.1	数据保留和处理政策、程序与流程是否按照下述要求实施：						
	(a) 数据存储量和保留时间是否限制在法律、法规和/或业务需求所需的范围内？	▪ 审核数据保留和处理政策、程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(b) 是否制定了特定流程来在不再因法律、法规和/或业务原因而需要时安全删除持卡人数据？	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 检查删除机制	☐	☐	☐	☐	☐
	(c) 是否存在针对持卡人数据的具体保留要求？ *例如因 Y 业务原因，需将持卡人数据保留 X 的时间。*	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 检查保留要求	☐	☐	☐	☐	☐
	(d) 是否制定了特定流程来按季度查找并安全删除所存储的超过规定保留期限要求的持卡人数据？	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 查看删除流程	☐	☐	☐	☐	☐
	(e) 是否所有存储的数据均满足数据保留政策中规定的要求？	▪ 检查文件和系统记录	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
3.2	(a) *此测试程序仅适用于发卡机构。*						
	(b) *此测试程序仅适用于发卡机构。*						
	(c) 完成授权流程后，是否删除了敏感验证数据或使其不可恢复？	▪ 审核相关政策和程序 ▪ 检查系统配置 ▪ 检查删除流程	☐	☐	☐	☐	☐
	(d) 是否所有系统均已遵循以下有关授权后不存储敏感验证数据（即使已经加密）的要求：						
3.2.1	授权后不存储任意磁道上的完整内容（位于卡背面的磁条中、芯片上或其他位置）。 *此类据也可称为全磁道、磁道、磁道 1、磁道 2 和磁条数据。* ***注：****在正常业务过程中，以下磁条数据元素可能需要保留：* • *持卡人姓名，* • *主帐户 (PAN)，* • *失效日，以及* • *业务码* *为将风险降至最低，只存储业务所需的数据元素。*	▪ 检查数据来源，其中包括： • 输入的交易数据 • 所有日志 • 存档文件 • 跟踪文件 • 数据库架构 • 数据库内容	☐	☐	☐	☐	☐
3.2.2	授权后不存储卡验证代码或值（印在支付卡正面或背面的三位或四位数值）？	▪ 检查数据来源，其中包括： • 输入的交易数据 • 所有日志 • 存档文件 • 跟踪文件 • 数据库架构 • 数据库内容	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
3.2.3	授权后不存储个人识别码 (PIN) 或经加密的 PIN 数据块？	▪ 检查数据来源，其中包括： • 输入的交易数据 • 所有日志 • 存档文件 • 跟踪文件 • 数据库架构 • 数据库内容	☐	☐	☐	☐	☐
3.3	PAN 是否在显示时被掩盖（只有前六位和后四位数字可以显示），以便仅有正当业务需要者才能看到除前六位/后四位以外的 PAN？ ***注：****该要求不能取代现行更严格的有关持卡人数据显示的要求，例如法律或支付卡品牌对销售点 (POS) 收据的要求。*	▪ 审核相关政策和程序 ▪ 审核需要能够查看完整 PAN 的角色 ▪ 检查系统配置 ▪ 查看 PAN 的显示	☐	☐	☐	☐	☐
3.4	是否已通过采取下列任一方法使所有位置（包括数据储存库、便携式数字媒介、备份媒介和检查日志中）存储的 PAN 均不可读？ ▪ 基于强效加密法的单向散列函数（散列必须要有完整的 PAN） ▪ 截词（不能用散列代替 PAN 被截词的部分） ▪ 索引令牌与索引簿（索引簿必须安全地存储） ▪ 具有相关密钥管理流程和程序的强效加密法。 ***注：****对恶意个人而言，如果能访问被截词和散列的 PAN，要重建原始 PAN 数据是件相当轻松的事。如果在实体环境中出现同一个 PAN 的散列版本和截词版本，则须采取额外控制措施，确保散列版本和截词版本不能被相互关联，用于重建原始 PAN。*	▪ 检查供应商文档 ▪ 检查数据储存库 ▪ 检查可移动媒介 ▪ 检查检查日志，包括支付应用程序日志	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
3.4.1	如果使用了磁盘加密（而非文件级或列级数据库加密），访问权限管理是否符合下述说明： ***注：****除了所有其他 PCI DSS 加密和密钥管理要求外，此要求也适用。*						
	(a) 对已加密文件系统的逻辑访问是否得到单独管理，并独立于本地操作系统的验证和访问控制机制（例如，不使用本地用户帐户数据库或通用网络登录凭证）？	▪ 检查系统配置 ▪ 查看验证流程	☐	☐	☐	☐	☐
	(b) 加密密钥是否已安全存储（例如存储在通过严格访问控制提供充分保护的可移动媒介上）？	▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(c) 存储在可移动媒介上任何位置的持卡人数据是否均已加密？ ***注：****如果未使用磁盘加密法对可移动媒介加密，则需通过一些其他方法使存储在该媒介上的数据实现不可读。*	▪ 检查系统配置 ▪ 查看流程	☐	☐	☐	☐	☐
3.5	是否按照下述要求使用密钥以保护存储的持卡人数据不被泄露和滥用： ***注：****此要求适用于用来为存储的持卡人数据加密的密钥，也适用于用来保护数据加密密钥的密钥加密密钥。此类密钥加密密钥至少要与数据加密密钥一样强效。*						
3.5.1	*此要求仅适用于服务提供商*						
3.5.2	是否只有极少数必需的保管人具有密钥访问权限？	▪ 检查用户访问列表	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
3.5.3	是否始终以下面的一种（或多种）形式存储用于加密/解密持卡人数据的机密密钥和私人密钥？ ▪ 使用至少与数据加密密钥一样强效且与数据加密密钥分开存储的密钥加密密钥进行加密 ▪ 在安全加密设备（例如，硬件（主机）安全模块 (HSM) 或 PTS 批准的交互点设备）内 ▪ 根据行业认可的方法，采用至少两个全长密钥组分或密钥共享。 ***注：****公共密钥不要求以这些形式存储。*	▪ 审核程序文档记录 ▪ 检查系统配置和密钥存储位置（包括密钥加密密钥存储位置）	☐	☐	☐	☐	☐
3.5.4	是否已尽量减少密钥存储位置？	▪ 检查密钥存储位置 ▪ 查看流程	☐	☐	☐	☐	☐
3.6	(a) 是否已针对用于加密持卡人数据的密钥完全记录和实施了所有密钥管理流程和程序？	▪ 审核密钥管理程序	☐	☐	☐	☐	☐
	(b) *此测试程序仅适用于服务提供商。*						
	(c) 是否已按照下述要求实施了密钥管理流程和程序：						
3.6.1	密钥程序是否包括生成强效密钥的程序？	▪ 审核密钥管理程序 ▪ 查看密钥生成方法	☐	☐	☐	☐	☐
3.6.2	密钥程序是否包括密钥安全分配的程序？	▪ 审核密钥管理程序 ▪ 查看密钥分配程序	☐	☐	☐	☐	☐
3.6.3	密钥程序是否包括密钥安全存储的程序？	▪ 审核密钥管理程序 ▪ 查看安全存储密钥的方法	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
3.6.4	密钥程序是否包括在密钥周期结束时（例如，指定期限过后和/或给定密钥产生一定量的密文后）根据相关应用程序供应商或密钥所有人的规定并基于行业最优方法和指南（例如，《NIST 特别出版物 800-57》）变更密钥的程序？	▪ 审核密钥管理程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
3.6.5	(a) 密钥程序是否包括在密钥的完整性变弱（例如，知道明文密钥部分的员工离职）时注销或替换（例如，存档、销毁和/或撤销）密钥的程序？	▪ 审核密钥管理程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(b) 密钥程序是否包括替换确定或怀疑受到威胁的密钥的程序？	▪ 审核密钥管理程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(c) 如果保留了已注销或替换的密钥，这些密钥是否仅用于进行解密/验证，而不再用于加密操作？	▪ 审核密钥管理程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
3.6.6	如果使用手动明文密钥管理操作，密钥程序是否按照下述要求包含密钥的分割知识和双重控制程序： ▪ 分割知识程序是否要求密钥的组成部分至少由两个人控制，且每个人只知道自己那部分的密钥？ 以及 ▪ 双重控制程序是否要求至少需要两个人执行任何密钥管理操作且他们无法访问对方的验证材料（例如，密码或密钥）？ ***注：****手动密钥管理操作包括但不限于：密钥生成、传输、加载、存储和销毁。*	▪ 审核密钥管理程序 ▪ 与工作人员面谈和/或 ▪ 查看流程	☐	☐	☐	☐	☐
3.6.7	密钥程序是否包括防止无授权替换密钥的程序？	▪ 审核程序 ▪ 与工作人员面谈和/或 ▪ 查看流程	☐	☐	☐	☐	☐
3.6.8	密钥保管人是否需要正式确认（以书面或电子形式）理解并接受密钥保管责任？	▪ 审核程序 ▪ 审核文档或其他证据	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
3.7	用于保护存储的持卡人数据的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 审核安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

要求 4：　　加密持卡人数据在开放式公共网络中的传输

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
4.1	(a) 是否使用了强效加密法和安全协议来保护经由公开、公共网络传输的敏感持卡人信息。 ***注：****若要使用 SSL/早期 TLS，须完成附录 A2 中的要求。* *在 PCI DSS 的范围内，公开、公共的网络包括但不限于，互联网、无线技术（包括 802.11 和蓝牙）、蜂窝技术（例如，全球移动通信系统 (GSM)、码分多址 (CDMA)）以及通用分组无线业务 (GPRS)。*	▪ 审核书面标准 ▪ 审核相关政策和程序 ▪ 审核传输或接收 CHD 的所有地点 ▪ 检查系统配置	☐	☐	☐	☐	☐
	(b) 是否只接受可信密钥和/或证书？	▪ 查看输入和输出传输 ▪ 检查密钥和证书	☐	☐	☐	☐	☐
	(c) 实施的安全协议是否仅使用安全配置且不支持非安全版本或配置？	▪ 检查系统配置	☐	☐	☐	☐	☐
	(d) 是否已根据所使用的加密方法实施了适当的加密强度（查看供应商建议/最优方法）？	▪ 审核供应商文档 ▪ 检查系统配置	☐	☐	☐	☐	☐
	(e) 对于 TLS 的实施，是否在传输或接收持卡人数据时始终启用了 TLS？ *例如，对于基于浏览器的实施：* • *"HTTPS"作为浏览器统一记录定位器 (URL) 协议，且* • 仅当"HTTPS"作为 URL 的一部分时才需要持卡人数据。	▪ 检查系统配置	☐	☐	☐	☐	☐
4.1.1	传输持卡人数据或连接到持卡人数据环境的无线网络是否使用了行业最优方法来对验证和传输实施强效加密？	▪ 审核书面标准 ▪ 审核无线网络 ▪ 检查系统配置设置	☐	☐	☐	☐	☐
4.2	(a) PAN 是否在通过终端用户通讯技术（例如，电子邮件、即时通讯、聊天等）传送的任意时刻均不可读或受强效加密法保护？	▪ 查看流程 ▪ 审核输出传输	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
	(b) 是否已制定政策来规定不会通过终端用户通讯技术传送不受保护的 PAN？	▪ 审核相关政策和程序	☐	☐	☐	☐	☐
4.3	用于对持卡人数据传输进行加密的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 审核安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

维护漏洞管理计划

要求 5： *为所有系统提供恶意软件防护并定期更新杀毒软件或程序*

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
5.1	是否在经常受恶意软件影响的所有系统中部署了杀毒软件？	▪ 检查系统配置	☐	☐	☐	☐	☐
5.1.1	杀毒程序是否能够检测、删除并阻止所有已知类型的恶意软件（例如，病毒、特洛伊木马、蠕虫病毒、间谍软件、广告软件和 rootkit 内核型病毒）？	▪ 审核供应商文档 ▪ 检查系统配置	☐	☐	☐	☐	☐
5.1.2	是否执行了定期评估以确定并评估不断进化的恶意软件威胁，从而确认之前认为通常不受恶意软件影响的系统是否仍然如此？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
5.2	是否按照下述要求保留了所有杀毒机制：						
	(a) 是否及时更新了所有杀毒软件和相关定义？	▪ 检查政策和程序 ▪ 检查杀毒配置（包括主体安装） ▪ 检查系统组件	☐	☐	☐	☐	☐
	(b) 是否已启用且正执行自动更新和定期扫描？	▪ 检查杀毒配置（包括主体安装） ▪ 检查系统组件	☐	☐	☐	☐	☐
	(c) 是否所有杀毒机制均可生成检查日志且按照 PCI DSS 要求 10.7 保留日志？	▪ 检查杀毒配置 ▪ 审核日志保留流程	☐	☐	☐	☐	☐
5.3	是否所有杀毒机制均： ▪ 积极运行？ ▪ 无法被用户禁用或修改？ ***注：****只有存在合理的技术需要且根据具体情况经管理人员批准时，才能暂时禁用杀毒解决方案。如果出于特定目的需要禁用杀毒保护，必须获得正式授权。杀毒保护禁用期间，可能还需要实施其他安全措施。*	▪ 检查杀毒配置 ▪ 检查系统组件 ▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
5.4	用于保护系统免遭恶意软件损害的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 审核安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

要求 6：　开发并维护安全的系统和应用程序

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
6.1	是否制定了包括以下方面的安全漏洞识别流程： ▪ 使用可信外源获取安全漏洞信息？ ▪ 为安全漏洞指定风险等级，包括对所有“高”风险和“重要”漏洞的识别？ ***注：****风险等级应以行业最优方法和潜在影响考虑为依据。例如，漏洞分级标准可能包括对 CVSS 基础得分的考虑和/或供应商的分类，及/或相关系统的类型。* *根据组织的环境和风险评估策略不同，评估漏洞和指定风险等级的方法也不尽相同。风险等级至少应标识出所有被视为对环境具有“高风险”的漏洞。除风险等级外，如果安全漏洞即将对环境造成威胁、影响关键系统且/或如果不解决可能会造成潜在危害，则可被视为“重要”。关键系统可能包括安全系统、面向公众的设备和系统、数据库以及其他存储、处理或传输持卡人数据的系统。*	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 查看流程	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
6.2	(a) 是否已安装供应商提供的适用安全补丁，以确保所有系统组件和软件均杜绝已知漏洞？	▪ 审核相关政策和程序	☐	☐	☐	☐	☐
	(b) 是否在发布后一个月内安装了关键的安全补丁？ ***注：****应按照要求 6.1 中规定的风险分级流程标识关键安全补丁。*	▪ 审核相关政策和程序 ▪ 检查系统组件 ▪ 对比安装的安全补丁列表和最新的供应商补丁列表是否相符	☐	☐	☐	☐	☐
6.3	(a) 软件开发流程是否以行业标准和/或最优方法为基础？	▪ 审核软件开发流程 ▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(b) 是否已将信息安全纳入软件开发的整个生命周期？	▪ 审核软件开发流程 ▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(c) 软件应用程序的开发是否符合 PCI DSS（例如，安全验证和记录）？	▪ 审核软件开发流程 ▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(d) 软件开发流程是否确保满足 6.3.1 - 6.3.2 中的下述要求：						
6.3.1	是否已在应用程序启动或向客户发布前删除了开发、测试和/或自定义应用程序帐户、用户 ID 和密码？	▪ 审核软件开发流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
6.3.2	是否已在发布到生产环境或向客户发布前按照下述要求检查了所有自定义代码，以识别任何潜在的编码漏洞（采用人工或自动流程）： ▪ 代码变更是否已由代码原作者以外人员以及熟悉代码审核方法和安全编码实践的人员进行了审核？ ▪ 代码审核是否可确保代码的开发符合安全编码指南？ ▪ 发布前是否已进行适当修正？ ▪ 代码审查结果是否已在发布前由管理人员审核并批准？ ***注：****这项代码审核要求适用于所有自定义代码（内部代码和面向公众的代码），可作为系统开发生命周期的组成部分。代码审核可由经验丰富的内部人员或第三方执行。面向公众的 Web 应用程序还应受到附加控制措施的约束，以应对实施后不断出现的威胁和漏洞，具体规定请参见 PCI DSS 要求 6.6。*	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 检查最新变更情况和变更记录	☐	☐	☐	☐	☐
6.4	系统组件的所有变更是否均已遵守包括以下方面的变更控制流程和程序：						
6.4.1	(a) 开发/测试环境是否独立于生产环境？	▪ 审核变更控制流程和程序 ▪ 检查网络文档记录和网络设备配置	☐	☐	☐	☐	☐
	(b) 是否设置了访问控制以确保开发/测试环境和生产环境的分离？	▪ 审核变更控制流程和程序 ▪ 检查访问控制设置	☐	☐	☐	☐	☐
6.4.2	是否对分配到开发/测试环境与生产环境中的人员的职责进行了分离？	▪ 审核变更控制流程和程序 ▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
6.4.3	是否***未***在测试或开发过程中使用生产数据（真实的 PAN）？	▪ 审核变更控制流程和程序 ▪ 查看流程 ▪ 与工作人员面谈 ▪ 检查测试数据	☐	☐	☐	☐	☐
6.4.4	是否已在系统激活/投入生产前删除了系统组件中的测试数据和帐户？	▪ 审核变更控制流程和程序 ▪ 查看流程 ▪ 与工作人员面谈 ▪ 检查生产系统	☐	☐	☐	☐	☐
6.4.5	(a) 变更控制程序是否已用文档记录且包括以下方面？ • 影响记录 • 相关被授权方的变更控制审批记录 • 功能测试，以确认该变更未对系统安全造成不利影响 • 取消程序	▪ 审核变更控制流程和程序	☐	☐	☐	☐	☐
	(b) 是否已针对所有变更执行和记录了以下项：						
6.4.5.1	影响记录？	▪ 跟踪变更控制文档的变更情况 ▪ 检查变更控制文档	☐	☐	☐	☐	☐
6.4.5.2	相关被授权方的变更控制审批记录？	▪ 跟踪变更控制文档的变更情况 ▪ 检查变更控制文档	☐	☐	☐	☐	☐
6.4.5.3	(a) 功能测试，以确认该变更未对系统安全性造成不利影响？	▪ 跟踪变更控制文档的变更情况 ▪ 检查变更控制文档	☐	☐	☐	☐	☐
	(b) 对于自定义代码变更，确认在将其部署到生产环境前，所有更新均经过测试符合 PCI DSS 要求 6.5？	▪ 跟踪变更控制文档的变更情况 ▪ 检查变更控制文档	☐	☐	☐	☐	☐
6.4.5.4	取消程序？	▪ 跟踪变更控制文档的变更情况 ▪ 检查变更控制文档	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
6.4.6	完成重要变更后，是否对所有新的或已更改的系统及网络实施了相关的 PCI DSS 要求，并在适当情况下更新了文档？ ***注：****本要求在 2018 年 1 月 31 日前属于最优方法，此后将成为一项要求。*	▪ 跟踪变更控制文档的变更情况 ▪ 检查变更控制文档 ▪ 与工作人员面谈 ▪ 查看受影响的系统或网络	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
6.5	(a) 软件开发过程中能否修复常见编码漏洞？	▪ 审核软件开发政策和程序	☐	☐	☐	☐	☐
	(b) 每年是否至少对开发人员进行一次最新安全编码技术（包括如何避免常见编码漏洞）方面的培训？	▪ 检查软件开发政策和程序 ▪ 检查培训记录	☐	☐	☐	☐	☐
	(c) 是否根据安全编码指南开发应用程序以保护其不受以下漏洞危害： ***注：****在本版本 PCI DSS 发布时，已采用行业最优方法将 6.5.1 到 6.5.10 中列举的漏洞保持为最新。但当有关漏洞管理的行业最优方法（例如开放式 Web 应用程序安全项目 (OWASP) 指南、前 25 大高危软件错误、CERT 安全编码等）出现更新时，这些要求必须采用当下最新的最优方法。*						
6.5.1	编码技术能否解决注入攻击（尤其是 SQL 注入）？ ***注：****同时还须考虑 OS 命令注入、LDAP、XPath 等其他注入攻击。*	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
6.5.2	编码技术能否解决缓冲区溢出漏洞？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
6.5.3	编码技术能否解决非安全加密存储？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
6.5.4	编码技术能否解决非安全通信？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
6.5.5	编码技术能否解决不正确的错误处理？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
6.5.6	编码技术能否解决漏洞识别流程中确认的所有“高风险”漏洞（具体规定请参见 PCI DSS 要求 6.1）？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
对于基于 web 的应用程序和应用程序接口（内部或外部），是否根据安全编码指南开发应用程序以保护其不受以下其他漏洞危害：							
6.5.7	编码技术能否解决跨站点脚本 (XSS) 漏洞？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
6.5.8	编码技术能否解决不正确的访问控制（例如不安全的直接对象引用、未能限制 URL 访问和目录遍历以及未能限制用户的功能访问）？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
6.5.9	编码技术能否解决跨站请求伪造 (CSRF)？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
6.5.10	编码技术能否解决失效的验证和会话管理？	▪ 检查软件开发政策和程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
6.6	对于面向公众的 web 应用程序，是否已不断解决新的威胁和漏洞，并通过以下*任一*方法确保这些应用程序不会受到已知攻击？ ▪ 按照下述要求利用手动或自动应用程序漏洞安全评估工具或方法审核面向公众的 web 应用程序： - 至少每年执行一次 - 在任意变更之后 - 由专注于应用程序安全的组织进行 - 至少要求 6.5 中的所有漏洞均包含在评估中 - 所有漏洞均已修复 - 修复漏洞后重新评估应用程序 ***注：****本评估与要求 11.2 中规定执行的漏洞扫描不同。* **– 或者 –** ▪ 安装如下所述的可检测并预防基于 Web 的攻击的自动化技术解决方案（例如，Web 应用程序防火墙）： - 位于面向公众的 web 应用程序之前，用以检查并防范网页式攻击。 - 积极运行且为最新（若适用）。 - 可生成检查日志。 - 配置为阻止网页式攻击，或生成需立即调查的警报。	▪ 审核流程文档记录 ▪ 与工作人员面谈 ▪ 检查应用程序安全评估记录 ▪ 检查系统配置设置	☐	☐	☐	☐	☐
6.7	用于开发和维护安全系统和应用程序的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 审核安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

实施强效访问控制措施

要求 7：　　按业务知情需要限制对持卡人数据的访问

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
7.1	是否如下所述只有具有相应工作需要的个人才能访问系统组件和持卡人数据：						
	▪ 是否制定了针对访问控制的书面政策且其中包含以下方面？ • 为每个角色定义访问需要和权限分配 • 将特权用户 ID 的访问权限限制为执行工作所需的最小权限， • 基于个人的工作分类和职能分配访问权限 • 被授权方对所有访问的审批记录（电子或书面形式），包括获批的特定权限列表	▪ 检查书面访问控制政策	☐	☐	☐	☐	☐
7.1.1	是否为每个角色定义了访问需要，包括： ▪ 每个角色依据工作职能需要访问的系统组件和数据资源？ ▪ 访问资源所需的权限级别（例如用户、管理员等）？	▪ 检查角色和访问需求	☐	☐	☐	☐	☐
7.1.2	是否按照下述要求对特权用户 ID 的访问权限进行了限制： ▪ 限制为执行工作所需的最小权限？ ▪ 只分配给明确需要此类特权访问的角色？	▪ 与工作人员面谈 ▪ 与管理人员面谈 ▪ 审核特权用户 ID	☐	☐	☐	☐	☐
7.1.3	是否基于个人的工作分类和职能分配了访问权限？	▪ 与管理人员面谈 ▪ 审核用户 ID	☐	☐	☐	☐	☐
7.1.4	是否需要由指定所需权限的被授权方作出书面批准？	▪ 审核用户 ID ▪ 与书面批准进行对比 ▪ 对比分配的权限与书面批准是否相符	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
7.2	是否按照下述要求为系统组件建立了访问控制系统，以根据用户的知情需要限制访问，并将系统设为“全部拒绝”（特别允许访问时除外）：						
7.2.1	是否为所有系统组件建立了访问控制系统？	▪ 审核供应商文档 ▪ 检查配置设置	☐	☐	☐	☐	☐
7.2.2	访问控制系统是否配置为基于工作分类和职能执行个人权限分配？	▪ 审核供应商文档 ▪ 检查配置设置	☐	☐	☐	☐	☐
7.2.3	访问控制系统是否默认设为“全部拒绝”？	▪ 审核供应商文档 ▪ 检查配置设置	☐	☐	☐	☐	☐
7.3	用于限制对持卡人数据的访问的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 检查安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

要求 8：　　识别并验证对系统组件的访问

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
8.1	是否按照下述要求针对所有系统组件中的非消费者用户和管理员规定并实施了用户识别管理控制政策和程序：						
8.1.1	在允许任何用户访问系统组件或持卡人数据前，是否为他们分配了唯一的用户 ID？	▪ 审核密码程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
8.1.2	是否已对用户 ID、凭证和其他标识符对象的添加、删除和修改进行控制，以便只有授权人员（包括具有指定权限）才能执行用户 ID 操作？	▪ 审核密码程序 ▪ 检查特权和普通用户 ID 以及相关授权 ▪ 查看系统设置	☐	☐	☐	☐	☐
8.1.3	是否已立即撤销或删除任何到期用户的访问权限？	▪ 审核密码程序 ▪ 检查到期用户帐户 ▪ 审核当前访问权限列表 ▪ 查看已退回的物理验证设备	☐	☐	☐	☐	☐
8.1.4	是否在 90 天内删除或禁用了无活动的用户帐户？	▪ 审核密码程序 ▪ 查看用户帐户	☐	☐	☐	☐	☐
8.1.5	(a) 是否仅在需要的时间段启用并在不用时禁用第三方用于通过远程访问来访问、支持或维护系统组件的帐户？	▪ 审核密码程序 ▪ 与工作人员面谈 ▪ 查看流程	☐	☐	☐	☐	☐
	(b) 是否对处于使用中的第三方远程访问帐户进行了监控？	▪ 与工作人员面谈 ▪ 查看流程	☐	☐	☐	☐	☐
8.1.6	(a) 是否通过在不超过 6 次尝试后锁定用户 ID 以限制反复访问尝试？	▪ 审核密码程序 ▪ 检查系统配置设置	☐	☐	☐	☐	☐
	(b) *此测试程序仅适用于服务提供商。*						

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
8.1.7	是否将用户帐户的锁定时间设为最少 30 分钟或直到管理员启用该用户 ID？	▪ 审核密码程序 ▪ 检查系统配置设置	☐	☐	☐	☐	☐
8.1.8	如果会话空闲时间超过 15 分钟，用户是否需要重新验证（例如，重新输入密码）或者重新激活终端或会话？	▪ 审核密码程序 ▪ 检查系统配置设置	☐	☐	☐	☐	☐
8.2	除了分配唯一 ID 以外，是否采用以下一种或多种方法来验证所有用户？ ▪ 所知，如密码或口令等 ▪ 所有，如令牌设备或智能卡等 ▪ 个人特征，如生物特征	▪ 审核密码程序 ▪ 查看验证流程	☐	☐	☐	☐	☐
8.2.1	(a) 是否使用了强效加密法以使所有验证凭证（例如密码/口令）在所有系统组件中传输和存储时均不可读？	▪ 审核密码程序 ▪ 审核供应商文档 ▪ 检查系统配置设置 ▪ 查看密码文件 ▪ 查看数据传输	☐	☐	☐	☐	☐
	(b) *此测试程序仅适用于服务提供商。*						
8.2.2	是否在修改任何验证凭证（例如，执行密码重置、提供新令牌或生成新密钥）前验证了用户身份？	▪ 审核验证程序 ▪ 查看人员	☐	☐	☐	☐	☐
8.2.3	(a) 用户密码参数是否配置为要求密码/口令满足以下要求？ • 密码长度至少为七个字符 • 同时包含数字和字母字符 或者，密码/口令必须具有至少与上面指定参数相当的复杂度和强度。	▪ 检查系统配置设置以验证密码参数	☐	☐	☐	☐	☐
	(b) *此测试程序仅适用于服务提供商。*						

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
8.2.4	(a) 是否至少每 90 天变更一次用户密码/口令？	▪ 审核密码程序 ▪ 检查系统配置设置	☐	☐	☐	☐	☐
	(b) *此测试程序仅适用于服务提供商。*						
8.2.5	(a) 个人提交的新密码/口令是否不得与最近所用的 4 个密码/口令相同？	▪ 审核密码程序 ▪ 系统组件采样 ▪ 检查系统配置设置	☐	☐	☐	☐	☐
	(b) *此测试程序仅适用于服务提供商。*						
8.2.6	是否将每个用户的首次使用密码/口令和重置密码/口令设为唯一值，并要求每个用户在首次使用后立即变更？	▪ 审核密码程序 ▪ 检查系统配置设置 ▪ 查看安全人员	☐	☐	☐	☐	☐
8.3	是否使用如下所述的多因素验证保护对 CDE 的所有单独非控制台管理访问和所有远程访问： ***注：****多因素验证要求在验证过程中至少使用三种验证方法中的其中两种（有关验证方法的说明，请参见 PCI DSS 要求 8.2）。使用一个因素两次（例如，使用两个不同的密码）不视为多因素验证。*						
8.3.1	是否针对所有非控制台访问在针对具有管理访问权限的工作人员的 CDE 中加入了多因素验证？ ***注：****本要求在 2018 年 1 月 31 日前属于最优方法，此后将成为一项要求。*	▪ 检查系统配置 ▪ 查看登录 CDE 的管理员	☐	☐	☐	☐	☐
8.3.2	是否针对来自该实体网络外部的所有远程网络访问（针对用户和管理员，并包括出于支持或维护目的的第三方访问）加入了多因素验证？	▪ 检查系统配置 ▪ 查看远程连接工作人员	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
8.4	(a) 是否已为所有用户记录并向其传达了验证政策和程序？	▪ 审核相关政策和程序 ▪ 审核分配方法 ▪ 与工作人员面谈 ▪ 与用户面谈	☐	☐	☐	☐	☐
	(b) 验证政策和程序是否包含以下方面？ • 选择强效验证凭证的指南 • 关于用户应如何保护其验证凭证的指南 • 关于不重用之前用过的密码的说明 • 关于用户如怀疑密码可能暴露则应修改密码的说明	▪ 审核相关政策和程序 ▪ 审核提供给用户的文档	☐	☐	☐	☐	☐
8.5	是否按照下述要求禁用了群组、共享或常规帐户、密码或其他验证方法： • 禁用或删除了常规用户 ID； • 用于系统管理活动和其他重要功能的共享用户 ID 不存在；以及 • 不使用共享和常规用户 ID 管理任何系统组件？	▪ 审核相关政策和程序 ▪ 检查用户 ID 列表 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
8.5.1	*此要求仅适用于服务提供商。*						
8.6	在使用其他验证机制（例如物理或逻辑安全令牌、智能卡、证书等）的情形下，是否按照下述要求分配了这些机制的用法？ • 验证机制必须分配到单个帐户，不得在多个帐户之间共享 • 必须要有物理和/或逻辑控制，以确保仅既定帐户可使用该机制获得权限	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 检查系统配置设置和/或物理控制	☐	☐	☐	☐	☐
8.7	是否按照下述要求限制了对任何包含持卡人数据的数据库的所有访问（包括应用程序、管理员和其他所有用户的访问）：						

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
	(a) 用户对数据库的所有访问、查询和操作（例如，移动、复制、删除）是否都只能通过编程方法（例如，通过存储的程序）完成？	▪ 审核数据库验证政策和程序 ▪ 检查数据库和应用程序配置设置	☐	☐	☐	☐	☐
	(b) 是否只有数据库管理员拥有用户直接访问或查询数据库的权限？	▪ 审核数据库验证政策和程序 ▪ 检查数据库访问控制设置 ▪ 检查数据库应用程序配置设置	☐	☐	☐	☐	☐
	(c) 应用程序 ID 是否仅可由这些应用程序使用（个人用户或其他流程不能使用）？	▪ 审核数据库验证政策和程序 ▪ 检查数据库访问控制设置 ▪ 检查数据库应用程序配置设置	☐	☐	☐	☐	☐
8.8	用于识别和验证的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 检查安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

要求 9：　限制对持卡人数据的物理访问

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
9.1	是否实施了适当的场所入口控制，以对物理访问持卡人数据环境中的系统进行限制和监控？	▪ 查看物理访问控制 ▪ 查看人员	☐	☐	☐	☐	☐
9.1.1	(a) 是否已使用摄像头和/或访问控制机制监控对敏感区域的个人物理访问？ ***注：****"敏感区域"指任何数据中心、服务器室或任何存储、处理或传输持卡人数据的系统所在区域。这不包括仅有销售点终端的公共区域，例如零售店的收银区。*	▪ 审核相关政策和程序 ▪ 查看物理监控机制 ▪ 查看安全功能	☐	☐	☐	☐	☐
	(b) 摄像头和/或访问控制机制是否受到安全保护以免遭到破坏或禁用？	▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(c) 通过摄像头和/或访问控制机制采集的数据是否经过核查并与其他条目关联？	▪ 审核相关政策和程序 ▪ 与安全人员面谈	☐	☐	☐	☐	☐
	(d) 通过摄像头和/或访问控制机制采集的数据是否至少存储了三个月（除非法律另有规定）？	▪ 审核数据保留流程 ▪ 查看数据存储 ▪ 与安全人员面谈	☐	☐	☐	☐	☐
9.1.2	是否已实施物理和/或逻辑控制，以限制对公共网络插座交换机的访问？ *例如，位于公共区域和访客可进入区域的网络插座交换机可能被禁用，并且仅在明确授权进行网络访问时才能启用。或者，也可以实施相应流程，以确保访客处在网络插座交换机正在运行的区域时始终有人陪同。*	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 查看位置	☐	☐	☐	☐	☐
9.1.3	对无线接入点、网关、手持式设备、网络/通信硬件和电信线路的物理访问是否受到限制？	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 查看设备	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
9.2	(a) 是否制定了相关程序以轻松识别现场工作人员和访客，包括： • 识别现场工作人员或访客（例如发放工卡）， • 修改访问要求，以及 • 废除已离职现场工作人员和过期访客的身份证件（例如工卡） *在要求 9 中，"现场工作人员"指出现在实体经营场所的全职和兼职员工、临时工、承包商和顾问。"访客"指供应商、任何现场工作人员的客人、服务工人，或任何需要短时进入经营场所的人员，停留时间通常不超过一天。*	▪ 审核相关政策和程序 ▪ 与工作人员面谈 ▪ 查看识别方法（例如工卡） ▪ 查看访客流程	☐	☐	☐	☐	☐
	(b) 身份识别方法（例如工卡）能否清楚地识别访客并轻松区分现场工作人员和访客？	▪ 查看识别方法	☐	☐	☐	☐	☐
	(c) 是否只有授权人员拥有工卡系统的访问权限？	▪ 查看针对工卡系统的物理控制和访问控制	☐	☐	☐	☐	☐
9.3	是否按照下述要求对现场工作人员物理访问敏感区域进行了控制： ▪ 访问权限是否经过授权且基于个人的工作职能？ ▪ 是否在相关人员离职后立即撤销其访问权限？ ▪ 是否在相关人员离职后退回或禁用所有物理访问机制（例如钥匙、访问卡等）？	▪ 与工作人员面谈 ▪ 检查访问控制列表 ▪ 查看现场工作人员 ▪ 对比离职人员名单和访问控制列表	☐	☐	☐	☐	☐
9.4	是否按照下述要求处理访客识别和访问权限：						
9.4.1	访客在进入处理或维护持卡人数据的区域前是否需要获得批准且在进入后是否始终有人陪同？	▪ 审核相关政策和程序 ▪ 查看访客流程（包括访问控制方式） ▪ 与工作人员面谈 ▪ 查看访客和工卡使用情况	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
9.4.2	(a) 是否识别了访客并给访客发放了工卡或能识别访客为非现场工作人员的其他身份证件？	▪ 查看工作人员和访客的工卡使用情况 ▪ 检查识别情况	☐	☐	☐	☐	☐
	(b) 访客工卡或其他身份证件是否已到期？	▪ 查看流程 ▪ 检查识别情况	☐	☐	☐	☐	☐
9.4.3	是否要求访客在离开场所或证件到期时交还工卡或其他身份证件？	▪ 查看流程 ▪ 查看离开场所的访客	☐	☐	☐	☐	☐
9.4.4	(a) 是否正在使用访客日志记录对经营场所以及存储或传输持卡人数据的计算机房和数据中心的物理访问？	▪ 审核相关政策和程序 ▪ 检查访客日志 ▪ 查看访客流程 ▪ 检查日志保留情况	☐	☐	☐	☐	☐
	(b) 访客日志中是否包含访客的姓名、代表的公司以及批准物理访问的现场工作人员姓名？	▪ 审核相关政策和程序 ▪ 检查访客日志	☐	☐	☐	☐	☐
	(c) 访客日志是否至少保留了三个月？	▪ 审核相关政策和程序 ▪ 检查访客日志保留情况	☐	☐	☐	☐	☐
9.5	是否已采取措施来保护所有媒介实体安全（包括但不限于计算机、可移动电子媒介、纸质收据、纸质报告和传真）？ *在要求 9 中，“媒介”指所有包含持卡人数据的纸质和电子媒介。*	▪ 审核用于保护媒介实体安全的政策和程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
9.5.1	是否至少每年审查一次存储媒体备份的位置，以确认存储的安全性？	▪ 审核针对检查非现场媒介位置的政策和程序 ▪ 与安全人员面谈	☐	☐	☐	☐	☐
9.6	(a) 是否严格控制任何媒介的内部或外部分发？	▪ 审核针对媒介分发的政策和程序	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
	(b) 相关控制是否包含以下方面：						
9.6.1	是否已对媒介进行分类以便确定数据的敏感性？	▪ 审核针对媒介分类的政策和程序 ▪ 与安全人员面谈	☐	☐	☐	☐	☐
9.6.2	媒介是否通过可靠的快递公司或可准确跟踪的其他投递方法发出？	▪ 与工作人员面谈 ▪ 检查媒介分发跟踪日志和文档	☐	☐	☐	☐	☐
9.6.3	转移媒介时（尤其是将媒介分发给个人时）是否经过管理层的批准？	▪ 与工作人员面谈 ▪ 检查媒介分发跟踪日志和文档	☐	☐	☐	☐	☐
9.7	是否严格控制对媒介的存储和获取？	▪ 审核相关政策和程序	☐	☐	☐	☐	☐
9.7.1	(a) 是否适当维护了所有媒介的盘存记录？	▪ 检查盘存记录	☐	☐	☐	☐	☐
	(b) 是否定期盘点媒介（至少每年一次）？	▪ 检查盘存记录 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
9.8	(a) 是否销毁了因业务或法律原因而不再需要的所有媒介？	▪ 审核媒介定期销毁政策和程序	☐	☐	☐	☐	☐
	(b) 是否制定了包含下述要求的媒介定期销毁政策？ • 硬拷贝材料必须粉碎、焚烧或打浆，以合理保证这些硬拷贝材料无法重建。 • 用于存放待销毁材料的容器必须安全。 • 电子媒介上的持卡人数据必须呈现不可恢复状态（例如，通过符合行业认可的安全删除标准的安全擦除程序，或者通过销毁媒介实体来实现）。	▪ 审核媒介定期销毁政策和程序	☐	☐	☐	☐	☐
	(c) 是否按照下述要求销毁媒介：						

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
9.8.1	(a) 硬拷贝材料是否已被粉碎、焚烧或打浆以确保无法重建持卡人数据？	▪ 与工作人员面谈 ▪ 检查程序 ▪ 查看流程	☐	☐	☐	☐	☐
	(b) 是否已确保待销毁材料所用存储容器的安全性以免他人访问相关内容？	▪ 检查存储容器的安全性	☐	☐	☐	☐	☐
9.8.2	电子媒介上的持卡人数据是否呈现不可恢复状态（例如，通过符合行业认可的安全删除标准的安全擦除程序，或者通过销毁媒介实体来实现），以确保无法重建持卡人数据？	▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
9.9	是否已按照下述要求保护通过直接接触卡本身便可捕获支付卡数据的设备以免其被篡改和替换？ ***注：****此要求适用于销售点实卡交易（即刷卡）中使用的读卡设备。本要求不适用于手动密钥输入组件，如计算机键盘和 POS 机键盘。*						
	(a) 相关政策和程序是否要求维护此类设备列表？	▪ 审核相关政策和程序	☐	☐	☐	☐	☐
	(b) 相关政策和程序是否要求定期检查设备以查找篡改或替换迹象？	▪ 审核相关政策和程序	☐	☐	☐	☐	☐
	(c) 相关政策和程序是否要求培训工作人员，以确保其了解可疑行为和举报篡改或替换设备行为？	▪ 审核相关政策和程序	☐	☐	☐	☐	☐
9.9.1	(a) 设备列表是否包含以下方面？ • 设备的外形、型号 • 设备位置（例如安放设备的现场或设施的地址） • 设备的序列号或其他独特验证方法	▪ 检查设备列表	☐	☐	☐	☐	☐
	(b) 该列表是否准确且已及时更新？	▪ 查看设备及设备位置，并与该列表进行对比	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
	(c) 设备列表是否随着设备的新增、更换位置、停用等进行更新？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
9.9.2	(a) 是否按照下述要求定期检查设备表面，以查找篡改（例如为设备增加读卡器）或替换（例如通过检查序列号或其他设备特征确认其未被欺诈性设备调换）迹象？ ***注：****设备可能被篡改或替换的迹象包括：不明附件或有线缆连接到设备，安全标签丢失或改变，外壳破损或颜色不同，序列号或其他外部标记改变。*	▪ 与工作人员面谈 ▪ 查看检查流程并与规定的流程进行对比	☐	☐	☐	☐	☐
	(b) 工作人员是否了解设备的检查程序？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
9.9.3	是否已按照下述要求培训工作人员，使其了解尝试篡改或替换设备的行为？						
	(a) 针对销售点所在地工作人员的培训材料是否包含以下方面？ • 在允许对设备进行调整或修理之前，验证任何自称修理或维护人员的第三方人员的身份。 • 在未经验证的情况下，不要安装、替换或退还设备。 • 注意设备周围的可疑行为（例如，陌生人尝试拔掉设备插头或打开设备）。 • 向相关人员（例如，经理或安全人员）报告篡改或替换设备的可疑行为和迹象。	▪ 审核培训材料	☐	☐	☐	☐	☐
	(b) 是否已培训销售点所在地的工作人员，使其了解用于检测和报告尝试篡改或替换设备行为的程序？	▪ 与 POS 所在地的工作人员面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
9.10	用于限制对持卡人数据的物理访问的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 检查安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

定期监控并测试网络

要求 10：　　跟踪并监控对网络资源和持卡人数据的所有访问

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
10.1	(a) 系统组件的检查记录是否已启用且处于活动状态？	▪ 查看流程 ▪ 与系统管理员面谈	☐	☐	☐	☐	☐
	(b) 对系统组件的访问是否已链接到个人用户？	▪ 查看流程 ▪ 与系统管理员面谈	☐	☐	☐	☐	☐
10.2	是否对所有系统组件实施了自动检查记录以重建以下事件：						
10.2.1	对持卡人数据的所有个人用户访问？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.2.2	任何具有 root 或管理员权限的个人执行的所有操作？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.2.3	对所有检查记录的访问？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.2.4	无效的逻辑访问尝试？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.2.5	识别和验证机制的使用和变更（包括但不限于新建帐户和提升权限）以及具有 root 或管理员权限帐户的所有变更、添加或删除？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
10.2.6	检查日志的初始化、关闭或暂停？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.2.7	系统级对象的创建和删除？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.3	是否已针对每次事件记录所有系统组件的以下检查记录条目：						
10.3.1	用户识别？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.3.2	事件类型？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.3.3	日期和时间？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.3.4	成功或失败指示？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.3.5	事件的起因？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
10.3.6	受影响的数据、系统组件或资源的特性或名称？	▪ 与工作人员面谈 ▪ 查看检查日志 ▪ 检查检查日志设置	☐	☐	☐	☐	☐
10.4	是否已使用最新的时间同步技术来同步所有关键系统的时钟和时间？ ***注：****网络时间协议 (NTP) 便是一种时间同步技术。*	▪ 审核时间配置标准和流程	☐	☐	☐	☐	☐
10.4.1	是否实施了以下流程以确保关键系统的时间正确且一致：						
	(a) 是否只有指定的中央时间服务器能接收外来的时间信号，且外来的时间信号以国际原子时或 UTC 为基础？	▪ 审核时间配置标准和流程 ▪ 检查与时间相关的系统参数	☐	☐	☐	☐	☐
	(b) 当存在多个指定时间服务器时，这些时间服务器是否会相互同步以保持时间准确？	▪ 审核时间配置标准和流程 ▪ 检查与时间相关的系统参数	☐	☐	☐	☐	☐
	(c) 系统是否只会接收来自指定中央时间服务器的时间信息？	▪ 审核时间配置标准和流程 ▪ 检查与时间相关的系统参数	☐	☐	☐	☐	☐
10.4.2	是否按照下述要求保护时间数据： (a) 是否只有具有相应业务需要的人员才能访问时间数据？	▪ 检查系统配置和时间同步设置	☐	☐	☐	☐	☐
	(b) 是否已记录、监控并审核关键系统中时间设置的任何变更？	▪ 检查系统配置和时间同步设置及记录	☐	☐	☐	☐	☐
10.4.3	时间设置是否来自行业认可的特定时间来源？（这是为了防止恶意个人更改时钟。） *可选择性地使用对称密钥加密此类更新，并创建访问控制列表指定客户端计算机（会接收时间更新）的 IP 地址（以防止内部时间服务器的非授权使用）。*	▪ 检查系统配置	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
10.5	是否已按下述要求保护检查记录以防被更改：						
10.5.1	是否只允许有工作需要的人查看检查日志？	▪ 与系统管理员面谈 ▪ 检查系统配置和许可	☐	☐	☐	☐	☐
10.5.2	是否已通过访问控制机制、物理隔离和/或网络隔离保护检查记录文件免遭非授权修改？	▪ 与系统管理员面谈 ▪ 检查系统配置和许可	☐	☐	☐	☐	☐
10.5.3	是否已即时将检查记录文件备份到难以更改的中央日志服务器或媒介中？	▪ 与系统管理员面谈 ▪ 检查系统配置和许可	☐	☐	☐	☐	☐
10.5.4	是否已将向外技术的日志写入安全的内部中央日志服务器或媒介中？	▪ 与系统管理员面谈 ▪ 检查系统配置和许可	☐	☐	☐	☐	☐
10.5.5	是否已对日志使用文件完整性监控或变更检测软件，以确保未生成警报时无法变更现有日志数据（虽然新增数据不应生成警报）？	▪ 检查设置、受监控文件和监控活动结果	☐	☐	☐	☐	☐
10.6	是否已按照下述要求审核所有系统组件的日志和安全事件以识别异常情况或可疑活动？ ***注：****可使用日志搜集、分析和告警工具来满足要求 10.6。*						
10.6.1	(a) 是否手动或通过日志工具制定了书面政策和程序，以至少每天审核一次以下内容？ • 所有安全事件 • 存储、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 • 执行安全功能的所有服务器和系统组件（例如，防火墙、入侵检测系统/入侵防御系统 (IDS/IPS)、验证服务器、电子商务重定向服务器等）的日志	▪ 审核安全政策和程序	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
	(b) 是否至少每天审核一次上述日志和安全事件？	▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
10.6.2	(a) 是否手动或通过日志工具制定了书面政策和程序，以根据组织的政策和风险管理策略定期审核所有其他系统组件的日志？	▪ 审核安全政策和程序	☐	☐	☐	☐	☐
	(b) 是否已根据组织的政策和风险管理策略审核所有其他系统组件？	▪ 审核风险评估文档 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
10.6.3	(a) 是否制定了书面政策和程序，以跟进审核过程中所发现的例外和异常情况？	▪ 审核安全政策和程序	☐	☐	☐	☐	☐
	(b) 是否已跟进例外和异常情况？	▪ 查看流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
10.7	(a) 是否制定了检查日志政策和程序并要求保留检查记录至少一年，且其中最少 3 个月的记录可立即访问以供分析（例如，在线、存档或可从备份恢复）？	▪ 审核安全政策和程序	☐	☐	☐	☐	☐
	(b) 检查记录是否保留了至少一年？	▪ 与工作人员面谈 ▪ 检查检查日志	☐	☐	☐	☐	☐
	(c) 是否有最少 3 个月的记录可立即访问以供分析？	▪ 与工作人员面谈 ▪ 查看流程	☐	☐	☐	☐	☐
10.8	*此要求仅适用于服务提供商*						
10.9	用于监控所有网络资源和持卡人数据访问的安全政策和操作程序是否： ▪ 已记录 ▪ 处于使用中 ▪ 为所有相关方了解？	▪ 审核安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

要求 11：　　定期测试安全系统和流程

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
11.1	(a) 是否已实施了流程以按季度检测和识别所有授权和非授权的无线接入点？ ***注：****可用于该流程的方法包括但不限于无线网络扫描、系统组件和基础架构的物理/逻辑检查、网络访问控制 (NAC) 或无线 IDS/IPS。* *无论使用何种方法，都必须足以检测并识别任何非授权设备。*	▪ 审核相关政策和程序	☐	☐	☐	☐	☐
	(b) 所用方法是否能够检测并识别任何非授权无线接入点（其中至少包括以下项）？ • 插入系统组件中的 WLAN 卡； • 连接到系统组件以创建无线接入点（例如通过 USB 等）的便携或移动设备；以及 • 连接到网络端口或网络设备的无线设备。	▪ 评估该方法	☐	☐	☐	☐	☐
	(c) 如果使用无线扫描来识别授权和非授权无线访问点，是否至少每季度扫描一次所有系统组件和设施？	▪ 检查最近的无线扫描结果	☐	☐	☐	☐	☐
	(d) 如果采用自动监控（例如无线 IDS/IPS、NAC 等），是否配置为会发出警报来通知工作人员？	▪ 检查配置设置	☐	☐	☐	☐	☐
11.1.1	是否已保留一份授权无线接入点清单，且所有授权无线接入点均具有业务理由记录？	▪ 检查清单记录	☐	☐	☐	☐	☐
11.1.2	(a) 是否制定了事故响应计划，且其中要求在检测到非授权无线接入点时需做出响应？	▪ 检查事故响应计划（参见要求 12.10）	☐	☐	☐	☐	☐
	(b) 是否已在发现非授权无线接入点时采取措施？	▪ 与负责人面谈 ▪ 检查最近的无线扫描和相关响应	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
11.2	是否按照下述要求至少每个季度运行一次内部和外部网络漏洞扫描，并在网络发生任何重大变化（例如安装新的系统组件、更改网络拓朴、修改防火墙规则、产品升级）时也运行漏洞扫描？ ***注：****可在季度扫描流程中综合多次扫描报告，以表明所有系统均已扫描，且所有漏洞均已解决。可能需要其他文档记录来确认解决过程中有未修复的漏洞。* *如果评估商确认 1) 最近的扫描结果为通过，2) 实体具备要求每季度扫描一次的书面政策和程序，3) 扫描结果中指出的漏洞在重新扫描中显示为已修复，则不要求四次季度扫描均通过才能认定最初 PCI DSS 合规。在最初 PCI DSS 审核后的几年里，必须出现四次季度扫描结果均为通过的情况。*							
11.2.1	(a) 是否每个季度运行了一次内部漏洞扫描？	▪ 审核扫描报告	☐	☐	☐	☐	☐
	(b) 每季度一次的内部扫描流程能否解决所有“高风险”漏洞，并包含重新扫描，以确认所有“高风险”漏洞（见 PCI DSS 要求 6.1 中的定义）均得到解决？	▪ 审核扫描报告	☐	☐	☐	☐	☐
	(c) 每季度一次的内部扫描是否由合格的内部人员或合格的外部第三方执行，且（如果适用）确保测试者的组织独立性（不要求是 QSA 或 ASV）？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
11.2.2	(a) 是否每个季度运行了一次外部漏洞扫描？ ***注：****季度外部漏洞扫描必须由支付卡行业安全标准委员会 (PCI SSC) 认证的授权扫描服务商 (ASV) 执行。* *如需了解扫描客户的责任、扫描准备等，请参阅 PCI SSC 网站上发布的《ASV 计划指南》。*	▪ 审核最近四个季度的外部漏洞扫描结果	☐	☐	☐	☐	☐
	(b) 每个季度的外部扫描和重复扫描结果是否符合 *ASV 计划指南*对扫描通过的要求（例如不存在 CVSS 评级为 4.0 或以上的漏洞或无自动故障）？	▪ 审核每个季度的外部扫描和重复扫描结果	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
	(c) 季度外部漏洞扫描是否由 PCI SSC 认证的授权扫描服务商 (ASV) 执行？	▪ 审核每个季度的外部扫描和重复扫描结果	☐	☐	☐	☐	☐
11.2.3	(a) 是否在发生任何重要变更后执行内部和外部扫描，并视需要执行重复扫描？ ***注：****必须由合格人员执行扫描。*	▪ 检查并关联变更控制文档和扫描报告	☐	☐	☐	☐	☐
	(b) 扫描流程是否包括重复扫描，直至： • 外部扫描不存在 CVSS 评级为 4.0 或以上的漏洞， • 内部扫描获得扫描通过，或 PCI DSS 要求 6.1 中定义的所有“高风险”漏洞均得以解决？	▪ 审核扫描报告	☐	☐	☐	☐	☐
	(c) 扫描是否由合格的内部人员或合格的外部第三方执行，且（如果适用）确保测试者的组织独立性（不要求是 QSA 或 ASV）？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
11.3	穿透测试法是否包括以下方面？ ▪ 以行业认可的穿透测试法为基础（例如 NIST SP800-115） ▪ 覆盖整个 CDE 环境和关键系统 ▪ 来自网络内部和外部的测试 ▪ 用于验证任何网段和范围缩小控制的测试 ▪ 定义应用层穿透测试，至少包括要求 6.5 中列出的漏洞 ▪ 定义网络层穿透测试，包括支持网络功能和操作系统的组件 ▪ 审核并考虑过去 12 个月内遇到的威胁和漏洞 ▪ 指明保留穿透测试结果和修复活动结果	▪ 检查穿透测试法 ▪ 与负责人面谈	☐	☐	☐	☐	☐
11.3.1	(a) 是否每年至少按照规定的方法执行一次*外部*穿透测试，并在环境发生任何重大的基础架构或应用程序变更时（例如操作系统升级、环境新增子网络或环境新增网络服务器）也执行该测试？	▪ 检查工作范围 ▪ 检查最近一次外部穿透测试的结果	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
	(b) 测试是否由合格的内部人员或合格的外部第三方执行，且（如果适用）确保测试者的组织独立性（不要求是 QSA 或 ASV）？	▪ 与负责人面谈	☐	☐	☐	☐	☐
11.3.2	(a) 是否每年至少按照规定的方法执行一次*内部*穿透测试，并在环境发生任何重大的基础架构或应用程序变更时（例如操作系统升级、环境新增子网络或环境新增网络服务器）也执行该测试？	▪ 检查工作范围 ▪ 检查最近一次内部穿透测试的结果	☐	☐	☐	☐	☐
	(b) 测试是否由合格的内部人员或合格的外部第三方执行，且（如果适用）确保测试者的组织独立性（不要求是 QSA 或 ASV）？	▪ 与负责人面谈	☐	☐	☐	☐	☐
11.3.3	在穿透测试中发现的可利用漏洞是否已得到修复，且已通过重复执行的测试确认修复？	▪ 检查穿透测试结果	☐	☐	☐	☐	☐
11.3.4	如果利用网络分段将 CDE 与其他网络隔离：						
	(a) 是否已规定用于测试所有分段方法的穿透测试程序以确认其行之有效，并已将所有范围外系统与 CDE 内的系统隔离？	▪ 检查分段控制 ▪ 审核穿透测试法	☐	☐	☐	☐	☐
	(b) 用于验证分段控制的穿透测试是否满足下述要求？ • 至少每年执行一次，且在分段控制/方法发生任何变更后也执行 • 覆盖使用中的所有分段控制/方法 • 确认分段方法行之有效并隔离所有范围外系统与 CDE 内的系统。	▪ 检查最近一次穿透测试的结果	☐	☐	☐	☐	☐
	(c) 测试是否由合格的内部人员或合格的外部第三方执行，且（如果适用）确保测试者的组织独立性（不要求是 QSA 或 ASV）？	▪ 与负责人面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
11.3.4.1	*此要求仅适用于服务提供商*						
11.4	(a) 是否已采用用于检测和/或防御网络入侵的入侵检测和/或入侵防御技术　以监控所有流量： • 持卡人数据环境周围，和 • 持卡人数据环境中的关键点。	▪ 检查系统配置 ▪ 检查网络图	☐	☐	☐	☐	☐
	(b) 入侵检测和/或入侵防御技术是否配置为会在发现可疑威胁时向工作人员发出警报？	▪ 检查系统配置 ▪ 与负责人面谈	☐	☐	☐	☐	☐
	(c) 是否已及时更新所有入侵检测和防御引擎、基线和签名？	▪ 检查 IDS/IPS 配置 ▪ 检查供应商文档	☐	☐	☐	☐	☐
11.5	(a) 是否部署了变更检测机制（例如文件完整性监控工具），以检测关键系统文件、配置文件或内容文件的非授权修改（包括更改、添加和删除）？ *应受监控的文件包括：* • *系统可执行文件* • *应用程序可执行文件* • *配置和参数文件* • *集中存储文件、历史或归档文件、日志和检查文件* • *由实体（例如，通过风险评估或其他方法）确定的其他重要文件*	▪ 查看系统设置和受监控文件 ▪ 检查系统配置设置	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
	(b) 变更检测机制是否已配置为可在重要的系统文件、配置文件或内容文件出现非授权修改时（包括更改、添加和删除）警示工作人员，并至少每周执行一次重要文件比对？ ***注：****在变更检测中，重要文件通常指那些不经常变更但一旦变更即表示系统受到威胁或面临威胁风险的文件。变更检测机制（例如文件完整性监控产品）通常预先配置了相关操作系统的重要文件。其他重要文件（例如自定义应用程序的重要文件）必须由该实体（即商户或服务提供商）评估和定义。*	▪ 查看系统设置和受监控文件 ▪ 审核监控活动结果	☐	☐	☐	☐	☐
11.5.1	是否已实施流程，以针对变更检测解决方案发出的任何警报做出响应？	▪ 检查系统配置设置	☐	☐	☐	☐	☐
11.6	用于安全监控和测试的安全政策和操作程序是否： • 已记录 • 处于使用中 • 为所有相关方了解？	▪ 检查安全政策和操作程序 ▪ 与工作人员面谈	☐	☐	☐	☐	☐

维护信息安全政策

要求 12：　　维护针对所有工作人员的信息安全政策

注：*在要求 12 中，"工作人员"指"常驻"实体经营场所或能够以其他方式访问该公司的持卡人数据环境现场的全职和兼职员工、临时工和工作人员、承包商和顾问。*

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
12.1	是否已建立、公布、维护并向所有相关人员宣传安全政策？	▪ 审核相关信息安全政策	☐	☐	☐	☐	☐
12.1.1	是否至少每年审核一次安全政策，并在环境发生变更时进行更新？	▪ 审核相关信息安全政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.2	(a) 是否已实施每年一次的风险评估流程以 • 确定重要资产、威胁和漏洞，并 • 形成正式的书面风险分析？ *风险评估方法包括但不限于 OCTAVE、ISO 27005 和 NIST SP 800-30。*	▪ 审核每年一次的风险评估流程 ▪ 与工作人员面谈	☐	☐	☐	☐	☐
	(b) 是否至少每年执行一次风险评估流程，并在环境发生重大变更时（例如收购、合并、迁址等）也执行评估？	▪ 审核风险评估文档 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3	是否已制定关键技术的使用政策，以规定这些技术的正确用法并包含以下方面： ***注：****关键技术包括但不限于，远程访问和无线技术、笔记本电脑、平板电脑、可移动电子媒介以及电子邮件和互联网的使用。*						
12.3.1	被授权方明确允许使用这些技术？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3.2	技术使用验证？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
12.3.3	一份列出所有此类设备和具有访问权的工作人员的列表？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3.4	一种确定负责人、联系信息和用途（例如设备的贴标、编码和/或盘存）的准确方便的方法？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3.5	可接受的技术使用方式？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3.6	技术可接受的网络位置？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3.7	公司批准的产品列表？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3.8	非活跃状态持续一定时间后自动中断远程访问技术的会话？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3.9	仅在供应商和业务合作伙伴需要时为其激活远程访问技术，并在使用后立即停用？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.3.10	(a) 对于通过远程访问技术访问持卡人数据的工作人员，政策是否指明除非因规定的业务需要获得明确许可，否则禁止将持卡人数据复制、移动和存储到本地硬盘及可移动电子媒介上？ *如果有经批准的业务需要，使用政策必须规定应按照所有适用的 PCI DSS 要求保护数据。*	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
	(b) 对于获得适当授权的工作人员，政策是否规定必须按照 PCI DSS 要求保护持卡人数据？	▪ 审核使用政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.4	安全政策和程序是否明确规定所有工作人员的信息安全责任？	▪ 审核信息安全政策和程序 ▪ 抽样选取部分负责人员进行面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
12.4.1	*此要求仅适用于服务提供商*						
12.5	(a) 是否已将信息安全职责正式分配给首席安全官或其他具有丰富安全知识的管理人员？	▪ 审核信息安全政策和程序	☐	☐	☐	☐	☐
	(b) 是否已将下列信息安全管理职责正式分配给个人或团队：						
12.5.1	制定、记录并分发安全政策和程序？	▪ 审核信息安全政策和程序	☐	☐	☐	☐	☐
12.5.2	监控和分析安全警报及信息，以及向适当的人员分发信息？	▪ 审核信息安全政策和程序	☐	☐	☐	☐	☐
12.5.3	建立、记录并分发安全事故响应和逐级上报程序，以确保及时有效地处理所有情况？	▪ 审核信息安全政策和程序	☐	☐	☐	☐	☐
12.5.4	管理用户帐户，包括添加、删除和修改？	▪ 审核信息安全政策和程序	☐	☐	☐	☐	☐
12.5.5	监控并控制所有数据访问？	▪ 审核信息安全政策和程序	☐	☐	☐	☐	☐
12.6	(a) 是否已实施正式的安全意识计划，以使所有工作人员了解持卡人数据安全政策和程序？	▪ 审核安全意识计划	☐	☐	☐	☐	☐
	(b) 安全意识计划程序是否包括以下方面：						
12.6.1	(a) 安全意识计划是否提供了多种传达意识和培训工作人员的方法（例如，海报、信函、备忘录、基于网络的培训、会议和宣传）？ ***注：****根据工作人员的角色及其对持卡人数据的访问级别，可采用不同的方法。*	▪ 审核安全意识计划 ▪ 审核安全意识计划程序 ▪ 审核安全意识计划出席纪录	☐	☐	☐	☐	☐
	(b) 人员是否一经录用即进行培训，且此后每年至少培训一次？	▪ 检查安全意识计划程序和文档	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复（为每个问题选中一个回复）				
			是	是，已填写 CCW	否	N/A	未测试
	(c) 员工是否已完成安全意识培训且已意识到持卡人数据安全的重要性？	▪ 与工作人员面谈	☐	☐	☐	☐	☐
12.6.2	是否要求工作人员每年至少确认一次自己已阅读并了解安全政策和程序？	▪ 检查安全意识计划程序和文档	☐	☐	☐	☐	☐
12.7	是否在录用人员（参见上文的"工作人员"定义）前筛选应征者，以最大程度地降低内部攻击的风险？ *背景调查包括以往的工作经历、犯罪记录、信用记录以及证明人调查。* ***注：**对于可能被录用为门店收银员等特定职位的应征者，本要求仅作为建议，因为他们在交易时一次只能访问一个卡号。*	▪ 与人力资源部管理人员面谈	☐	☐	☐	☐	☐
12.8	是否已按照下述要求实施并维护政策和程序以管理共享持卡人数据或可能影响持卡人数据安全的服务提供商：						
12.8.1	已维护服务提供商列表（包括所提供服务的说明）？	▪ 审核相关政策和程序 ▪ 查看流程 ▪ 审核服务提供商名单	☐	☐	☐	☐	☐
12.8.2	是否维护书面协议，其中确认服务提供商负责其处理或者代表客户以其他方式存储、处理或传输的持卡人数据的安全性以及他们可能会影响客户持卡人数据环境的安全性？ ***注：**"确认"的确切措辞取决于双方协议、所提供服务的详情以及分配给每一方的责任。"确认"不一定要包含与本要求完全相同的措辞。*	▪ 查看书面协议 ▪ 审核相关政策和程序	☐	☐	☐	☐	☐
12.8.3	是否已建立雇用服务提供商的流程（包括雇用前的相应尽职调查）？	▪ 查看流程 ▪ 审核政策、程序和支持文档	☐	☐	☐	☐	☐
12.8.4	是否已维护相应计划来至少每年监控一次服务提供商的 PCI DSS 遵从性状态？	▪ 查看流程 ▪ 审核政策、程序和支持文档	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
12.8.5	是否已维护有关分别由各服务提供商和实体管理的 PCI DSS 要求的信息？	▪ 查看流程 ▪ 审核政策、程序和支持文档	☐	☐	☐	☐	☐
12.9	*此要求仅适用于服务提供商。*						
12.10	是否已按照下述要求实施随时准备立即响应系统漏洞的事故响应计划：						
12.10.1	(a) 是否已建立在出现系统漏洞时实施的事故响应计划？	▪ 审核事故响应计划 ▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
	(b) 该计划是否至少包括以下内容：						
	• 出现威胁时的角色、责任以及沟通和联系策略（至少包括支付品牌通知）？	▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
	• 详细的事故响应程序？	▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
	• 业务恢复和继续程序？	▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
	• 数据备份流程？	▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
	• 报告威胁的法律要求分析？	▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
	• 所有关键系统组件的范围和响应？	▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
	• 支付品牌对事故响应程序的参考或应用？	▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
12.10.2	是否至少每年对计划进行一次审核，包括要求 12.10.1 中列出的所有元素？	▪ 审核事故响应计划程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
12.10.3	是否指定了可全天候响应警报的特定人员？	▪ 查看流程 ▪ 审核政策 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.10.4	是否为具有安全漏洞响应责任的员工提供了恰当的培训？	▪ 查看流程 ▪ 审核事故响应计划程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.10.5	事故响应计划中是否包含来自安全监控系统的警报？	▪ 查看流程 ▪ 审核事故响应计划程序	☐	☐	☐	☐	☐
12.10.6	是否已根据以往的经验教训并结合行业发展情况，制定了修改和改进事故响应计划的流程？	▪ 查看流程 ▪ 审核事故响应计划程序 ▪ 与负责人面谈	☐	☐	☐	☐	☐
12.11	*此要求仅适用于服务提供商*						

附录 A： PCI DSS 附加要求

附录 A1： 针对共享托管服务提供商的 PCI DSS 附加要求

此附录不用于商户评估。

附录 A2： 针对使用 SSL/早期 TLS 的实体的 PCI DSS 附加要求

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是，已填写 CCW	否	N/A	未测试
A2.1	*针对使用 SSL 和/或早期 TLS 的 POS POI 终端（及其连接到的 SSL/TLS 终端点）：* • 是否已证实这些设备不易受到任何已知 SSL/早期 TLS 漏洞的影响 *或者：* • 是否根据要求 A2.2 制定了适当的正式风险降低和迁移计划？	▪ 查看证明 POS PIO 设备不受任何已知 SSL/早期 TLS 使用影响的文档（例如供应商文档、系统/网络设置详情等）	☐	☐	☐	☐	☐
A2.2	是否针对使用 SSL 和/或早期 TLS 的所有实施（A2.1 中允许的实施除外）制定了适当的正式风险降低和迁移计划，包括： ▪ 使用说明，包括传输的数据、使用和/或支持 SSL/早期 TLS 的系统的类型和数量、环境类型； ▪ 风险评估结果和适当的风险降低控制； ▪ 对用于监控 SSL/早期 TLS 相关漏洞的流程的说明； ▪ 对实施以确保 SSL/早期 TLS 未实施到新环境的变更控制流程的说明； ▪ 迁移项目计划概述，包括目标迁移完成时间不迟于 2018 年 6 月 30 日？	▪ 查看记录的风险降低和迁移计划	☐	☐	☐	☐	☐

PCI DSS 问题		预期测试	回复 *（为每个问题选中一个回复）*				
			是	是， 已填写 CCW	否	N/A	未测试
A2.3	*此要求仅适用于服务提供商*						

附录 A3： 指定实体补充认证 (DESV)

此附录仅适用于支付品牌或收单机构要求对现有 PCI DSS 要求进行补充认证时指定的实体。要求验证此附录的实体应使用 DESV 补充报告模板和报告遵从性补充证明书，并咨询适当的支付品牌和/或收单机构了解提交程序事宜。

附录 B： 补偿性控制工作表

使用本工作表为任何选中"是，已填写 CCW"的要求定义补偿性控制。

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

有关补偿性控制和如何填写本工作表的信息，请参见 PCI DSS 的附录 B、C 和 D。

要求编号和定义：

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

附录 C： 不适用性说明

如果在此调查问卷中选中了"N/A"（不适用）列，请使用本工作表说明相关要求为何不适用于您所在组织。

要求	理由要求不适用
示例：	
3.4	持卡人数据从未以电子方式存储

附录 D： 未测试的要求说明

如果在此调查问卷中选中了"未测试"列，请使用本工作表说明为何未在评估过程中审核相关要求。

要求	说明相关要求的哪个部分未进行测试	说明为何未测试要求
示例：		
要求 12	*仅测试了要求 12.2。要求 12 中的其他所有要求均被排除。*	*本次评估仅涵盖优先方法的里程碑 1 中的要求。*
要求 1-8、10-12	*本次评估仅审核了要求 9。其他所有要求均被排除。*	*相关公司为物理托管服务供应商 (CO-LO)，因此本次评估仅考虑物理安全控制方面。*

第 3 节： 认证和证明书详情

第 3 部分 PCI DSS 认证

此 AOC 基于*（SAQ 填写日期）填写的 SAQ D（第 2 节）中的结果。*

基于上述 SAQ D 中记录的结果，第 3b-3d 部分中指明的签署者（如果适用）针对本文档第 2 部分中指明的实体声明以下遵从性状态 （***选中一个选项）：***

☐	**遵从：**已填写 PCI DSS SAQ 的所有章节且已针对所有问题提供积极回复，从而获得了总体**遵从**评分；因此*（商户公司名称）*已证明其完全遵从 PCI DSS。
☐	**未遵从：**未填写 PCI DSS SAQ 的部分章节或未针对所有问题提供积极回复，从而获得了总体**未遵从**评分，因此*（商户公司名称）*未证明其完全遵从 PCI DSS。 **遵从目标日期：** 如果某实体提交的本表单具有未遵从状态，则可能需要填写本文档第 4 部分中的行动计划。*在填写第 4 部分之前，请先咨询您的收单机构或支付品牌。*
☐	**遵从但包含法律规定的例外情况：**由于受到阻止满足相关要求的法律限制，因此一项或多项要求选为了“否”。此选项要求收单机构或支付品牌进行附加审核。 *如果选中此选项，请填写以下内容：*

相关要求	有关法律限制如何阻止满足相关要求的详情

第 3a 部分 确认状态

签署者确认：

（选中所有合适选项）

☐	已根据本文中的说明填写第 *（SAQ 版本）*版 PCI DSS 自我评估调查问卷 D。
☐	上述引用的 SAQ 和本证明书中的所有信息在一切重要方面均完全代表本次评估的结果。
☐	已向相应的支付应用程序供应商确认自己的支付系统未在验证后存储敏感验证数据。
☐	已阅读 PCI DSS 且了解必须始终遵从适用于所在环境的 PCI DSS。
☐	了解如果所在环境发生变化则必须重新评估所在环境，并实施任何适用的 PCI DSS 附加要求。

第 3a 部分 确认状态（续）	
☐	未在本次评估所审核的 ANY 系统中发现交易授权后仍存储完整磁道数据[1]、CAV2、CVC2、CID、CVV2 数据[2]或 PIN 数据[3]的迹象。
☐	ASV 扫描正由 PCI SSC 认证的授权扫描服务商（*ASV 名称*）完成

第 3b 部分 商户证明书	
商户执行官签名 ↑	*日期:*
商户执行官姓名:	*职务:*

第 3c 部分 合格安全性评估商 (QSA) 确认（如适用）	
如果 QSA 参与了或帮助完成本次评估，请说明其执行的角色：	

QSA 公司正式授权管理人员签名↑	*日期:*
正式授权管理人员姓名:	*QSA 公司:*

第 3d 部分 内部安全性评估商 (ISA) 参与（如适用）	
如果 ISA 参与了或帮助完成本次评估，请确认该 ISA 工作人员，并说明其执行的角色：	

[1] 实卡交易中用于授权的磁条编译数据或芯片上的类似数据。实体不得在交易授权后保留完整磁道数据。唯一可保留的磁道数据部分为主帐户 (PAN)、失效日期和持卡人姓名。

[2] 用于验证非实卡交易而印于支付卡签名条或正面的三位或四位数值。

[3] 持卡人在实卡交易中输入的个人识别码，和/或交易消息中包含的加密 PIN 数据块。

第 4 部分 针对未遵从要求的行动计划

针对每项要求的“PCI DSS 要求遵从性”选择合适的回复。如果您针对任一要求回复了“否”，则需要提供您所在公司预计遵从该要求的日期，并简要说明为满足该要求所采取的行动。

在填写第 4 部分之前，请先咨询您的收单机构或支付品牌。

PCI DSS 要求	要求说明	遵从 PCI DSS 要求（选择一个选项）		补救日期和行动（如果针对任一要求选择了“否”）
		是	否	
1	安装并维护防火墙配置以保护持卡人数据	☐	☐	
2	不要使用供应商提供的默认系统密码和其他安全参数	☐	☐	
3	保护存储的持卡人数据	☐	☐	
4	加密持卡人数据在开放式公共网络中的传输	☐	☐	
5	为所有系统提供恶意软件防护并定期更新杀毒软件或程序	☐	☐	
6	开发并维护安全的系统和应用程序	☐	☐	
7	按业务知情需要限制对持卡人数据的访问	☐	☐	
8	识别并验证对系统组件的访问	☐	☐	
9	限制对持卡人数据的物理访问	☐	☐	
10	跟踪并监控对网络资源和持卡人数据的所有访问	☐	☐	
11	定期测试安全系统和流程	☐	☐	
12	维护针对所有工作人员的信息安全政策	☐	☐	
附录 A2	针对使用 SSL/早期 TLS 的实体的 PCI DSS 附加要求	☐	☐	