支付卡行业 (PCI)

数据安全标准

自我评估调查问卷 P2PE

和遵从性证明书

仅限使用 PCI SSC 列出的 P2PE 解决方案中的支付终端硬件的商户 – 无电子持卡人数据存储

适用于 PCI DSS 3.2 版

2016 年 4 月

文档变更记录

日期	PCI DSS 版本	SAQ 修订版	描述
N/A	1.0		未使用。
2012 年 5 月	2.0		针对仅使用 PCI SSC 清单上经认证的 P2PE 解决方案中的终端硬件的商户制定 SAQ P2PE-HW。 本 SAQ 与 PCI DSS 2.0 版搭配使用。
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"*。 从 SAQ 标题中移除了"HW"，因为使用 HW/HW 或 HW/混合 P2PE 解决方案的商户可能会使用。
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"。
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"*。

目录

开始之前

SAQ P2PE 的商户适用条件

SAQ P2PE 用于解决适用于仅通过 PCI 清单上列出的经认证点对点加密 (P2PE) 解决方案中的支付终端硬件处理持卡人数据的商户的要求。

SAQ P2PE 商户无法通过任何计算机系统访问持卡人数据明文，且仅能通过 PCI SSC 认证 P2PE 解决方案中的支付终端硬件访问帐户数据。SAQ P2PE 商户可以是实体（实卡交易）商户，也可以是邮件/电话订购（非实卡交易）商户。例如，如果一家邮件/电话订购商户通过纸质媒介或电话接收持卡人数据，且仅将其直接嵌入经认证的 P2PE 硬件设备，则该商户符合 SAQ P2PE 的适用条件。

SAQ P2PE 商户确认，对于此支付渠道：

- 所有支付处理均通过经 PCI SSC 批准和列出的经认证 PCI P2PE 解决方案完成；
- 商户环境中用于存储、处理或传输帐户数据的系统均为获批与 PCI 清单认证 P2PE 解决方案搭配使用的交互点 (POI) 设备；
- 您的公司未以其他形式的电子方式接收或传输持卡人数据。
- 未在该环境中保留存储的电子持卡人数据；
- 如果您所在公司存储持卡人数据，则此类数据仅包含在纸质报告或纸质收据副本中且未以电子方式接收，**以及**
- 您所在公司已实施相应 P2PE 解决方案提供商提供的 *P2PE 说明手册 (PIM)* 中的所有控制。

此 SAQ 不适用于电子商务渠道。

本简要版 SAQ 包含适用于符合上述适用条件的特定类型小型商户环境的问题。如果某些适用于您所在环境的 PCI DSS 要求未包含在本 SAQ 中，可能表示本 SAQ 不适用于您所在环境。

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. 确认您所在环境的范围适当且满足您所使用的 SAQ 的适用条件（参见遵从性证明书的第 2g 部分）。
3. 确认您已实施该 PIM 的所有元素。
4. 评估您所在环境是否遵从相应的 PCI DSS 要求。
5. 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 P2PE)
   - 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）
6. 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。

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阅读 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。

某些特定要求的不适用性指南

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”。

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 (PCI DSS) 要求和安全评估程序*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 ☐ 邮件/电话订购 ☐ 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） 和所在地点概要。

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 P2PE 解决方案

提供有关您所在组织使用的经认证 PCI P2PE 解决方案的下列信息：

P2PE 解决方案提供商名称：	
P2PE 解决方案名称：	
PCI SSC 引用号	
列出的商户使用的 P2PE POI 设备（PTS 设备依赖条件）：	

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、航班订票代理商、忠诚计划代理商等）共享持卡人数据？ ***如果是的话：***	☐ 是 ☐ 否

服务提供商名称：	**所提供服务的说明：**

注：*要求 12.8 适用于此问题的回复中所列出的所有实体。*

第 2g 部分 填写 SAQ P2PE 的适用条件

商户证明符合填写本简要版自我评估调查问卷的适用条件，因为对于此支付渠道：

☐	所有支付处理均通过 PCI SSC（参见上文）批准和列出的经认证 PCI P2PE 解决方案完成。
☐	商户环境中用于存储、处理或传输帐户数据的系统均为获批与 PCI 清单认证 P2PE 解决方案搭配使用的交互点 (POI) 设备。
☐	商户未以其他形式的电子方式接收或传输持卡人数据。
☐	商户确认未在该环境中保留存储的电子持卡人数据。
☐	如果商户存储持卡人数据，则此类数据仅包含在纸质报告或纸质收据副本中且未以电子方式接收，**以及**
☐	商户已实施 P2PE 解决方案提供商提供的 P2PE 说明手册 (PIM) 中的所有控制。

第 2 节：自我评估调查问卷 P2PE

***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实际 PCI DSS 要求和测试程序顺序相符。由于本 SAQ P2PE 中仅包含部分 PCI DSS 要求，因此这些问题的编号可能不是连续的。*

自我评估实施日期：

保护持卡人数据

要求 3：保护存储的持卡人数据

***注：**要求 3 仅适用于拥有纸质记录（例如，收据、打印报告等）的 SAQ P2PE 商户 的 SAQ P2PE-HW 商户。*

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
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	☐	☐	☐	☐

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
	(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	☐	☐	☐	☐
指南： *针对要求 3.1 选择"是"表示，如果某商户存储了任何包含帐户数据的纸质媒介（例如收据或纸质报告），则该商户仅出于业务需求、法律和/或法规要求原因存储该纸质媒介并在不再需要时立即将其销毁。* *如果某商户从未打印或存储任何包含帐户数据的纸质媒介，则该商户应选中"N/A"列并在附录 C 中填写"不适用性说明"工作表。*						
3.2.2	对于所有纸质存储，是否未在授权后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）？	▪ 检查纸质数据来源	☐	☐	☐	☐
指南： *针对要求 3.2.2 选择"是"表示，如果某商户在执行交易时记录了卡安全代码，则该商户在交易完成后立即销毁（例如利用碎纸机）了该纸质媒介，或者已在存储该纸质媒介前将该代码遮盖住（例如用标记涂上）。* *如果该商户从未请求获得印在支付卡正面或背面的三位或四位数字（"卡安全代码"），则该商户应选中"N/A"列并在附录 C 中填写"不适用性说明"工作表。*						
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	☐	☐	☐	☐
指南： *针对要求 3.7 选择"是"表示，如果该商户通过纸质媒介存储了帐户数据，则已针对要求 3.1、3.2.2 和 3.3 制定相关政策和程序。这可帮助确保工作人员了解并遵守用于持续管理持卡人数据安全存储的安全政策和书面操作程序。*						

实施强效访问控制措施

要求 9：限制对持卡人数据的物理访问

注：*要求 9.5 和 9.8 仅适用于拥有纸质记录（例如，收据、打印报告等）的 SAQ P2PE 商户 的 SAQ P2PE-HW 商户。*

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
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	☐	☐	☐	☐
9.8	(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	☐	☐	☐	☐
	(c) 是否按照下述要求销毁媒介：					
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？	▪ 审核媒介定期销毁政策和程序 ▪ 与工作人员面谈 ▪ 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？	▪ 审核媒介定期销毁政策和程序 ▪ 检查存储容器的安全性	☐	☐	☐	☐
指南：*针对要求 9.5 和 9.8 选择“是”表示，该商户已安全存储任何包含帐户数据的纸质媒介（例如，通过将其存储在上锁的抽屉、橱柜或保险箱中），且在不再因业务原因需要时销毁了此类纸质媒介。这包括制定了针对员工的书面文档或政策，以便他们了解如何保护包含帐户数据的纸质媒介和在不再需要时销毁此类纸质媒介。* *如果该商户从未存储任何包含帐户数据的纸质媒介，则应选中“N/A”列并在附录 C 中填写“不适用性说明”工作表。*						
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。*					

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
	(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	☐	☐	☐	☐
	(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	☐	☐	☐	☐

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
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	☐	☐	☐	☐
指南：*针对要求 9.9 选择“是”表示，该商户已针对要求 9.9.1 – 9.9.3 制定了相关政策和程序，且已维护当前设备列表、定期进行设备检测并为员工提供了有关检测遭篡改或替换设备时的查找对象的培训。*						
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	☐	☐	☐	☐
指南：*针对要求 9.10 选择“是”表示，该商户已针对要求 9.5、9.8 和 9.9 制定了适用于您所在环境的政策和程序。这可帮助确保工作人员了解并遵从安全政策和操作程序文档记录。*						

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：要求 12 规定，商户必须制定针对其工作人员的信息安全政策，该政策的篇幅可因其业务规模和复杂性而异。该政策文档必须提供给所有工作人员，以便其了解自己对于支付终端和任何包含持卡人数据的纸质文档等的保护责任。如果某商户未雇佣任何员工，则该商户应了解并确认其对于自身商店内信息安全的责任。

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
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	☐	☐	☐	☐
指南：*针对要求 12.1 选择"是"表示，该商户已根据其业务规模和复杂性制定了合理的安全政策，且该政策每年审核一次并在需要时进行更新。例如，此类政策可以是一篇简单的文档，其中指明如何按照 P2PE 说明手册 (PIM) 保护商店和支付设备，以及紧急情况下的联系人。*						
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	☐	☐	☐	☐
指南：*针对要求 12.4.1 选择"是"表示，该商户的安全政策根据其业务规模和复杂性规定了所有工作人员的基本安全责任。例如，可以按照员工级别的基本职责规定安全责任，例如经理/负责人的责任和文员的责任。*						
12.5	是否已将下列信息安全管理职责正式分配给个人或团队：					
12.5.3	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	☐	☐	☐	☐
指南：*针对要求 12.5.3 选择"是"表示，该商户已指派专门人员负责要求 12.9 中规定的事故响应和逐级上报计划。*						
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	☐	☐	☐	☐
指南：*针对要求 12.6 选择"是"表示，该商户已根据其业务规模和复杂性制定了安全意识计划。例如，一份简单的安全意识计划可以作为传单贴在后勤办公室，也可以定期通过电子邮件发送给所有员工。安全意识计划通讯包括说明所有员工均应掌握的安全技能，例如如何为门和存储容器上锁、如何确定支付终端是否遭到篡改，以及如何识别可正当访问支付终端硬件的人员。*						

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
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	☐	☐	☐	☐
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	☐	☐	☐	☐
指南：*针对要求 12.8 选择“是”表示，该商户拥有共享持卡人数据的服务提供商清单，并与这些服务提供商达成了相应协议。例如，如果商户通过文档保留公司存储包含帐户数据的纸质文档，则此类协议适用。*						
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	☐	☐	☐	☐
指南：*针对要求 12.10 选择“是”表示，该商户已根据其业务规模和复杂性通过文档记录了用于紧急情况的事故响应和逐级上报计划。例如，此类计划可以是贴在后勤办公室的简单文档（其中列出不同情况下的联系人且需每年审核一次以确认仍然有效）；也可以扩展为指明备用“热站”设施且经过年度全面测试的完整事故响应计划。该计划应可作为紧急情况资源提供给所有工作人员。*						

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

此附录不用于 SAQ P2PE 商户评估

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：	
12.8	从未与服务提供商共享持卡人数据。

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 P2PE（第 2 节）中的结果。*

基于上述 SAQ P2PE 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 P2PE 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 P2PE 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，因为并非所有支付品牌都要求填写此部分。*
☐	**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）

☐	第*（SAQ 版本）*版 PCI DSS 自我评估调查问卷 P2PE 已根据本文中的说明填写完成。
☐	上述引用的 SAQ 和本证明书中的所有信息均完全代表本次评估的结果。
☐	已阅读 PCI DSS 且了解必须始终遵从适用于所在环境的 PCI DSS。

第 3a 部分 确认状态（续）

☐	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。
☐	未在本次评估所审核的 ANY 系统中发现任何完整磁道数据[1]、CAV2、CVC2、CID、CVV2 数据[2]或 PIN 数据[3]。

[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。交易授权之后，实体不得保留完整的磁条数据。可以被保留下来的磁道数据元素只能包括账号、失效期与姓名。

[2] 用于验证非实卡交易而印于支付卡签名条上或右侧或者支付卡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 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：	

第 4 部分 针对未遵从状态的行动计划

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，因为并非所有支付品牌都要求填写此部分。

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	
3	保护存储的持卡人数据	☐	☐	
9	限制对持卡人数据的物理访问	☐	☐	
12	维护针对所有工作人员的信息安全政策	☐	☐	

** 此处提及的 PCI DSS 要求是指本 SAQ 第 2 节中的问题。*