PCI DSS v4.0 变更系列之十

——新要求点统计

PCI DSS v4.0 新要求点		适用于		生效日期	
		所有实体	仅限服务供应商	立即生效	2025 年 3 月 31 日
2.1.2	记录、分配和理解执行要求2中各项活动的角色和责任。	是		是	
3.1.2	记录、分配和理解执行要求3中各项活动的角色和责任。	是		是	
3.2.1	通过实施数据保留和处理政策、程序和过程，将授权完成前存储的任何SAD保持在最低限度。	是			是
3.3.2	在完成授权之前，使用强效加密法来加密以电子方式存储的SAD。	是			是
3.3.3	使用强效加密法来加密发行机构存储的 SAD。		是		是
3.4.2	在使用远程访问技术时，除非有明确授权，否则应采取技术控制来防止复制和/或重新定位 PAN。	是			是
3.5.1.1	用于使PAN不可读的散列（根据要求3.5.1 的第一个项目符号）是整个PAN的密钥加密散列以及相关的密钥管理过程和程序。	是			是
3.5.1.2	当用于使 PAN 不可读时，实施磁盘级或分区级加密。	是			是
3.6.1.1	加密结构的记录描述包括防止在生产和测试环境中使用加密密钥。		是		是
4.1.2	记录、分配和理解执行要求 4 中各项活动的角色和责任。	是		是	
4.2.1	确认用于在开放的公共网络上传输过程中保护 PAN 的证书有效且没有过期或撤销。	是			是
4.2.1.1	维护实体的可信密钥和证书的清单。	是			是
5.1.2	记录、分配并理解执行要求5中各项活动的角色和责任。	是		是	
5.2.3.1	执行目标风险分析，以确定被视为无恶意软件风险的系统组件定期评估的频率。	是			是
5.3.2.1	执行目标风险分析，以确定定期恶意软件扫描的频率。	是			是
5.3.3	在使用可移动电子媒体时，执行反恶意软件扫描。	是			是
5.4.1	建立机制，检测并保护人员免受网络钓鱼攻击。	是			是
6.1.2	记录、分配并理解执行要求 6 中各项活动的角色和责任。	是		是	
6.3.2	维护定义或定制软件的清单，以促进漏洞和补丁管理。	是			是

PCI DSS v4.0 新要求点		适用于		生效日期	
		所有实体	仅限服务供应商	立即生效	2025 年 3 月 31 日
6.4.2	为面向公众的网络应用程序部署自动技术解决方案，以持续检测和防止基于网络的攻击。	是			是
6.4.3	管理加载于消费者浏览器并在其上执行的所有支付页面脚本。	是			是
7.1.2	记录、分配并理解执行要求 7 中各项活动的角色和责任。	是		是	
7.2.4	适当地审核所有用户账户和相关访问权限。	是			是
7.2.5	适当地分配和管理所有应用程序和系统账户以及相关访问权限。	是			是
7.2.5.1	审核所有应用程序和系统账户的权限以及相关访问权限。	是			是
8.1.2	记录、分配和理解执行要求8中各项活动的角色和责任。	是		是	
8.3.6	当作为验证因素使用时，密码的最低复杂程度。	是			是
8.3.10.1	如果密码/口令是客户用户访问的唯一验证因素，则至少每 90 天更换一次密码/口令，或者动态分析账户安全状况，以确定对资源的实时访问。		是		是
8.4.2	所有 CDE 访问的多因素验证。	是			是
8.5.1	适当实施多因素验证系统。	是			是
8.6.1	管理系统或应用程序所使用的账户的交互式登录。	是			是
8.6.2	保护用于应用程序和系统账户交互式登录的密码/口令免于滥用。	是			是
8.6.3	保护任何应用程序和系统账户的密码/口令免于滥用。	是			是
9.1.2	记录、分配和理解执行要求 9 中各项活动的角色和责任。	是		是	
9.5.1.2.1	执行目标风险分析，以确定定期POI设备检查的频率。	是			是
10.1.2	记录、分配和理解执行要求 10 中各项活动的角色和责任。	是		是	
10.4.1.1	自动化检查日志审核。	是			是
10.4.2.1	执行目标风险分析，以确定针对所有其他系统组件的日志审核频率。	是			是
10.7.2	及时检测、提醒、处理关键安全控制系统的故障。	是			是
10.7.3	及时响应关键安全控制系统的故障。	是			是

PCI DSS v4.0 新要求点		适用于		生效日期	
		所有实体	仅限服务供应商	立即生效	2025 年 3 月 31 日
11.1.2	记录、分配和理解执行要求 11 中各项活动的角色和责任。	是		是	
11.3.1.1	处理所有其他适用的漏洞（未被列为高风险或关键的漏洞）。	是			是
11.3.1.2	通过验证扫描来执行内部漏洞扫描。	是			是
11.4.7	多租户服务提供商支持其客户执行外部渗透测试。		是		是
11.5.1.1	通过入侵检测和/或入侵防御技术，检测、提醒和/或预防并解决秘密的恶意软件通信渠道。		是		是
11.6.1	将变更和篡改检测机制部署于支付页面。	是			是
12.3.1	记录目标风险分析，以支持每个 PCI DSS 要求，为其执行频率提供灵活性。	是			是
12.3.2	对每个PCI DSS要求执行有目标风险分析，通过定制方法满足这些要求。	是		是	
12.3.3	记录和审核正在使用的加密密码套件和协议。	是			是
12.3.4	审核硬件和软件技术。	是			是
12.5.2	PCI DSS范围至少每12个月记录和确认一次。	是		是	
12.5.2.1	PCI DSS 范围至少每六个月并在发生重大变更时记录和确认一次。		是		是
12.5.3	记录和审核重大组织变更对 PCI DSS 范围的影响，并将结果传达给执行管理层。		是		是
12.6.2	至少每12个月审核一次安全意识计划，并视需要进行更新。	是			是
12.6.3.1	安全意识培训包括对可能影响 CDE 安全的威胁的认识，以包括网络钓鱼和相关攻击以及社会工程。	是			是
12.6.3.2	安全意识培训包括对最终用户技术的可接受使用的认识。	是			是
12.9.2	第三方服务供应商（TPSP）应支持客户的要求，提供PCI DSS遵从性状态以及由TPSP负责的PCI DSS要求的相关信息。		是	是	
12.10.4.1	执行目标风险分析，以确定事件响应人员的定期培训频率。	是			是
12.10.5	安全事件响应计划包括支付页面变更和篡改检测机制的警报。	是			是
12.10.7	建立事件响应程序，并在发现 PAN 时启动。	是			是
A1.1.1	多租户服务提供商确认是否逻辑隔离了进出客户环境的权限，以防止未经授权的访问。		是		是
A1.1.4	多租户服务提供商每六个月通过渗透测试确认用于分离客户环境的逻辑分离控制的有效性。		是		是

PCI DSS v4.0 新要求点		适用于		生效日期	
		所有实体	仅限服务供应商	立即生效	2025 年 3 月 31 日
A1.2.3	多租户服务提供商实施流程或机制，报告和处理可疑或确认的安全事件和漏洞。		是		是
A3.3.1	及时检测、提醒和报告以下故障： 自动日志审核机制。 自动代码审核工具。	是			是
总数	64	53	11	13	51

表 1：PCI DSS V4.0 新要求点总结表

对于新要求的时间点要求，再次提醒如下：

1、在 2022 年开始，所有合规机构均可以按照 PCI DSS v4.0 的要求进行合规认证。

2、如果按 v4.0 的要求进行合规认证，所有对应于“立即生效”的要求点必须达到要求。

3、理论上讲，所有标记为“2025 年 3 月 31 日”的要求点（共 51 个）在 2025 年 3 月 31 日前可以按不适用处理。但仍然建议合规机构尽早研究和分析这些要求点，落实所对应的控制措施。