《支付卡行业（PCI）
数据安全标准》

PCI DSS 3.1 版到 3.2 版的变更汇总

2016 年 4 月

简介

本文档为 PCI DSS 3.1 版到 PCI DSS 3.2 版的变更汇总。表 1 是对变更类型的概要。表 2 是对 PCI DSS 3.2 版中重大变更的汇总。

表 1：变更类型

[1]变更类型	定义
说明性	说明要求的目的。确保该《标准》中简洁的措辞传达出要求的预期目的。
其他指南	解释、定义和/或说明，用以加深理解，或就某一特定主题提供更多信息或指南。
不断进化的要求	相关变更用以确保该《标准》与市场中出现的新威胁和各种变化保持同步。

表 2：变更汇总

章节		变更描述	类型 [1]
PCI DSS 3.1 版	PCI DSS 3.2 版		
全部	全部	解决了细微印刷错误（语法、标点、格式等），并兼并了小版本更新以提升文件的易读性。	说明性
PCI DSS 与 PA-DSS 的关系	PCI DSS 与 PA-DSS 的关系	添加了指南，即安全威胁正在不断演变，而且不受供应商支持的支付应用程序可能不具有和受支持版本一样的安全级别。	其他指南
PCI DSS 要求的范围	PCI DSS 要求的范围	阐明需在确认 PCI DSS 范围时考虑备份/恢复站点。	说明性
在常规业务流程中实施 PCI DSS 的最优方法	在常规业务流程中实施 PCI DSS 的最优方法	更新了注释，以阐明一些常规业务原则对某些实体（例如，指定实体补充认证（附录 A3）中定义的实体）而言可能会变成要求。	说明性
	PCI DSS 版本	新增章节，说明了此 PCI DSS 版本如何影响之前的有效版本。	其他指南
要求			
综述	综述	删除了许多要求中的“强大”或“安全”协议示例，因为这些内容可能会随时发生变更。	说明性
综述	综述	将示例从许多要求和/或测试程序移至指南栏，并在适当情况下添加了指南。	说明性
综述	综述	将“密码/短语”更改为“密码/口令”，以保证前后一致性。	说明性
综述	综述	阐明正确术语为“多因素验证”，而非双因素验证，因为可能会用到两个或两个以上因素。	说明性
综述	综述	删除了提及生效日为 2015 年 7 月 1 日的要求注释，因为这些要求现已生效。受影响的要求为要求 6.5.10、8.5.1、9.9、11.3 和 12.9。	说明性
1.1.6	1.1.6	阐明本理由中包含业务用途审批。 删除了“非安全”协议示例，因为这些示例可能会随行业标准变更。	说明性
1.2.1	1.2.1	添加了指南，以阐明要求的目的。	说明性
1.3	1.3	添加了指南，以阐明要求的目的。	说明性
1.3.3		删除了要求，因为已通过 1.2 和 1.3 部分中的其他要求达到了目的。	说明性
1.3.4 – 1.3.8	1.3.3 – 1.3.7	因删除了原先的要求 1.3.3 而进行了重新编号。	说明性

章节		变更描述	类型 [1]
PCI DSS 3.1 版	PCI DSS 3.2 版		
1.3.6	1.3.5	进行了更新，以阐明要求的目的，而非特定技术类型的用途。	说明性
1.4	1.4	通过用包括的*或等效功能*替代个人防火墙软件提高了灵活度。 阐明此要求适用于可在此网络外连接到互联网并且还可以访问 CDE 的所有便携式计算设备。	说明性
2.1	2.1	阐明此要求适用于支付应用程序。	说明性
2.2.3	2.2.3	删除了有关删除 SSL/早期 TLS 并将其移至新附录 A2 的注释和测试程序。	说明性
2.3	2.3	删除了有关删除 SSL/早期 TLS 并将其移至新附录 A2 的注释和测试程序。 将参考移至“基于 Web 的管理”，因为此要求已指定“所有非控制台管理访问”，根据定义，这包括任何基于 Web 的访问。	说明性
3.3	3.3	更新了要求，以阐明仅有正当业务需要者才能看到除前六位/后四位以外的 PAN。添加了常见掩盖情况相关指南。	不断进化的要求
3.4.d	3.4.d	更新了测试程序，以阐明检查日志检查包括支付应用程序日志。	说明性
3.4.1	3.4.1	为此要求添加了注释，以阐明除所有其他 PCI DSS 加密和密钥管理要求外，此要求也适用。	说明性
	3.5.1	新增要求，针对维护加密架构文档描述的服务提供商。 *2018 年 2 月 1 日生效*	不断进化的要求
3.5.1 – 3.5.3	3.5.2 – 3.5.4	因新增了要求 3.5.1 而进行了重新编号。	说明性
3.6.1.b	3.6.1.b	更新了测试程序语言，以阐明测试涉及程序查看，而非密钥生成方法本身，因为密钥生成方法不可查看。添加了“密钥生成”词汇定义的相关指南	说明性
4.1	4.1	删除了有关删除 SSL/早期 TLS 并将其移至新附录 A2 的注释和测试程序。	说明性
6.2	6.2	添加了对指南栏的说明，即修补所有软件的要求包括支付应用程序。	说明性
6.4.4	6.4.4	更新了要求以符合测试程序。	说明性
6.4.5	6.4.5	阐明变更控制流程不限于补丁和软件修改。	说明性

章节		变更描述	类型 [1]
PCI DSS 3.1 版	PCI DSS 3.2 版		
	6.4.6	新增要求，针对将包括受变更影响的 PCI DSS 要求验证的变更控制流程。 *2018 年 2 月 1 日生效*	不断进化的要求
6.5	6.5	阐明开发人员培训须及时更新，并至少每年开展一次。	说明性
6.5.a – 6.5.d	6.5.a – 6.5.c	删除了测试程序 6.5.b，并对剩余的测试程序进行重新编号以适应此变更。	说明性
7.2	7.2	更新了要求、测试程序和指南栏，以阐明可使用一个或多个访问控制系统。	说明性
要求 8	要求 8	为要求 8 简介添加了注释，即验证要求不适用于消费者（例如持卡人）使用的帐户。	说明性
8.1.5	8.1.5	阐明适用于所有可进行远程访问的第三方而非供应商的要求。	说明性
8.2.3	8.2.3	更新了指南栏，以体现不断改变的行业标准。	说明性
8.3	8.3	阐明正确术语为“多因素验证”，而非双因素验证，因为可以使用两个或两个以上因素。	说明性
8.3	8.3, 8.3.1, 8.3.2	将要求 8.3 扩展到子要求，以要求可进行非控制台管理访问的所有工作人员，以及可对 CDE 进行远程访问的所有工作人员使用多因素验证。 新要求 8.3.2 针对适用于可对 CDE 进行远程访问的所有工作人员的多因素验证（包含原先的要求 8.3）。 新要求 8.3.1 针对适用于可对 CDE 进行非控制台管理访问的所有工作人员的多因素验证。 *要求 8.3.1 将于 2018 年 2 月 1 日生效*	不断进化的要求
9.1.1	9.1.1	阐明可使用摄像头和/或访问控制机制。	说明性
9.5.1.a – 9.5.1.b	9.5.1	合并了测试程序，以阐明评估商确认至少每年审查一次存储位置。	说明性
	10.8, 10.8.1	新增要求，针对检测和报告关键安全控制系统故障的服务提供商。 *2018 年 2 月 1 日生效*	不断进化的要求
10.8	10.9	因新增了要求 10.8 而进行了重新编号。	说明性
11.2.1	11.2.1	阐明所有“高风险”漏洞均须根据实体的漏洞评级（见要求 6.1 中的定义）得到处理，并通过重新扫描予以确认。	说明性

章节		变更描述	类型 [1]
PCI DSS 3.1 版	PCI DSS 3.2 版		
11.3.4	11.3.4	添加了测试程序 11.3.4.c，以确认已由合格内部资源或合格外部第三方进行了穿透测试。	说明性
	11.3.4.1	新增要求，针对至少每半年对分段控制进行一次穿透测试的服务提供商。 *2018 年 2 月 1 日生效*	不断进化的要求
11.5.a	11.5.a	删除了测试程序中的“在持卡人数据环境中”以与此要求保持一致，因为此要求可能适用于位于指定 CDE 外的关键系统。	说明性
12.3.3	12.3.3	为叙述清楚，重新编排了测试程序的格式。	说明性
	12.4	新增要求，针对确立持卡人数据和 PCI DSS 遵从性计划保护责任的服务提供商行政管理人员。 *2018 年 2 月 1 日生效*	不断进化的要求
12.4	12.4.1	因新增了要求 12.4 而进行了重新编号。	说明性
12.6	12.6	阐明安全意识计划的目的在于确保工作人员了解持卡人数据安全政策和程序。	说明性
12.8.1	12.8.1	阐明服务提供商列表包含所提供服务的说明。	说明性
12.8.2	12.8.2	添加了指南，说明服务提供商的职责将取决于提供的特定服务，以及双方之间达成的协议。	其他指南
12.10.2	12.10.2	阐明事故响应计划审查包含要求 12.10.1 中列出的所有要素。	说明性
	12.11, 12.11.1	新增要求，针对至少每季度进行一次审查以确认工作人员遵守安全政策和操作程序的服务提供商。 *2018 年 2 月 1 日生效*	不断进化的要求
附录 A	附录 A1	由于包含了新附录，因此对附录“*针对共享托管服务提供商的 PCI DSS 附加要求*”进行了重新编号。	说明性
	附录 A2	带有附加要求的新附录，针对使用 SSL/早期 TLS 的实体，其内容包含删除 SSL/早期 TLS 的最新最后迁移期限。	说明性
	附录 A3	将包含“指定实体补充认证”(DESV) 的新附录，该附录之前是一个独立文档。	说明性