PCI DSS v4.0 变更系列之二

——主体章节的变更情况说明

PCI DSS v4.0 标准在主体章节的变更情况说明

笔者基于“PCI DSS v4.0”和“PCI DSS V3.2.1”文档，对标准文档的主体部分（第 2 章至第 14 章节）的变更内容进行了梳理。

主体章节的结构基本与 v3.2.1 保持一致，v4.0 在每个章节的具体内容中做了更进一步的澄清。详细的说明如下：

第二章：进一步澄清了 PCI DSS 的适用对象

第二章 PCI DSS 适用性，澄清 PCI DSS 适用于对持卡人数据/敏感认证数据进行存储、处理与传输的机构。

对于不进行持卡人数据/敏感认证数据的存储、处理与传输的机构（比如将持卡人数据的处理与操作外包给第三方的机构），澄清这些机构仍需要确保持卡人数据按要求得到了保护。

为了增加易读性，在该部分列举了多种不存储/处理与传输持卡人数据，但适用于 PCI DSS 合规的情形。说明如下：

- 对于存储敏感认证数据（SAD）的机构， 涉及要求 3 里关于 SAD 存储的要求将适用。
- 如果机构引入第三方供应商，由第三方供应商进行持卡人数据的存储、处理与传输，涉及要求 12 的服务供应商管理的要求仍适用于该机构。
- 因为机构的基础设施的安全性能影响持卡人数据如何处理，比如通过 web 服务器控制支付表单或页面的生成，该机构将可能影响持卡人数据环境（CDE）的安全性，相关要求将适用于该机构。
- 如果持卡人数据仅存在于物理介质（比如纸张），要求 9 关于物理介质安全及销毁的要求将适用。
- 涉及事件响应计划的要求适用于所有机构，以确保在出现威胁持卡人数据机密性的可疑或实际行为时能进行响应。

第三章：澄清与 PCI SSF 的关系

第三章 PCI DSS 与 PCI SSF 软件标准的关系，更新 PA-DSS 在 2022 年 10 月到期的情况，并进一步澄清安全软件标准和安全软件生命周期（Secure SLC）标准的适用性。通过了 PCI SSF 将有助于相应的软件或软件生命周期的流程符合并通过 PCI DSS 的评估，但采用通过 SSF 的软件部署后的环境仍需要进行独立的 PCI DSS 验证。对于完全采用标委会网站上列出的软件的情形，需要 PCI QSA 进行环境中实际部署的软件与标委会网站上列出的软件的比对，并通过实施指导文档与实际部署情况的比对确认软件进行了安全的部署。对于参照 PCI SSF 或安全生命周期标准进行开发与维护的定制化软件，对 SSF 的参考同样会对通过 PCI DSS 要求 6 提供支持。

在该章节，也进一步澄清软件开发供应商在涉及持卡人数据的存储、处理与传输的情况下（比如远程访问到客户的持卡人数据环境），仍涉及到 PCI DSS 的合规。这些适用于 PCI DSS 供应商的范围可能包括：

- 提供支付服务的供应商。

- 在云环境中提供了支付终端的云服务供应商。
- SaaS 供应商。
- 提供电子商务支付功能的云供应商。

第四章：进一步澄清 PCI DSS 要求的适用范围

第四章 PCI DSS 要求的范围，进一步澄清了 PCI DSS 要求的适用范围，包括持卡人数据环境及影响持卡人数据环境的人员、组件及流程。对于持卡人数据环境，应包括存储/处理/传输持卡人数据/敏感认证数据的人员、流程及组件，也包括其它不受限制连接到存储/处理/传输持卡人数据/敏感认证数据的组件。通过澄清，使得在 PCI DSS 范围的界定上更加清晰。

新版本还扩展了系统组件（system component）的范围，包括了原来的网络设备、服务器、计算设备，还包括了虚拟组件、云组件以及软件。为增加易读性，新版本还对范围内可能的系统组件进行了举例，容易被忽略的组件包括虚拟组件（如虚拟机、虚拟硬件、hypervisor）、云组件、打印设备、存储介质（纸、录音、图像、视频）、订购的服务、工具、代码库等等。

为了使读者更清晰了解范围界定，同时给出了完整的范围界定流向图如下：

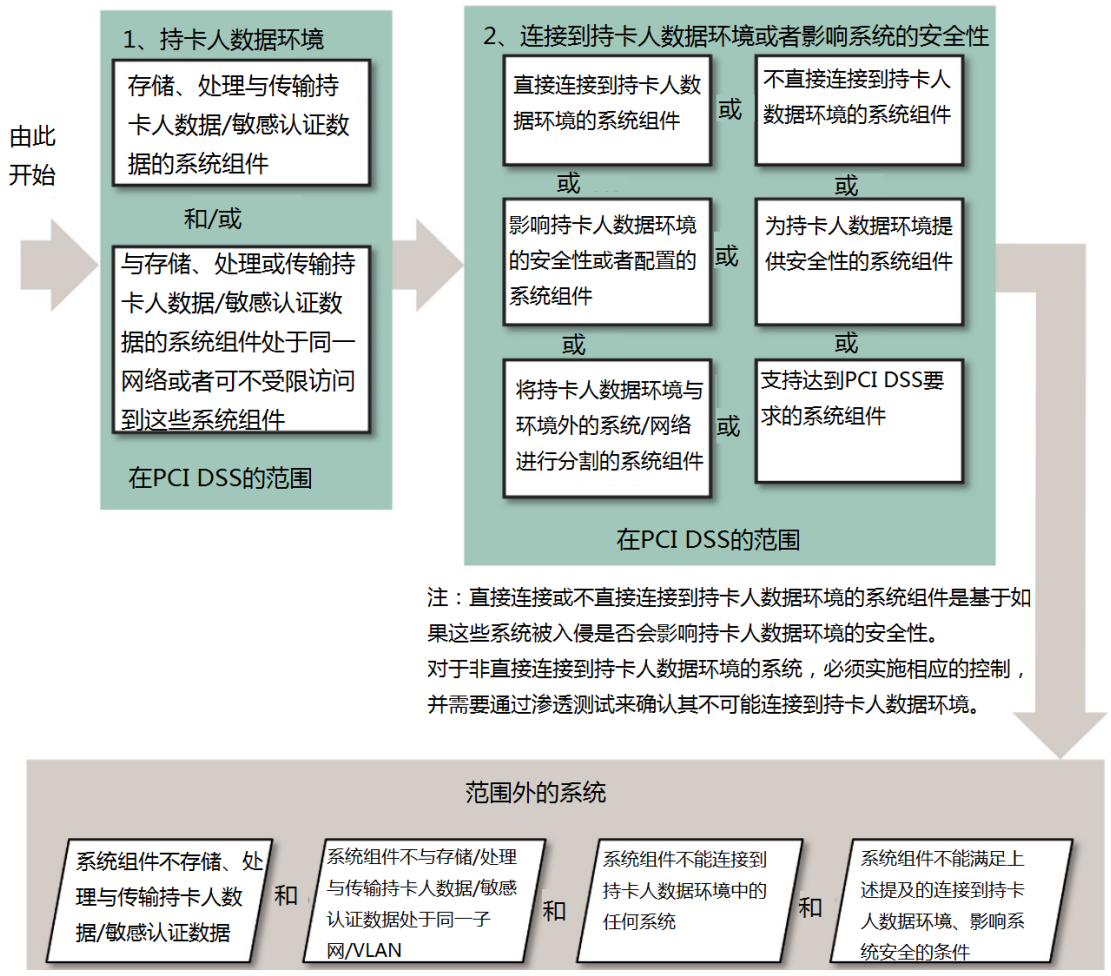

图 1：PCI DSS 范围的确定

在新版本中，进一步重申了范围确认的必要性。增加的要求 12.5.2 明确要求被审核机构每年确认 PCI DSS 的范围，作为后续年度展开 PCI DSS 合规的依据。

4.1 关于分段（segmentation）

由 v3.2.1 的网络分段（network segmentation）调整为 v4.0 的分段（segmentation）的说法，以适用于各种可实施分段的技术。新版本调整后的分段的工作流向图如下：

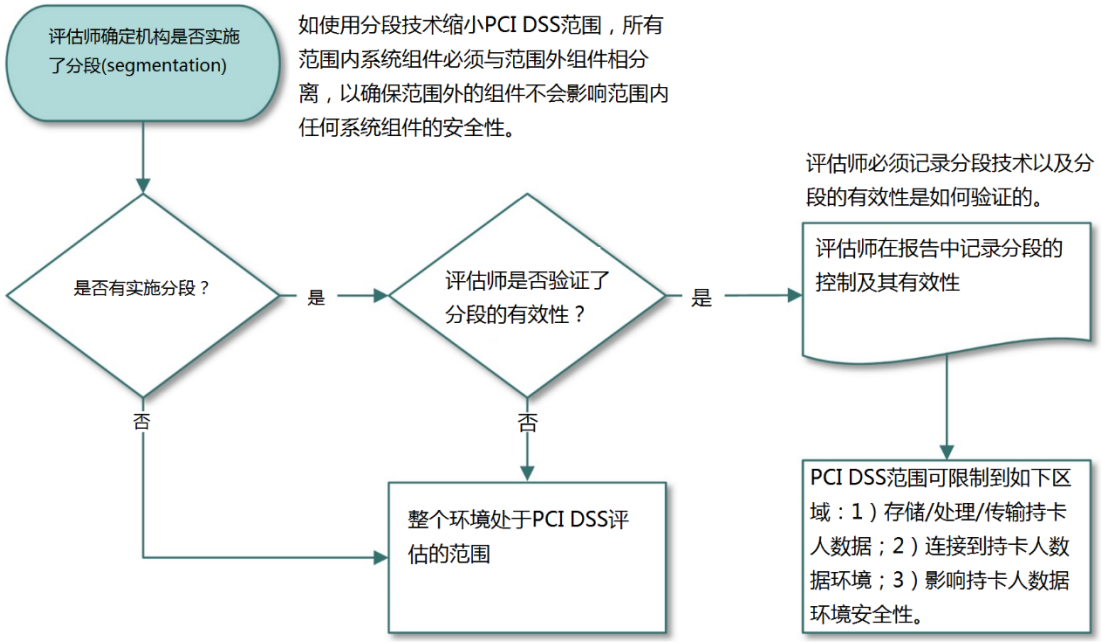

图 2：分段的确定

4.2 关于无线（wireless）部分

对于要求 11.2.1，重申即使在持卡人数据环境中没有无线且安全策略禁止无线使用的情况下，仍需要进行非法无线的探测。

4.3 加密的持卡人数据以及对范围的影响

这一部分为 v4.0 新添加的澄清，明确了将持卡人数据加密后，不足以影响 PCI DSS 范围。并举例如下情况仍在 PCI DSS 的范围内：

- 对持卡人数据进行加解密、完成密钥管理功能的系统。
- 未隔离于加解密及密钥管理流程之外的加密数据。
- 与解密密钥处于同一系统或介质的加密数据。
- 与解密密钥处于同一环境的加密数据。
- 机构能访问到解密密钥，同时也可访问到加密数据。

4.4 加密的持卡人数据及其对第三方服务供应商范围的影响

这一新添加的部分澄清了涉及第三方服务供应商（TPSP）接收或存储加密持卡人数据的适用性。在满足特定条件时（仅接收或存储另一机构的加密的持卡人数据、且没有能力对数据进行解密），第三方服务供应商可将加密的持卡人数据识别在范围之外。

4.5 使用第三方服务供应商

进一步澄清需要纳入到合规监控的供应商的范围，包括访问到 CDE 的供应商、管理范围内组件的供应商以及影响持卡人数据安全的供应商。

澄清第三方供应商需要呈现其所管理部分的合规状态（如提供合规证据），以使被审核机构达到合规状态。基于此，被审核机构与第三方服务供应商应清晰识别和划分责任，以识别：

- 第三方服务供应商范围内的服务及系统组件。
- 第三方服务供应商审核中所覆盖的 PCI DSS 要求点。
- 被审核机构自行维护的要求点。
- 被审核机构与第三方服务供应商共同维护的要求点。

基于 12.9.2 的要求，第三方服务供应商应提供其合规状态以及其职责范围内应覆盖的 PCI DSS 要求点。此处也明确期望第三方服务供应商提供其客户（被审核机构）足够的证据以支持其客户的合规。包括在需要时，提供 AOC 文件。在被审核机构需要 ROC 的相关部分时，第三方服务供应商在做好信息销密的情况下提供。如果第三方服务供应商没有执行 PCI DSS 合规，应提供相应的证据以支持客户的合规。

新版本还澄清了关于在卡品牌网站上列出的关于第三方服务供应商的合规状态的意义。对于该供应商的合规状态，如果卡品牌网站上能够清晰呈现则可作为该供应商合规状态的证据。但在需要确认这个供应商是否符合到 PCI DSS 标准的具体要求点时，仅仅查验卡品牌网站上的呈现并不能作为充分的证据用于验证所覆盖的具体要求点的证据。在此情形下，则需要该供应商补充额外的证据，比如合规声明（AOC）。

第五章：实施 PCI DSS 到日常业务过程的最佳实践

对比于 v3.2.1 的内容，v4.0 在第五章节给出了更详细的应纳入到日常业务过程的控制点，也对 PCI DSS 评估所需要的审核证据准备提供了相应的建议。

第六章：关于 PCI DSS 审核抽样

对比于 v3.2.1 的内容，v4.0 在第六章节给出了针对抽样的考虑更详细地阐述，并给出了多种场景下的抽样考虑，使得抽样更具有准确性、更高效。此版本也给出了抽样的考虑决策图如下：

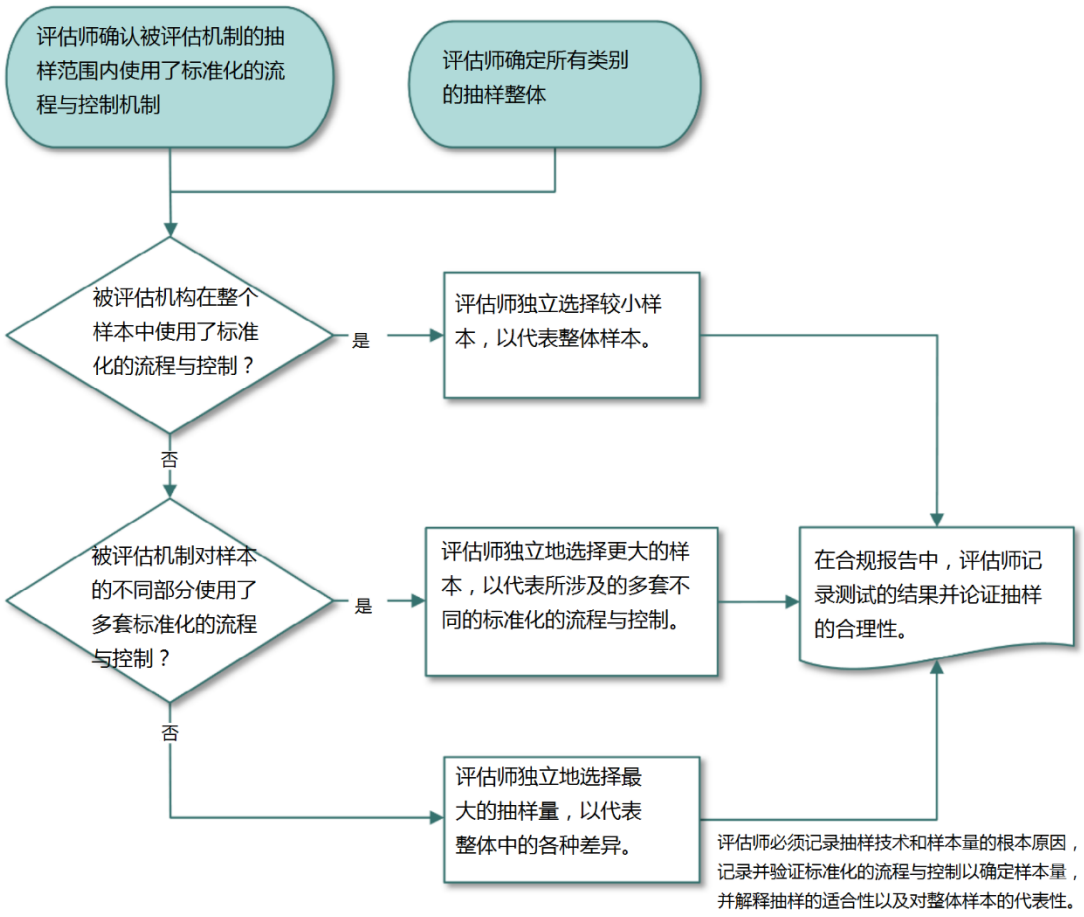

图 3：抽样的方法论

第七章：关于 PCI DSS 中执行频率的澄清

第七章节为新添加的内容，此章节进一步澄清了标准要求中所提及的频率的具体含义。如下表格供参考：

PCI DSS 要求的时间频率	描述及示例
每日（daily）	一年中的每 1 天（不仅仅是在工作日）。
每周 （weekly）	至少每 7 天一次。
每月 （Monthly）	至少每 30 至 31 天一次，或在每月的第 n 天。
每3个月（“每季度”）一次（Quarterly）	至少每 90 至 92 天一次，或在每三个月的第 n 天。
每6个月（every 6 months）	至少每 180 至 184 天一次，或在每六个月的第 n 天。
每12个月（“每年”）一次（annually）	至少每 365 天（或闰年为 366 天）一次，或在每年的同一天。

*定期（periodically）	发生的频率由被审核机构自行确定，经由风险分析进行评估和记录。该机构必须确保该频率是恰当并可满足对应要求的控制目标。
立即（immediately）	毫不拖延。实时或接近实时。
迅速（promptly）	在合理范围内尽快进行。
重大变化（significant change）	对某些要求，在实体环境发生重大变化时，应执行相应的要求。虽然构成重大变更的因素在很大程度上取决于特定环境的配置，但以下每项活动至少对 CDE 的安全性产生潜在影响，必须被视为重大变更： •添加新的硬件、软件或网络设备到持卡人数据环境中。 •持卡人数据环境中硬件和软件的任何更换或重大升级。 •账户数据流动或存储的任何变更。 •持卡人数据环境的边界和/或PCI DSS评估范围的任何变更。 •持卡人数据环境底层支持基础设施的任何变更（包括但不限于目录服务、时间服务器、日志和监控的变更）。 •支持持卡人数据环境或代表该实体满足 PCI DSS 要求的第三方供应商/服务提供商（或提供的服务）的任何变更。

表 1：执行频率的澄清

注：如上提及的“定期”，应遵循要求 12.3.1 进行评估和分析，以确定相应的频率。为方便大家使用，对需要确定频率的要求点归纳如下：5.2.3.1，5.3.2.1，7.2.5.1，8.6.3，9.5.1.2.1，10.4.2.1，11.3.1.1，11.6.1，12.10.4.1。

在此版本中，还提供了相应的指导以防止时间线被错过以及出现错过情况下的补救措施。包括如下：

- 在未按时执行相应计划事项时，立即进行通告。
- 确定可能会导致计划事项被错过的事件。
- 立即实施已错过的计划。
- 对上述事项的发生进行文档化。

第九章：对被审核机构信息的安全保护

第九章节为新添加的内容，提及了被审核机构的审核材料（包括配置标准、加密协议、拓扑图、数据流向图、AOC 等）的保护，也提出了对审核机构对被审核机构的信息保护要求。

附录：主要参考的文档

PCI DSS v3.2.1 版本至 v4.0 版本的变更摘要

https://www.pcisecuritystandards.org/documents/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r1.pdf

PCI DSS v4.0 标准文档

https://www.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf

PCI DSS v4.0 at a glance

https://www.pcisecuritystandards.org/documents/PCI-DSS-v4-0-At-A-Glance.pdf