PCI DSS v4.0 变更系列之一

——变更概述

1 变更概述

支付卡产业安全标准委员会（PCI SSC） 在 2022 年 3 月正式发布了 PCI DSS v4.0 版本，以替代现行的 PCI DSS v3.2.1 版本。

基于支付卡产业安全标准委员会所发布的“PCI DSS v3.2.1 版本至 v4.0 版本的变更摘要”、“PCI DSS v4.0 标准文档”以及举行的 PCI DSS v4.0 研讨会中提及的内容，本文旨在向读者介绍 PCI DSS v4.0 版本所带来的主要变化。本文主要适合于致力于 PCI DSS 合规的机构知晓并了解 PCI DSS v4.0 标准与现行的 PCI DSS v3.2.1 版本的主要变化。

另外，笔者尝试梳理新标准的所有技术要求点的变化，但也可能存在不全面之处。强烈建议读者在了解本文的基础上深入阅读 PCI DSS v4.0 标准的英文版本，以便更清晰地理解标准的出发点、详细的要求及审核方法。

1.1 版本变更的时间线

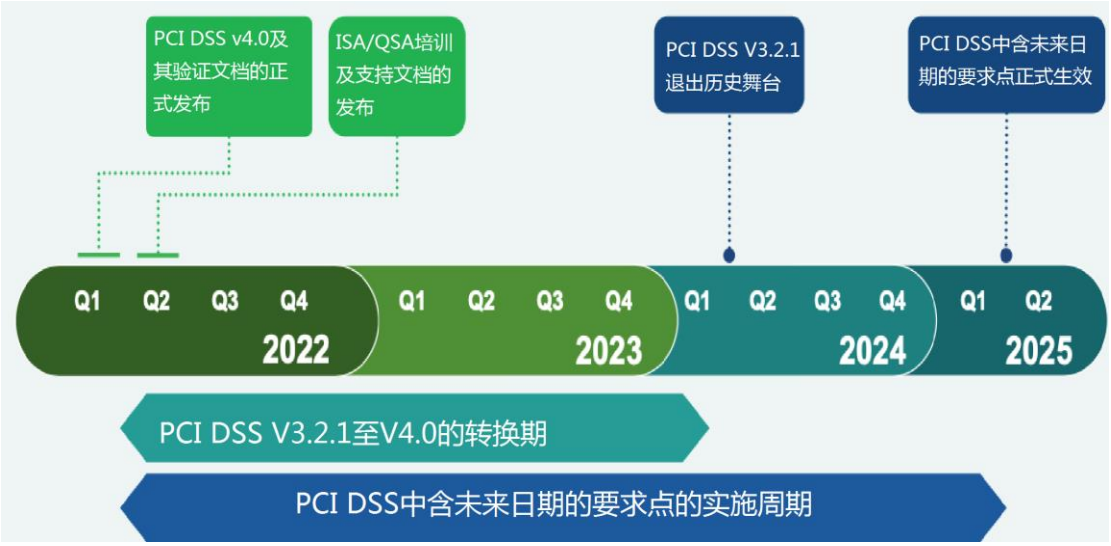

图 1:PCI DSS v4.0 的时间线计划

如上图所示，我们将 PCI DSS 的时间计划分为三个阶段。详细的说明如下：

1.1.1 发布与培训阶段（2022 年 6 月至 2022 年底）

按照标委会计划，已经从 2022 年 6 月开始发布了相关的支持文档，并展开该标准的相关培训工作。通过培训和考试的机构及评估人员将获得具备执行 PCI DSS v4.0 审核的资质。atsec 作为 PCI 标委会授权的评估认证机构，已于 2022 年 7 月中旬完成了标委会相关培训和考试，并成为首批可执行 PCI DSS v4.0 标准评估的认证机构。

1.1.2 从旧版本向新版本的转换阶段（2022 年 6 月至 2024 年 3 月）

在此阶段，被审核机构可依据自身情况，选择使用 v3.2.1 或 v4.0 标准进行合规建设和合规审核工作，直至 2024 年 3 月 31 日。在那个时间点，PCI DSS v3.2.1 版本将正式退出历史舞台。

基于 PCI DSS 标准中有很多标注为未来日期的要求点（2025 年 4 月 1 日正式变为强制的要求点），强烈建议涉及到 PCI DSS 合规的机构尽早研究和落实这些技术要求点，以便更从容地完成新版本的转换。同时，atsec 将在未来针对新版本向产业推出相应的培训活动，以助力相关机构更高效地完成版本的转换工作。

1.1.3 新标准阶段（2024 年 4 月及以后）

从 2024 年 4 月 1 日开始，PCI DSS 合规将强制使用 v4.0 版本，基于 v3.2.1 版本的评估报告将不再被产业所接受。从那时起，v4.0 将作为唯一现行的 PCI DSS 标准。

在 2025 年 4 月 1 日开始，v4.0 版本涉及未来日期的要求点，将正式变为强制要求开始实施。

1.2 主要变化概述

新版本的变化主要体现在如下几个方面：引入更灵活的合规和审核方法、标准易读性更强、标准要求点格式变化以及更强的控制点要求等等。

1.2.1 引入了灵活性

该版本的一个突出的变化是在 PCI DSS v4.0 的第八章节，引入了“定制方法”（Customized approach）的审核方法。这个审核方法，允许被审核的机构基于 PCI DSS 标准的控制目标定义适合于本机构的控制矩阵，由审核机构独立地审核其控制措施。这种审核方法增加了标准要求的灵活性，更适应于安全管理能力突出、技术先进的机构。

1.2.2 易读性更强

新版本在 PCI DSS 适用范围、抽样等章节，做了更多的澄清说明，使得标准的要求更清晰、更易读。

在 PCI DSS 技术要求部分，PCI DSS 仍是 6 大类 12 个要求章节。但在要求点的格式、要求点的组织结构以及章节的措辞等方面，呈现的思路更清晰，更易理解。

1.2.2.1 要求点的格式变化

对比于 v3.2.1，v4.0 在具体要求点的呈现上，更清晰、更易读。主要体现在：

第一列添加了定制方法目标（customized approach objective），以用于开发定制化验证的需要。

第一列添加了适用性说明（applicability notes），阐述对应要求的适用性情况。

第三列的指南（guidance）使用了更清晰的思路，按目的（purpose）、良好做法（good practice）、定义（definition）、示例（examples）、更多信息（further information）的格式进行呈现。

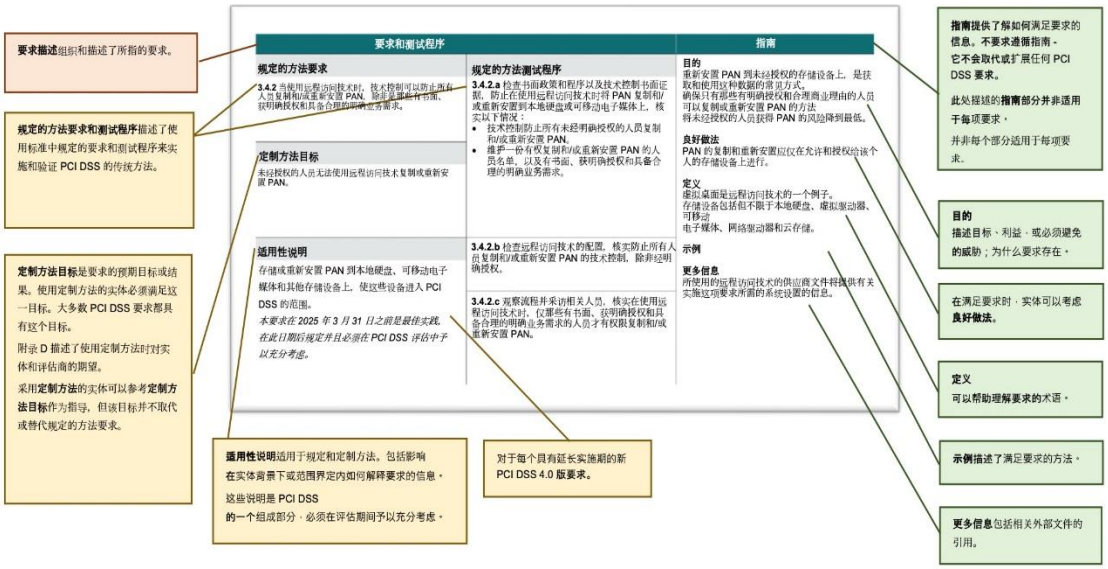

图 2：要求点的格式说明

1.2.2.2 要求点的组织结构

由 v3.2.1 在每个大的要求点的最后一部分（如要求 1 最后的要求 1.5）提出安全策略与流程的要求，转变为在每个大的要求的第一个要求提出安全策略与流程的要求。

1.2.2.3 各章节的主题

整体使得各章节更易读，更符合各章节具体要求的主题。比如：

要求 1 针对防火墙的要求，变为针对网络安全控制，以适用于更广泛的网络访问控制措施。

要求 2 从禁止厂商默认设置（“vendor defaults”）调整为对所有的系统组件应用安全设置。

要求 3 从对持卡人数据的保护，调整为对账户数据的保护。

要求 4 进一步强调对公网传输“强加密”的使用。

要求 5 明确防止恶意软件也适用于网络设备。

要求 6 从“开发和维护安全的系统与应用”调整为“开发和维护安全的系统与软件”，强调对软件的维护。

要求 7 从“限制对持卡人数据的访问到业务必须”调整为“限制对持卡人数据和系统组件的访问到业务必须”。

要求 10 措辞从“追踪和监控所有对网络资源和持卡人数据的访问”到“记录和监控所有对系统组件和持卡人数据的访问”。

要求 11 措辞从“定期测试系统和流程的安全性”变为“定期测试系统和网络的安全性”。

1.2.3 更严格的控制要求点

除了措辞和描述上进行了更新的要求点，新版本在 v3.2.1 版本 263 个要求点的基础上增加了 64 项要求，新版本的要求点增至 327 个。整体来看，在要求 3 持卡人数据存储保护、要求 5

恶意软件防护、要求 11 扫描与修复管理、要求 12 合规范围维护等方面均提出了新的或更高要求。比较显著的变化如下：

- 要求 3.3.2：对授权完成前所存储的敏感认证数据进行强加密保护。
- 要求 3.5.1.1：在使用到哈希对持卡人数据进行保护时，需要引入密钥及其安全管理。
- 要求 5.3.3：对可移动介质的防恶意软件要求。
- 要求 5.4.1：增加了对钓鱼攻击的防护要求。
- 要求 6.4.3：对支付页面的保护要求。
- 要求 11.3.1.2：使用认证登录的方法执行内部漏洞扫描。
- 要求 11.3.2.1：CVSS4.0 及以上的外部漏洞扫描的漏洞必须进行修复。
- 要求 12.3.3、12.3.4、12.5.2: 对所使用的加密套件、硬软件技术、PCI DSS 合规范围进行维护。
- 要求 A1.1.1 和 A1.1.4：实施多租户供应商环境与客户环境的逻辑分离，并通过渗透测试的方法确认逻辑分离的有效性。

对于增加的 64 个要求点，有 53 项针对所有的合规机构，另外 11 项仅针对服务供应商。

新增加的要求点中，有 13 项新要求在 v4.0 发布后（2022 年 6 月起）立即生效，这些主要是围绕各要求章节的角色定义及分配的要求。尽管另外的 51 项要求将在 2025 年 3 月 31 日变为强制要求，但 atsec 仍建议合规机构尽早了解和落实新要求所对应的技术措施与流程，以便更平缓地完成新版本的转换工作。具体的 64 项新要求，请参见本系列的“PCI DSS v4.0 新要求点统计”或者“PCI DSS v3.2.1 版本至 v4.0 版本的变更摘要”第六章节。