PCI DSS V3.2 再回首
——谈谈在 2018 年强制执行的要求

作者：沈国华、高向东（atsec 中国）

2018 年 1 月

关键词：PCI DSS、信息安全、变更管理、事件管理，密码学

atsec(Beijing) information technology Co., Ltd

Floor 3, Block C, Building 1, Boya C-Center,

Beijing University Science Park, Life Science Park

Changping District, Beijing, Postcode: 102206

P.R.China
Tel +86-10-53056681
Fax +86-10-53056678

www.atsec.cn

目录

1 PCI DSS 标准发展背景

根据 PCI（Payment Card Industry）标准生命周期要求，每三年更新标准版本，并伴随 IT 信息技术产业发展不定期发布标准的小版本更新。早在 2016 年 4 月，PCI SSC（Payment Card Industry Security Standards Council）支付卡产业安全标准委员会就已经正式发布了 PCI DSS（Payment Card Industry Data Security Standard）支付卡产业数据安全标准的 V3.2 版，并要求于当年的 11 月开始全面使用 V3.2 开展评估工作并出具合规性报告。

自 PCI DSS V3.2 发布至今已有近两年的时间，很多接受评估的机构（包括收单机构、发卡机构、服务提供商或商户）已经连续两年使用 V3.2 标准开展合规建设和评估工作。而在 PCI DSS V3.2 的诸多要求中，存在这样一些特殊的标准要求：这些要求在 2018 年 1 月 31 日之前可作为机构进行 PCI DSS 标准合规建设的最优方法，而在 2018 年 1 月 31 日之后成为标准的正式强制要求。本文的目的是分析这些在 2018 年变为强制的要求，以期对执行合规的机构有相应的指导与帮助。

2 第一部分：PCI DSS V3.2 标准回顾

PCI DSS V3.2，共计 6 大类 12 个要求，该标准框架自 PCI DSS V1.0 开始至今没有变化。基于 12 个要求，标准提出更为细致的具体要求，而这些具体的要求才是最终指导标准合规工作的落脚点。

建立并维护安全的网络和系统	
要求 1	安装并维护防火墙配置以保护持卡人数据
要求 2	不要使用供应商提供的默认系统密码和其他安全参数
保护持卡人数据	
要求 3	保护存储的持卡人数据
要求 4	加密持卡人数据在开放式公共网络中的传输
维护漏洞管理计划	
要求 5	为所有系统提供恶意软件防护并定期更新杀毒软件或程序
要求 6	开发并维护安全的系统和应用程序
实施强效访问控制措施	
要求 7	按业务知情需要限制对持卡人数据的访问
要求 8	识别并验证对系统组件的访问
要求 9	限制对持卡人数据的物理访问
定期监控和测试网络	
要求 10	跟踪并监控对网络资源和持卡人数据的所有访问
要求 11	定期测试安全系统和流程
维护信息安全策略	
要求 12	维护针对所有工作人员的信息安全政策
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
附录 A2	针对使用 SSL/早期 TLS 的实体的 PCI DSS 附加要求
附录 A3	指定实体补充认证(DESV)

3 第二部分：2018 年 1 月 31 日起强制实施的要求

PCI DSS 标准自 2018 年 1 月 31 日起强制实施的要求，均是 PCI DSS V3.2 对比 V3.1 单独新增的具体要求（更多 PCI DSS 标准变更分析请参见：http://www.atsec.cn/downloads/pdf/PCI_DSS_standard_V3.2_change_analysis.pdf），而非原有要求的修订，这些要求均被注释：“本要求在 2018 年 1 月 31 日前属于最优方法，此后将成为一项要求。”

对于这些新要求，开展标准合规工作的机构可能面临着理解和实施方面的挑战。为此，atsec 逐一解读如下：

3.1 PCI DSS 要求 3.5.1

3.5.1 ***仅针对服务提供商的额外要求：***维护包含以下内容的加密架构文档描述：
• 用于保护持卡人数据的所有算法、协议和密钥的详情，包括密钥强度和到期日
• 每个密钥主要用途的说明
• 用于进行密钥管理的任何 HSM 和其他 SCD 的清单

如果说我们把 PCI DSS 的要求从实施方法层面分为管理类要求和技术类要求的话，那么 3.5.1 这个新增要求无疑属于管理类要求。因为本要求的主要目的是维护一份“加密架构文档”，文档的内容需包括上述要求中列举的三点。

要求 3.5.1 是在“要求 3 保护存储的持卡人数据”下的具体要求，前提是机构选择了“具有相关密钥管理流程和程序的强效加密法”对持卡人数据进行了保护，那么无论是数据加密密钥（DEK： Data Encrypted Key），还是可能存在的密钥加密密钥（KEK：Key Encrypted Key），或是涉及的加密机等设备，都需要在相关文档中加以说明。基于 atsec 以往实施经验，维护相应的“加密架构文档”需要关注如下三个关键点：

1，建立文档本身的管理制度，或者符合企业现有管理体系的文档管理制度。比如需要清楚定义文档编写责任人、评审责任人、批准责任人，以及文档如何正式发布和如何定期评审等。

2，文档的范围。应该与 PCI DSS 合规性范围一致，间接保护持卡人数据的情况，特别是 KEK 的情况，也应纳入管理的范围。

3，该要求具体实施时，需要特别关注密钥到期之后的处理流程，这也是目前很多机构在实际运行中最薄弱的一个环节。

最后，请特别注意该要求仅针对服务提供商，即商户可不履行此要求。

3.2 PCI DSS 要求 6.4.6

6.4.6 完成重要变更后，须对所有新的或变更的系统和网络实施所有相关的 PCI DSS 要求，并在适当情况下更新文档记录。

要求 6.4.6 也是一项管理类要求，是在“要求 6.4 系统组件的所有变更均须遵守变更控制流程和程序。”下的一个具体要求，因此也是归属于变更管理的一项要求。

从标准合规一致性的角度出发，一个变更前符合 PCI DSS 要求的系统和网络，理论上变更后也应符合 PCI DSS 要求。但在实际运行过程中仍存在变更后的系统或网络因管理疏忽而没有符合 PCI DSS 标准的情况。因此，在 PCI DSS V3.2 中，要求 6.4.6 明确地提出在变更管理中需加入标准合规一致性检查的要求，以确保变更前后，特别是重要变更之后，能保证标准合规的一致性。

虽然标准 6.4.6 是从结果的角度对变更流程的标准合规一致性做出了要求，即“完成重要变更后”，要确保变更后合规。但从 ITSM（IT 服务管理）的视角看，变更管理的重点更在于变更之前的评估，所以在标准实际实施的过程中，往往会把一致性检查的工作前移到变更评估的环节中，要求变更方案制订者清楚的说明变更过程中要如何确保标准合规的一致性，也要求变更管理委员会（CCB：Change Control Borad）在对变更方案进行评估的过程中要确认标准合规一致性的可行性和有效性。同时，建议在变更方案中还要说明变更之后需要更新哪些文档的记录，例如：需更新网络拓扑图、资产清单等。

以上是在标准实施落地方面的一些建议。如果该要求体现在流程和制度上，则一般建议相应的机构修改自身管理体系中已有的“变更管理流程”，例如变更方案制定、变更评审、变更后回顾等加入标准合规一致性检查的要求。如果能在相应的表单模板中增加标准合规一致性的检查项，也会更有助于该要求的落地实施。

3.3 PCI DSS 要求 8.3.1

8.3.1 将针对所有非控制台访问的多因素验证融入针对具有管理访问权限的工作人员的持卡人数据环境。

要求 8.3.1 是一项技术类的要求，因为要实现多因素验证，往往需要一些技术手段的配合。

所谓多因素验证，PCI DSS 的术语表中给出的说明是：“通过认证至少两个因素验证用户身份的方法。这些因素包括用户所有（例如智能卡），用户所知（例如密码、口令或 PIN）或者用户特征或用户所为（例如指纹或其他类型的生物特征）。”

这个要求是从 V3.1 中的双因素要求演化而来，与 V3.1 的要求类似，认证两种或两种以上因素，可被认为是多因素认证。因此在具体实施时，机构原有的双因素验证机制是可以沿用的，所不同的是 V3.2 在验证场景上发生了扩展。

- 首先，V3.1 的验证场景在 V3.2 中依然沿用，被放到了要求 8.3.2 中，即“针对来自该实体网络外部的所有远程网络访问（针对用户和管理员，并包括出于支持和维护目的的第三方访问）加入多因素验证。”
- 其次，V3.2 在要求 8.3.1 中新增了一个场景，即所有个人基于管理访问需要而通过非控制台进入持卡人数据环境（CDE：Cardholder Data Environment）的情况。该场景下的要求比 8.3.2 的要求更进一步，要求所有“非控制台”的管理访问均需要多因素验证。

何谓“非控制台”，其术语说明是：“对系统组件的逻辑访问，通过网络接口（而不是通过直接的物理连接）连接到系统组件上。非控制台访问包括通过本地/内部网络进行的访问，也包括通过外部或远程网络进行的访问。”即除了直接把键盘鼠标连接到服务器上，或直接通过 console 线连接到网络设备上之外的所有网络访问，无论是内网还是外网，都称之为非控制台访问。

要满足 8.3.1 和 8.3.2 的要求，等于是所有对于 CDE 中系统组件的管理访问都需要多因素验证，无论是内网还是外网。基于 atsec 以往项目的实施经验，通常有两种做法，一是为 CDE 中的每个系统组件实施多因素控制，这对于合规范围小的环境勉强可行，大型机构的环境范围则基本不可取。二是在 CDE 的边界实施一个多因素控制设备作为跳板机，再通过跳板机连接到 CDE 内的系统组件，这是比较常见的做法，因为这与大型机构的登录管理要求（如统一登录和认证、操作审计等）不谋而合。目前比较常见的堡垒机部署方案可以支持多因素验证的要求。

由于要求 8.3.1 是技术类要求，虽然大部分机构都有较好的基础来实现非控制台多因素控制，但也有机构现有的设备无法支持，这就意味着一些新设备的引入或现有设备的改造，可能会带来资金和时间方面的挑战。因此对于要求 8.3.1 的落实，相关合规建设机构还应该未雨绸缪，尽快开展评估和落实整改工作。

3.4 PCI DSS 要求 10.8 和 10.8.1

10.8 ***仅针对服务提供商的额外要求***：实施流程，以便及时检测和报告关键安全控制系统故障，包括但不限于以下方面故障：
• 防火墙
• IDS/IPS
• FIM
• 杀毒
• 物理访问控制
• 逻辑访问控制
• 检查日志机制
• 分段控制（如使用）
10.8.1 ***仅针对服务提供商的额外要求***：及时响应任何关键安全控制故障。安全控制故障响应流程须包括：
• 恢复安全功能
• 识别并记录安全故障持续时间（日期以及从开始到结束的时间）
• 识别并记录故障原因（包括根本原因），并记录解决根本原因所需的补救措施
• 识别并解决故障期间引发的任何安全问题
• 执行风险评估，确定是否需要因安全故障执行进一步操作
• 实施控制，以防故障原因再次发生
• 恢复安全控制监控
要求 10.8 和 10.8.1 也是管理类要求，主要是针对关键安全控制系统故障的检测、报告和响应流程。其中“关键安全控制系统故障”在要求 10.8 中做了列举，其相应流程的要求在 10.8.1 中也做了说明。

实体在实施要求 10.8 和 10.8.1 时，比较简单的做法是参照 ITSM 中的“事件管理流程”和“问题管理流程”：

- 要求 10.8.1 中对于流程的要求，包括尽快恢复服务、寻找根本原因，这与 ITSM 中的事件管理和问题管理都有所关联，可借鉴并参考。
- 要求 10.8 中有关故障的检测、报告以及要求 10.8.1 中恢复安全功能以及记录持续时间等要求，可以参考“事件管理流程”。
- 要求 10.8.1 中后续查找故障原因，并实施控制防止故障再次发生的要求，可以参考问题管理流程以及变更流程。当然，如果实体已经实施了 ITSM 流程，基本上只要定义好故障的范围，即可满足要求。

除了流程方面的要求，新增的要求 10.8 和 10.8.1 与原有的要求 12.10.1，即事故响应要求之间的关系，可参考 ISO/IEC 27001 中所提出的事态（Event）和事件（Incident）的概念：

- 要求 10.8 和 10.8.1 所关注的故障类似于事态，要求 10.8 中所列举的“关键安全控制系统故障”，很少会直接影响业务的开展。比如防火墙的失效，可能并不会直接导致支付业务的暂停，但是会带来安全风险。
- 要求 12.10.1 更关注对业务的影响，需要启动事故响应计划。比如导致业务中断的大“故障”。

故而，我们不难理解 PCI DSS V3.2 新增要求 10.8 和 10.8.1，标准要求明确列出“关键安全控制系统故障”，虽然不会直接影响业务，但一旦发生故障，会大大增加业务发生问题的风险。

3.5 PCI DSS 要求 11.3.4.1

11.3.4.1 ***仅针对服务提供商的额外要求***：如果使用了分段，请通过至少每半年执行一次穿透测试以及在分段控制/方法有任何变更后执行穿透测试，以确认 PCI DSS 范围。

要求 11.3.4.1 是在渗透测试要求下的一个具体要求：如果机构采用了网络分段（Segmentation）的技术，则要在原来每年一次内部和外部渗透测试的要求下，新增每半年一次的渗透测试，以及网络分段方法实施之后执行渗透测试，以确认 PCI DSS 范围。

所谓网络分段，术语中的阐述如下：也称为“分段”或“隔离”。网络分段可将存储、处理或传输持卡人数据的系统组件与其他无法执行此类操作的系统隔离开来。充足的网络分段可缩小持卡人数据环境的范围，从而缩小 PCI DSS 评估的范围。关于使用网络分隔的相关指南，请参见《PCI DSS 要求和安全评估程序》中的“网络分段”部分。网络分隔并不属于 PCI DSS 的强制要求。

虽然网络分段不是标准要求，但对于大部分机构而言，为了减少标准合规性的风险和成本，往往还是会通过防火墙或者其他网络控制技术，把 CDE 与其他网络隔离开。因此，这些实体就需要在原有每年一次全面的渗透测试的基础上（包括要求 11.3.1 的外部渗透测试、要求 11.3.2 的内部渗透测试以及 11.3.4 的分段验证渗透测试），新增一次半年度的分段验证渗透测试。测试的目的是验证分段技术的有效性，即验证 PCI DSS 范围。

网络分段技术发生变更之后需要再次进行分段验证渗透测试。这一要求如有可能，也可以和变更管理流程相结合，实施效果会更好。

PCI DSS 中并没有对渗透测试由谁来执行提出要求，不过考虑到渗透测试是一项较为专业的技术工作，在 atsec 以往实施的合规评估工作中 atsec 自有渗透测试实验室@PT Lab 将会为机构执行全面的渗透测试服务。

3.6 PCI DSS 要求 12.4.1

12.4.1 ***仅针对服务提供商的额外要求***：行政管理人员应明确保护持卡人数据和 PCI DSS 遵从性计划的责任，包括：
• 全面负责维护 PCI DSS 遵从性
• 规定 PCI DSS 遵从性计划以及与行政管理人员进行沟通的相关章程
要求 12 都是管理类要求，要求 12.4.1 也不例外。该要求具体规定了机构高层以及所谓 PCI DSS 合规性负责人的职责。

所谓行政管理人员，一般认为是公司的高级管理层，或最高管理层。要求 12.4.1 首先明确了最高管理层的职责，即把机构全面负责 PCI DSS 合规性的职责归属于最高管理层，这是非常明智的做法。由最高管理

层来全面负责标准的合规性工作，在以 ISO 9001 为代表的管理体系（Management System）类标准中由来已久，这是管理体系类标准在 30 多年推行工作中被实践证明非常重要也非常行之有效的方法。PCI DSS 标准也在要求中明确指出了最高管理层的职责，这对于采用 PCI DSS 进行机构信息安全合规建设非常重要。

要求 12.4.1 本身并没有强制需要指定一位 PCI DSS 合规性负责人，但在 PCI DSS 的指南中有提到：“可指定组织内的个人角色和/或业务单元对 PCI DSS 合规性计划全面负责。”在管理体系类标准中，往往都会提及一个“管理者代表”的概念，该角色来自于机构高层，但又对特定的管理体系全面负责，该角色即有责任又有资源，便于在机构内部不同部门之间开展相关工作。因此，设定一个 PCI DSS 合规性负责人（类似于管理者代表）将非常有助于 PCI DSS 持续合规工作的开展。

除了人员的角色和职责确定之外，要求 12.4.1 中还包括“规定 PCI DSS 合规性计划以及与行政管理人员进行沟通的相关章程”，机构需拟定并发布这份正式的章程（Charter）。Charter 也可以简单理解为授权书，其中可以说明为满足 PCI DSS 合规性而设定的相关人员角色和职责，及其正式的授权。此外，也可以在 Charter 中丰富 PCI DSS 合规工作人员的工作方式、与高层沟通的要求等内容。

3.7 PCI DSS 要求 12.11 和 12.11.1

12.11 ***仅针对服务提供商的额外要求***：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。审查须涵盖以下流程：
• 日常日志审查
• 防火墙规则集审查
• 将配置标准应用于新系统
• 响应安全警报
• 更改管理流程
12.11.1 ***仅针对服务提供商的额外要求***：维护季度审查流程文档记录，使其包括：
• 记录审查结果
• 由负责 PCI DSS 遵从性计划的指定工作人员审查并签核结果

12.11 和 12.11.1 仍然是管理类要求，关于建立机构内部季度审查制度。该要求与管理体系类标准所提倡的内审制度在形式和内容上都有着很大的不同。管理体系类标准所要求的内审，一般是一年一次，内容是对于所有标准要求的检查；而 PCI DSS V3.2 所要求的审查制度，频率是一个季度一次，内容则不少于上述标准要求 12.11 所提到的五点即可。所以 PCI DSS 所要求的季度审查，频率较高，但审查的内容反而不是特别多。但无论是年度内审还是季度审查，目的是一致的，即希望机构在两次外部审查之间能够自觉地保持持续合规性。

针对该要求，机构在具体实施层面则不难，通过在流程上建立季度审查制度即可。为了保证季度审查制度的可操作性，制度中建议规定以下内容：

- 首先是开展季度审查的人员，借鉴管理体系类标准内审的经验，可能需要确保开展季度审查的人员有相应的技能，包括但不限于了解 PCI DSS 标准以及知晓如何开展审查工作。此外在具体人选的选择方面要考虑回避原则，即不能审查自己的工作。
- 其次，在工作流程和模板方面，可以建立检查计划、检查单、检查报告的模板，确保检查工作的规范性。
- 第三，要求 12.11.1 提到的最终检查结果（可以理解为检查报告）要得到必要的评审和批准。
- 最后，PCI DSS 该要求没有明确说明要像管理体系类标准建立纠正措施流程，但是值得借鉴的最佳实践。对于检查中出现的问题，开展纠正、原因分析和纠正措施的三部曲。

4 第三部分：2018 年 6 月 30 日起强制实施的要求

第二部分中已说明 PCI DSS V3.2 中自 2018 年 1 月 31 日开始强制实施的要求。除此之外，PCI DSS 正文所提到的要求没有其他需要在特定时间点开始实施的要求了。

但是，在 PCI DSS 的附录中提到了另外一个时间点，即 2018 年 6 月 30 日，而这个时间点提出的一项要求，对很多开展合规性的机构而言，可能面临着比第二部分实施更大的挑战。在 PCI DSS V3.2 的附录 A2 中提到：

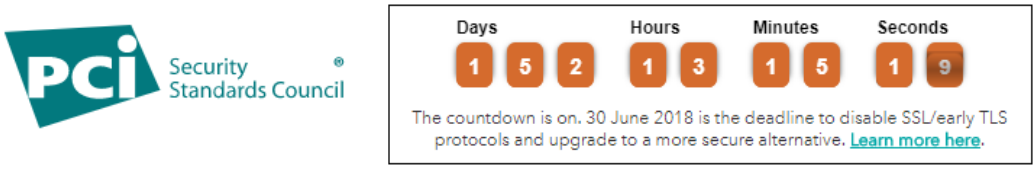
• 2018 年 6 月 30 日后，所有实体均须已停止将 SSL/早期 TLS 用作安全控制，并且仅使用协议的安全版本（下文最后一个要点对特定 POS POI 终端许可进行了说明）。

• 2018 年 6 月 30 日前，使用 SSL 和/或早期 TLS 的现有实施项目须采用正式的风险降低和迁移计划。

• 可被确认为不易受任何已知 SSL 和早期 TLS 漏洞影响的 POS POI 终端（及其连接到的 SSL/TLS 终端点），可在 2018 年 6 月 30 日后继续将这些 POS POI 终端用作安全控制。

相信很多持续开展 PCI DSS 合规工作的机构均已了解，在 PCI DSS V3.1 的要求 2.2.3、2.3 和 4.1 中就已经分别提到了要停止使用 SSL 和早期 TLS 的要求，当时的限制时间是 2016 年 6 月 30 日。但是由于产业一些条件的限制，PCI SSC 在 2015 年底公告将停止使用 SSL 和早期 TLS 的时限推迟到 2018 年 6 月 30 日，这个事件在某种程度上也促成了 PCI DSS V3.2 在 2016 年 4 月的公布。

由于 SSL 和早期 TLS 存在着众所周知的安全漏洞，如 POODLE 等，因此 PCI SSC 给出的 2018 年 6 月 30 日的时限应该不会再有变化。特别是最近 PCI SSC 已经在官网放出倒计时，以一种相当有紧迫感的方式提醒各机构执行停止使用 SSL 和早期 TLS 的工作。



对于广大还在使用 SSL 和早期 TLS 的实体而言，要关闭 SSL 和早期 TLS，需要考虑的可能更多是业务层面的挑战，而非技术方面。因为关闭 SSL 和早期 TLS 就意味着放弃对一些早期浏览器的支持，如 IE6 等。这也是 PCI DSS 中提出需要“正式的风险降低和迁移计划”的原因。在后续几个月的时间里，建议各机构能尽早考虑关闭 SSL 和早期 TLS 的工作，否则在 6 月 30 日之后将无法通过 ASV 季度扫描。

当前情况下对早期 TLS 的判定，建议参考美国国家标准与技术研究院（NIST：National Institute of Standards and Technology）的出版物：SP 800-52 Rev. 2 (DRAFT)。简而言之，在当前的安全情况下：

- 仅使用 TLS 1.2 是强烈建议的
- TLS 1.1 是目前暂时可以接受的
- TLS 1.0 及 SSL 2.0、3.0 则不被接受。

5 小结和参考文献

本文通过三个部分的介绍，说明了 PCI DSS V3.2 中需要从 2018 年 1 月 31 日开始强制实施的要求，以及从 2018 年 6 月 30 日开始需要停止使用 SSL 和早期 TLS 的要求。为此，对于广大开展 PCI DSS 合规工作的机构而言，2018 年将是非常重要且富有挑战性的一年。同时， atsec 也将一如既往地为各机构以及 PCI 产业提供有关 PCI DSS 标准及其他信息安全方面的服务，为营造更安全的支付环境而共同努力。

参考文献

[1]. PCI DSS: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2.pdf

[2]. atsec: http://www.atsec.com

[3]. ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements

[4]. ISO 9001:2015 Quality management systems – Requirements

[5]. Office of Government Commerce，ITIL/Service Support, TSO for OGC, 2006

[6]. NIST SP 800-52 Rev. 2 (DRAFT) Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, 2017