浅谈信用卡收单机构和发卡机构的 PCI DSS 合规

作者：刘岩（atsec 中国）

2012 年

关键词：支付卡产业、安全评估、PCI 、QSA、ASV

atsec(Beijing) information technology Co., Ltd

Room 119, Building 2, No.1, Street 7, Shangdi,

Haidian District, Beijing, P.R.China 10085

Tel +86-10-84834011

Fax +86-10-82890017

近年来，信用卡用卡安全问题备受关注。众所周知，支付卡产业数据安全标准（PCI DSS：Payment Card Industry Data Security Standard）是该领域最为权威且全球广泛采用的信息安全合规建设以及安全评估的最佳实践。世界范围内，诸多信用卡收单机构和发卡机构、商户，以及支付服务提供商已经实现了合规评估，或者正在致力于合规建设。而在我国国内，服务提供商的 PCI DSS 合规评估工作已经比较广泛的被接受和认可，比如快钱、易宝支付、首信易支付、盛付通、Oncard Payments 等诸多的支付服务机构已经通过了 PCI DSS 的合规建设并持续通过 atsec 的中立的第三方的评估；国内银行的信用卡收单机构和发卡机构的 PCI DSS 合规建设也在近两年得到了越来越多的关注，VISA 作为卡组织，其风险管理的要求中对于收单和发卡机构的 PCI DSS 合规建设也是重中之重。多年以来，VISA 组织在全球范围推行基于 PCI 相关要求的风险管理体系，比如亚太地区的帐户信息安全（AIS：Account Information Security）。

本文谨从 atsec 独立的第三方评估和 VISA 风险管理的角度分享收单机构和发卡机构致力于 PCI DSS 合规建设中的一些心得和经验，希望能够对于国内信用卡安全起到些许的推进作用。

PCI DSS 合规价值

PCI DSS 标准从信息安全管理体系、网络安全、物理安全、数据加密等方方面面提出了诸多的安全基线要求。虽然没有任何一个信息安全标准或者安全建设可以保障实现百分之百的抵御安全风险，然而根据业界的积累，能够实现 PCI DSS 并且严格按照 PCI DSS 的要求持续实施针对持卡人数据环境的安全防护，安全事件发生的可能性将大大降低。

除了很多具体的技术改进和安全防护提高之外，致力于 PCI DSS 合规建设合评估工作的价值大体可以总结为以下几个层面：

- ☐ 识别和发现机构可能被攻击的薄弱环节
- ☐ 通过外部独立的第三方评估机构的安全评估提高客户自身的安全级别和降低安全风险
- ☐ 提高人员对于信息安全的意识
- ☐ 管理体系的符合性建设可以塑造经营良好的机构形象，正式评估结果更进一步验证并公开认可其符合性；增强与机构业务往来伙伴的信心和满意度
  - ☐ 监管机构或者权威部门
  - ☐ 客户、合作伙伴、供应商
  - ☐ 机构内部组织和部门之间
  - ☐ 保险公司
- ☐ 管理体系的建设进一步加强机构的内部管理和控制：
  - ☐ 加强公司管理的高级别的安全性，使高层的方针政策融入到具体的业务流程、操作流程、和人事财务等行政管理流程之中，并通过工作模版/工具使得各项记录更加简化有效
  - ☐ 建立可计量的机制来获得管理支持，管理和技术使用共同语言对话
  - ☐ 在公司内增强安全控制的实务保障
  - ☐ 加强中立、独立、且管理层信任的外部审计，分担部分管理层审核（management review）的压力
  - ☐ 全员提高安全意识，全员深刻体会企业文化
  - ☐ 加强投资信心
- ☐ 可以降低诸多的成本和费用：
  - ☐ 有效的管理和降低安全事件的影响，减小处理风险的投资；完整的风险管理、业务连续性和应急响应等细节的完善更是直接降低了重大事件发生的风险；

- 通过符合性的审计和认证，可以减少其他各个领域的外部审查或调研，比如西方客户或者法律领域经常发生的尽职调查（Due Diligence）等；
- 可以减少保险相关费用（insurance premium），通过符合性建设直接带来长期的必要保险费用的减低，或者保险额、保险范围的增加；
- 通过管理体系职责明确，可以与相关人员分担安全工作。

- 符合性建设和认证具有市场价值，在同行业同领域对手面前占据绝对的优势，提高自身竞争力。
- 符合性建设和认证可以为全球信息交流建立国际信任且认可的平台，是机构在世界舞台上展现自己的重要因素，也很有可能是先决条件。

最后想说的是，PCI DSS 是面向支付产业链上所有机构的基线要求，需要这个产业链上所有涉及到持卡人数据（比如信用卡主账号等信息）的存储、交易和传输的各个机构的共同参与，只有全面广泛的实现了合规才能真正做到保护持卡人数据降低信用卡盗用的风险。

合规的重点和难点

PCI DSS 是一个技术基线标准，它和 ISO/IEC 27001 及其系列关注在信息安全管理体系建设的标准有较大程度的相容和互通性，然而 PCI DSS 更加专注在持卡人数据的保护，要求会更加具体化和细节化。故而，可能从某种意义上来看，实现 PCI DSS 的合规建设工作也不是非常容易的事情，因为需要做到每条要求的明确的合规。

致力于 PCI DSS 合规工作的第一步也是比较重要的环节就是范围的确定。PCI DSS 标准鼓励机构采用合理的方式精简持卡人数据环境，这不仅仅是为了降低审核的难度和时间，更是为了降低机构处理持卡人数据的风险。

根据 atsec 以往项目经验和业界积累，依据实现 PCI DSS 合规建设目标的优先级将整个 PCI DSS 合规建设分为六个里程碑。每一个里程碑所要达到的目的如下：

- 第一个里程碑的目标为删除敏感认证数据并限制不必要位置和非业务必须的持卡人数据的存储；
- 第二个里程碑的目标为保护边界、内部和无线网络；
- 第三个里程碑的目标为安全的支付卡应用；
- 第四个里程碑的目标为监控和控制系统的访问；
- 第五个里程碑的目标为保护存储的持卡人数据；
- 第六个里程碑的目标为完成所有的剩余合规工作，并确保所有的控制措施到位。

从数据安全的角度，对于敏感数据和持卡人数据，机构应该做到有效的管理，存储的位置越少越好，这样它带来的风险就会越低，实现合规的整体难度也会越小。

首先针对收单机构而言，敏感的认证数据在授权完成后，是必须要安全删除的。敏感的认证数据包括完整的磁条信息、CVC2/CVV/CID/CAV2，PIN 或者 PIN block。对于发卡机构，敏感的认证数据是可以存储的，然而必须进行保护，比如强加密机制和密钥管理技术的引入是一个非常有效和常见的做法。

持卡人数据是指信用卡持卡人主账号（PAN）、持卡人姓名、有效期、服务码。对于持卡人数据，如果没有必要存储的位置尽量不要进行存储，必要时可以考虑进行截断（仅仅存储保留卡号的前六位和后四位）、基于强加密算法的单向哈希或令牌化技术（Tokenization）（使用令牌的方式可以参考 PCI 关于令牌解决方案的指导 Tokenization_Guidelines_Info_Supplement）。对于必须存储的持卡人数据，较为普遍和常见的做法是进行强加密，并针对密钥进行严格的密钥管理。

PCI DSS 认可的强加密算法总体来讲和 NIST 所颁发的密码领域最为权威的标准 FIPS 140 相一致。目前强加密算法包括但不限于（该密钥强度和认可算法会根据业界积累不断更新）：

对称算法：

- AES 128 bit 以上（建议使用 256bit）
- TDES 128 bit （建议使用 256bit 3 key）

☐ AKIPJACK / ESS 128 bit（建议使用 256bit）

非对称算法：

☐ RSA 1024 bit （建议使用 2048bit 以上）

☐ DSA 1024 bit （建议使用 2048bit 以上）

如果采用强加密算法对持卡人数据进行保护，机构需要首先考虑密钥管理体系的构建，以下是密钥管理体系建设的思路：

☐ 使用几个密钥来构建密钥管理体系？

☐ 使用对称算法还是非对称算法以及加密密钥的长度？

☐ 密钥的存储保护（防止密钥非授权访问和更改）

☐ 密钥的安全分发（确保密钥在传输过程当中的安全）

☐ 密钥泄露或者弱化的操作流程

☐ 密钥到期后的变更流程

目前国内大部分银行对于存储在它们系统里的持卡人数据大都没有进行加密处理，导致这种现状的原因可能是因为业务的需要，早期系统对于数据加密支持程度不高，或者是外部开发商在前期系统设计之初并没有对安全方面有太多的考虑。在这种现状之下，如果客户从业务连续性角度和生产运行工作的效率来考虑，可能比较避讳使用加密的方式进行持卡人数据的保护，又或者使用加密的方式来实现对持卡人数据的加密保护的难度非常大，这时候补偿控制性措施是一个备选的解决方案。机构可以和 PCI QSA 一起探讨并开发补偿控制性措施。对于存储的持卡人数据的补偿控制性措施可以考虑同时满足如下条件：(1) 内部网络分割；(2) IP 地址或者 MAC 地址的过滤；(3) 来自内部网络的双因素认证。

此外，根据笔者项目的经验，期待在如下层面较为关注，也可能是一些实际实施整改阶段的难点：

☐ 重要的功能要做到单一功能单一服务器；

☐ 对数据的存取实施强加密，或者采取补偿控制措施（参见上述说明）

☐ 敏感数据存储（收单业务在授权完成之后不能进行敏感数据的存储；发卡业务可以存储，但要进行强加密保护）

☐ 公用网络的数据加密（如果存在公共开放网络的话，比如互联网、GPRS、无线）

☐ 安全测试环节，比如 OWASP TOP 10 的参考

☐ 重大补丁及时安装（建议先测试后安装，可以考虑引入风险管理理念）

☐ 密码复杂度要求

☐ 日志记录信息的全面性和存储的要求

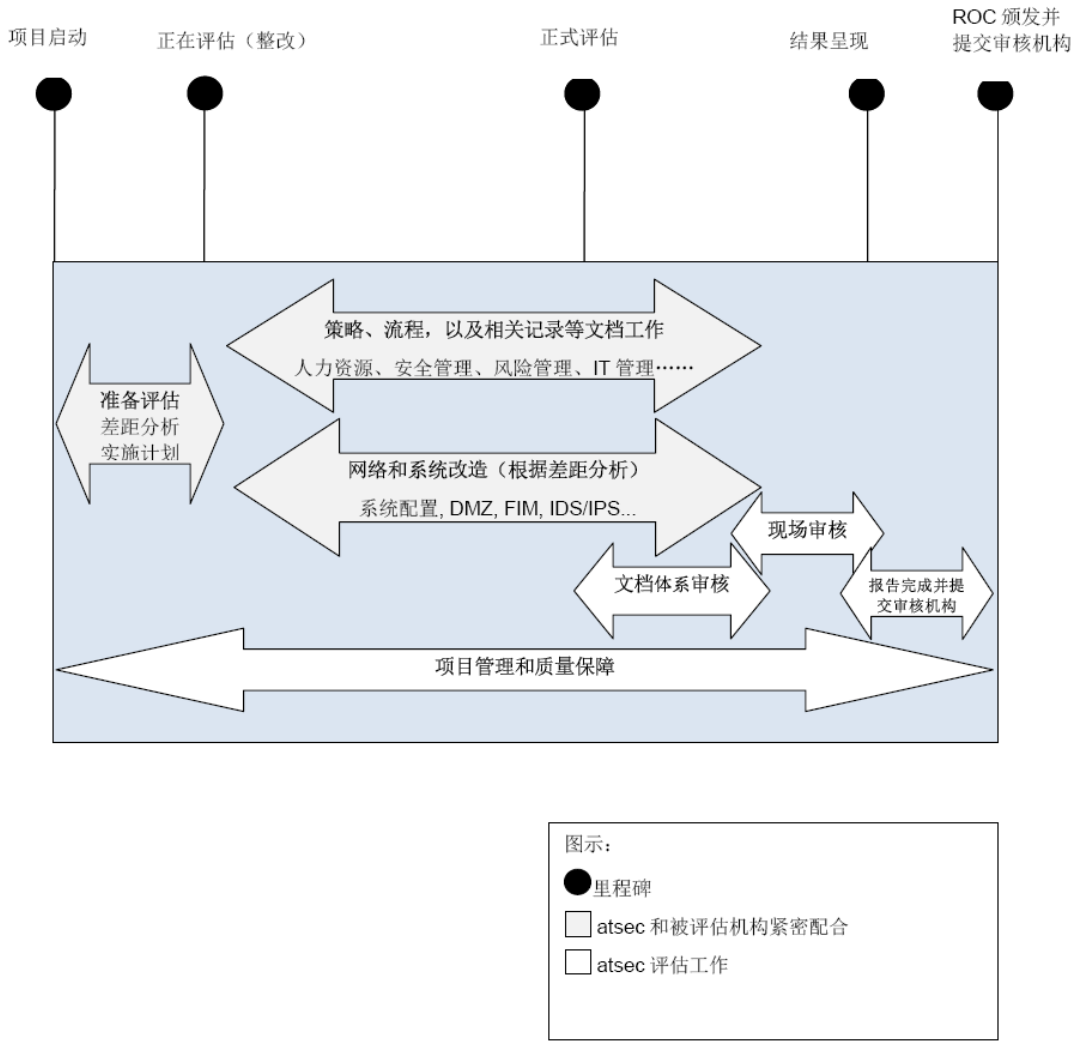
☐ 入侵检测和文件完整性监控的部署

☐ 机房环境的物理安全

☐ 信息安全管理体系（策略和流程等），特别是权限分配等相关环节

合规评估流程

如下图所示，PCI DSS 整体项目大体可以分为三个阶段。第一个阶段是准备评估阶段，atsec 开发了完整先进的准备评估的方法论，可以协助机构进行明确持卡人数据环境范围，并共同识别差距，提出详细的整改建议和解决方案。第二个阶段是基于差距的整改阶段，这个阶段的周期通常根据机构现状差距和整改的工作量等因素有所不同。第三个阶段是正式评估阶段，具有资质的评估人员 QSA 将开展全面的合规评估，之后出具合规报告和合规证明。



图：整体项目参考示意

支付产业的参与和发展

PCI DSS 的标准制定和更新过程中，不仅包含标准委员会的成员，而且众多支付产业链的相关机构如协会、POS 厂商、服务提供商、商户、金融机构、处理机构或者其他组织也都参与其中，目前致力到 PCI 工作中的机构和组织有 600 余家，详情请浏览：
https://www.pcisecuritystandards.org/get_involved/member_list.php。

目前来讲，诸多全球的大型金融机构已经加入了 PCI SSC 的参与机构，包括但不限于：Austrialia and New Zealand Banking Group Limited、Bank of America、BMO、BNZ、Bank of the West、Deutsche Card Services、First National Bank、HSBC、Merrick Bank、Royal Bank of Scotland、Scotiabank、Swedban Card Services AB、TD Bank、US Bank、USAA 等。

而参与组织提供的意见和建议对于 PCI 无疑是非常重要且具有价值的。笔者鼓励更多的中国机构，特别是收单机构和发卡机构共同参与到 PCI 的工作中。参与机构可以针对标准本身提出反馈意见，也可以更好的展示自己致力于 PCI 安全工作的贡献。

PCI 委员会将针对参与组织给予以下特权：

- ☐ 在 PCI 安全标准委员会顾问团为参与组织代表投票。
- ☐ 提名选入 PCI 安全标准委员会顾问团的候选人代表。
- ☐ 对 DSS 规范的所有修订版的草案和新规范（公开发布之前）发表意见。
- ☐ 参加 PCI 安全标准委员会主办的一年一度的标准团体会议。
- ☐ 为 PCI 安全标准委员会需要考虑的事项建议新方法。

怎样选择合适的合规评估机构

上述内容简单介绍了 PCI DSS 合规评估中的经验分享，以及合规建设和评估项目的一般流程，然而在实际执行 PCI DSS 合规工作的时候，应该如何选择合适的 PCI 合规评估机构 QSA 或者评估人员提供协助并执行安全合规工作呢？以下的参考因素能够为机构在合规过程当中可能会面临的安全风险提供很好的安全保障。

- ☐ 专业性，QSA 公司和团队人员资质，以及相关金融行业经验，作为行业领导者，提供标准和相关领域的协助和支持；
- ☐ 专注性，信息安全评估是否是该公司的主营的业务，且专注在该业务领域；
- ☐ 独立性， QSA 公司是否独立于厂商，可以提供不带有任何偏见的实施整改建议和解决方案；
- ☐ 诚信；
- ☐ 该公司自身是否切实建立并执行质量管理和安全管理体系，具有优化的策略流程；
- ☐ 该评估机构是否能够提供除安全评估以外其他能够提高客户流程等有价值的服务；
- ☐ 该评估机构是否能够在很多不同的技术领域提供专业知识和经验；
- ☐ 该评估机构是否为客户提供足够的保险和合理的法律协议保障。

结束语

信息安全和风险管理工作应做到事前的防御，而不是事后去弥补。合规的安全评估机构以及风险监管机构是各个金融机构的朋友和战略伙伴，虽然从安全的角度会提出这样或者那样的难题，引入机构整改的工作量和成本，但是我们的目标是共同抵御黑客的入侵，共同避免安全事件的发生。

安全工作重在实施的过程和控制，而合规的状态仅仅是水到渠成的保障结果。我们期待着与更多的参与和合作，使得整个产业能够以构建“安全和风险”为根基，而不是仅仅去应对“合规要求和审计”。期待着通过微薄之力为中国的整体支付安全做出我们的贡献。

参考文档和链接

[1] PCI SSC: https://www.pcisecuritystandards.org/

[2] VISA AIS: http://www.visa-asia.com/ap/sea/merchants/riskmgmt/ais.shtml