atsec NEWS 03/2011
the information security provider

atsec 是一座桥梁。

在这个信息技术迅速发展成熟的时代，信息安全越来越得到关注和重视。atsec 作为全球化发展公司，为客户提供广泛的信息安全服务，不仅吸取领先的技术和先进的思想帮助中国的客户和合作伙伴了解国际的信息安全动态，并尽可能打开国外的市场，同时也协助国外的机构了解中国信息安全领域的相关法律、法规和标准，并达到一定程度的合规要求。

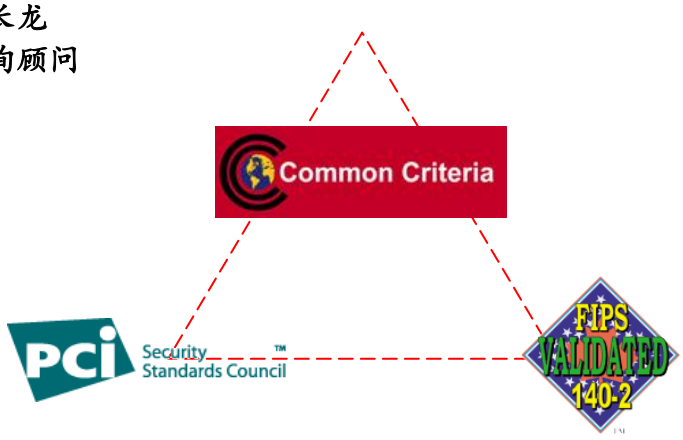
atsec 全球化的客户更加受益于 atsec 高瞻远瞩的战略，atsec 是全球 CC（Common Criteria）领域的领导者，并随后不断关注相关标准的合规评估和验证，比如支付卡产业（PCI：Payment Card Industry）标准、FIPS 140。atsec 近日也很自豪的宣布获得了美国 NIST 授权的生物识别技术（Biometrics）测评实验室资质，且目前正在致力于 EMV 测评资质的获得。atsec 并没有停止于已有的成绩，继续致力于全球新技术新标准的研究工作，投入到相关标准的开发和编写，并专注地在信息安全领域开展更为广泛的中立合规测评评估工作。

客户为什么会选择并且信赖 atsec?因为我们一直走在信息安全技术领域的前沿，不仅仅帮助客户完成某个项目，而是把好的想法和广泛的知识给予分享和传达，以期共同推动国内外信息安全的发展和进步。我们还通过自我学习，内部培训和交流探讨来促进自我提高和发展，高质量、高效率的完成每个项目是我们受到业界客户高度评价的基础。

近日，atsec 中国获得由中国信息安全认证中心（ISCCC：China Information Security Certification Center）颁发的 ISO/IEC 27001 认证证书，并且获得首家经 CNAS（China National Accreditation Service for Conformity Assessment）认可的外资、独立的商业 IT 安全实验室的资质。资质的获得是有挑战性的，但我们勇于接受挑战，在长达数月的资质认可评估过程中，我们积极配合、不懈努力，凭借资深的专业技术经验最终赢得了挑战的胜利。

资质的获得代表着 atsec 的服务更加值得信任，同时也代表着 atsec 中国实验室整体能力在不断提升。我们将为国内外搭建 IT 信息安全坚实的桥梁而不懈的努力！

王长龙
咨询顾问



最近新闻一览

IBM(R) z/OS(R)版本1 R. 11系统SSL密码模块获得FIPS 140-2 证书

atsec信息安全满足了NVLAP生物识别测试体系下的认可要求，获得测评资质

atsec出席2011年RSA大会

atsec中国获得由中国信息安全认证中心颁发的ISO/IEC 27001认证证书

atsec中国成为首家经CNAS认可的外资、独立的商业IT安全实验室

atsec为中国IT安全专家提供FIPS和PCI培训

Enterprise Key Management解决方案通过了atsec测评并获得FIPS 140证书

atsec自身获得了ISO 9001质量管理体系认证证书

更多的新闻，请浏览我们的网站
www.atsec.com

PCI DSS 数据安全标准 V2.0 变更分析

atsec 高级咨询顾问 高向东(xiangdong@atsec.com)

PCI 安全标准委员会（PCI SSC）最近发布了关于 PCI-DSS 和 PCI PA-DSS 的更新版本 V2.0。该版本的发布，经过了近两年从客户和厂商收集，并将审议的结果体现于新版本中。值得注意的是，V2.0 并未引入新的重大要求。下载地址如下：
https://www.pcisecuritystandards.org/security_standards/updates.php

新标准产生的影响

对于 PCI-DSS 的变更，整体上趋向于更合理、更严格，同时也更多地引用和借鉴了业界的标准和实践。在原版本的 PCI PA-DSS 中，频繁地引用至 PCI DSS，使得客户和评估人员在完成 PCI PA-DSS 审核时要同时打开两个标准。由此，在 PA-DSS 的新版本中投入了大量工作以消除 PCI-DSS 和 PA-DSS 这两个标准间的信息冗余。

新标准的转换日期

对于 PCI DSS 和 PA-DSS 这两个标准的转换日期是一致的，如下表所示：

日　期	所应用的标准
2010 年 12 月 31 日前	V1.2.1 版本用于评估。在 2010 年不可使用 V2.0 版本。
在 2011 年	可使用 V1.2.1 或 V2.0 用于评估。V2.0 于 2011 年 1 月 1 日正式生效。
在 2012 年	评估中必须使用 V2.0。
2012 年 7 月 1 日	自该日起，PCI-DSS 要求 6.2、6.5.6 和 11.1 变为正式要求。在之前，这三个条款为最佳实践。

对于当前正基于 V1.2.1 版本进行评估的用户，意味着还有大约 11 个月的时间完成评估。客户也可选择在 2011 年使用 V2.0 展开评估。总之，在 2011 年，客户可基于新版本或旧版本展开评估，但在 2012 和 2013 年，所有评估必须使用 V2.0 版本。

atsec 在此建议需要通过 PCI-DSS 标准的组织尽早展开新版本的转换工作，以减少合规建设过程中对信息系统的影响。对于正在开展 PCI-DSS 合规的组织，推荐使用新版本进行 PCI 合规。

PCI DSS 的变更

注：本章内容所描述的“原版本”指的是 PCI-DSS 的 V1.2.1 版本，“新版本”指的是 PCI-DSS 的 V2.0 版本。

➢ 引用概念的变化

为更灵活地适应各种组织形式、组织规模以及组织的架构，新版本通过相应的概念变化使得组织在合规过程中的范围更清晰、要求更明确。

变化的方面	概念的变化	备　注
合规所涉及对象的变化	评估对象由旧版本的 company 变更为新版本的 entity。	这使得标准所适用的组织范围更广。
合规所涉及人员的变化	组织所涉及的人员由 employee 变更为 personnel。	该变化将组织的外部和相关人员均纳入到 PCI-DSS 的要求之中，通用性更强。
授权管理人员的变化	对管理过程的授权人员由 management 变更为 authorized party。	这使得授权和批准过程的管理更适用。

除此之外，新版本对 PCI DSS 所涉及的”介质 media”、“现场人员 onsite personnel”、“访客 visitor”等均给出了更明确的定义。

➢ 部分要求的合理化

在原版本的技术要求中，有些要求的通用性不高，使得组织在合规过程中的可选措施较少。新版本更多地关注于技术措施的有效性，在某些点不再局限于具体的某一种技术，使得组织在合规建设中的可选措施的范围更广一些。新版本主要对地址隐藏、帐号安全性要求、公共网络上的信息传输等方面提出了更为合理的技术要求，并在服务器的功能分布方面进行了合理化。

➢ 对组织的要求更严格

新版本在漏洞管理流程、系统配置标准的应用、主密钥的替换条件以及无线网络的识别等过程提出了更高要求。重大的变更包括：

1.持卡人数据环境的网络层保护要求更严格；

2.安全配置标准的应用范围更广，更求更严格；

3.持卡人数据存储和销毁体系的要求更明确，且需要定期检查；

4.对密钥管理过程的保护措施和密钥替换的要求更严格；

5.明确提出对组织进行统一的漏洞管理的要求；

6.另外，对时间一致性的保护、无线访问点的检查范围以及文件完整性的监控措施均提出了更高要求。

➢ 对审核过程的要求

作为QSA审核阶段最重要的工作，新版本对QSA审核范围和抽样的确定提出了更明确的要求。

更多的审核要求

在原版本的某些要求中，存在对测试规程的多个描述，具体所要求的条目不够清晰。在新版本中，将这些规程分隔分解为独立的要求，使得要求更明确。比如将原版本中1.1.3要求验证配置标准包括防火墙以及确认所提供的拓扑结构是最新，新版本则分解为两个流程1.1.3.a和1.1.3.b。

审核范围的确定过程

在范围的确定过程中，新版本进一步明确主帐号（PAN）是PCI DSS是否适用的定义性因素。新版本明确要求通过首先识别持卡人数据的位置和流向，进而确定支撑业务的IT系统，由QSA最终确定持卡人数据环境的范围。

抽样过程的论证

对于抽样过程，增加了对抽样论证的要求，要求QSA采用抽样方法论，并在合规性报告（ROC）中论证抽样方法的合理性和充分性。

代码发布过程的审核

在审核过程中，要求QSA抽取最近的应用变更，并依据标准所提及的安全编码、编码检查、变更审批、影响分析、回退方案以及实施验证等过程进行验证。

PCI-DSS 合规建议

如前所述的主要变化可以看出，新版本除了对合理性和可用性进行了完善，也在相当大地程度上提高了标准的具体要求。这就需要合规的组织需要作出更多地努力，以达到PCI DSS标准的合规。以下是几点建议，希望对组织在PCI DSS的合规工作中有所帮助。

➢ 安全实践与业务系统的有效融合

组织无论是在应对各种安全风险，还是在各种合规过程中，都涉及具体的安全措施。从新标准对大量业界实践的引入以及更侧重于全过程安全控制的变化来看，积累更多地实践并不遗余力地将其应用到业务过程中是一个行之有效的积累和建设过程。我们也能看到，经过充分融合的安全过程，其在合规过程中所带来的痛点也会小得多。

➢ 充分借助和利用现有体系和措施

组织在信息安全的建设中，会有一些在体系建设方面和安全措施方面。在体系建设过程中，组织可最大化地重用已有的成熟的体系建设成果和安全措施，如ISMS管理体系中的人力资源管理要求就可以较全面地满足PCI DSS在人力资源方面的要求，这在实践中证明是投入最小的办法。

➢ 持续合规与改进

PCI DSS的合规并不是一劳永逸的工作，需要每年进行审核，同时ASV、风险评估、渗透测试等等各种工作也要定期开展。不建议为获得PCI DSS的资质而花费大量资源通过认证，认证过后放松安全要求的做法。组织虽然通过了PCI DSS，但在不合规状态下出现安全事故，其后果与未进行PCI DSS合规的后果是一样的。由此看来，PCI DSS的合规是需要持续合规与改进。建议组织在通过PCI DSS后，更多地关注于PCI DSS要求与现有业务运行体系的有效融合，并通过持续改进的方法使组织一直处于合规状态。

多年以来，atsec 对PCI DSS标准持续关注，积累了大量的最佳实践和合规建议，并形成了一整套完整的方法论，在此也希望为涉及PCI DSS合规的服务供应商、商户和收单机构的合规性建设提供相应的支持和帮助！

*全文可在以下链接查看：
http://www.atsec.com/cn/publications-white-papers.html。

引入 SCAP 标准提高系统配置安全

atsec 资深顾问 张力(li.zhang@atsec.com)

随着计算机通信技术的飞速发展，由系统配置而导致的安全问题越来越多，安全内容自动化协议（SCAP）为系统配置的标准化以及对系统配置的脆弱性评估提供了一种统一的方法。越来越多的厂商、组织与社团已加入到 SCAP 的研究与发展中，也推动 SCAP 成为真正意义的全球标准。

SCAP 的产生背景：

由于计算机通信技术的飞速发展，美国联邦政府强烈的意识到由于计算机系统配置问题而暴漏出越来越多的安全漏洞，为此，2007 年美国联邦预算管理办公室（OMB：Office of Management and Budget）提出要求所有的政府部门开始试行联邦桌面核心配置计划（FDCC：Federal Desktop Core Configuration）。2008 年则开始强制执行。FDCC 最初是由美国国家标准与技术研究所联合 OMB、DHS（Department of Homeland Security）、NSA（National Security Agency）以及 Microsoft 共同开发，用于美国空军 Windows XP 的公共安全配置，2008 年 6 月发布第一个版本 FDCC1.0，在本文发稿前最新的版本为 2009 年 8 月发布的 1.2 版本。

SCAP 提供了一种自动、标准化的方法来维护企业系统的安全，如实现安全配置基线，验证当前的补丁程序，进行系统安全配置设置的持续性监测，检查系统的折衷标记（sign of compromise），以及能在任意设定时刻给出系统的安全状态。SCAP 的提出主要源于如下几个方面的原因：

- 大量的以及多样的系统需要保护。
- 快速响应新的威胁。
- 缺乏互操作性。

SCAP 协议框架：

SCAP 包含两个主要元素。首先，它是一个协议，一组标准化格式与术语的开放规范，通过它软件安全产品可以互通软件缺陷与安全配置信息，每一个规范也被称作一个 SCAP 组件；其次，SCAP 包括软件缺陷与安全配置标准化的参考数据，也被称作 SCAP 内容。

关于SCAP content，存在多个资源，例如，NVD拥有CPE与CVE标识项，MITRE公司拥有OVAL数据库，并且维护CCE标识项的列表。每一个SCAP组件提供唯一的功能，可以被独立地运用，但是联合的运用能带来更大的好处，例如，用XCCDF格式依据CPE表达CCE的能力形成了用于SCAP表达检查列表的基本元素，换句话说，SCAP表达的检查列表用一种标准化的语言（XCCDF）来表达所讨论的平台是什么（CPE），访问什么安全设置（CCE）。运用SCAP表达检查列表可以很容易的帮助组织实现对系统的安全控制，进行安全监测，自动化高级安全需求的合规性报告。

总之检查列表用SCCDF来描述评估什么，用OVAL在目标系统做相应的测试，用CPE标识检查列表是有效的以及运行测试的平台，用CCE标识在检查列表中被访问或被评估的安全配置设置，用CVE参考已知的脆弱性，CVSS用于分级这些脆弱性。

标准的评估认证:

NIST 已经建立了 SCAP 产品认证体系与 SCAP 实验室委任体系，这些体系一起确保 SCAP 产品的测试与验证过程。SCAP 测评实验室需要经过美国国家实验室自愿认可计划（NVLAP）的授权。实验室一经授权，实验室就可以根据 NISTIR （National Institute of Standards and Technology Interagency Report）7511 中的 DTR (Derived Test Requirements)的描述进行 SCAP 产品测试。产品经测试后，测评实验室将发布测试报告（包括特定产品的需求列表，被需要的开发商文档，由实验室做的详细的测试总结）给 SCAP 产品认证体系，产品认证体系专家将审阅测试报告，然后发布产品认证。

SCAP 展望:

截至此文章发稿前，已有 30 个厂商获得了扫描与审计产品的 SCAP 认证，正式通过 SCAP 认证的厂商可以参考链接：http://nvd.nist.gov/scapproducts.cfm。我们不难发现越来越多的厂商，组织与社团加入到 SCAP 的研究与发展中，它已经成为业界事实上的标准，目前正式发布的版本为 SCAP 1.0（包括 XCCDF 1.1.4，OVAL 5.3 与 5.4，CPE 2.2，CCE 5，CVE 与 CVSS 2.0），SCAP1.1 目前处于修订中，并且 SCAP 已经正式提交 IETF 讨论组，相信不久的将来即会成为正式的全球标准。（*全文可在以下链接查看：http://www.atsec.com/cn/publications-white-papers.html）

联系我们

艾特赛克（北京）信息技术有限公司
北京市海淀区上地七街1号2号楼119室
100085
电话：84834011
传真：82890017
Email:info_cn@atsec.com