全球支付卡产业安全动态分享

刘岩 （yan@atsec.com），atsec中国

CISSP, CC Evaluator, ISO/IEC 27001 LA, O-TTPS, NASPO Auditor, PCI QSA, PA DSS QSA, PCI PFI, ASV, CNAS Auditor

内容概述

- 数据泄露与事后取证
- 支付卡产业标准及其相关指导的发展动态
- PCI安全标准委员会和国际监管机构体系
- atsec合规方法论分享

数据泄漏与事后取证

数据泄露与事后取证

- 持续增长的安全风险，2009年以来每年度66%数字的增长，近期年度发生了43 Million起安全事件。
- 事后取证调研PFI（PCI Forensic Investigation）。

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) continues to improve, but four out of five companies still fail at interim assessment. This indicates that they've failed to sustain the security controls they put in place.

- 应急响应
  - 制定7*24应急响应流程，明确角色和职责
  - 应急演练
  - 通知监管机构
- 取证准备
  - 收集证据
  - 计划安排
- 证据分析
  - 分析内容包括日志、文件、配置、内存空间、硬盘
  - 也包括流程和人员层面
- 取证结论
- 跟进和改进

PFI 调查取证机构列表

Find a PCI Forensic Investigator Company

Search by Company Name

SUBMIT

Filter by: PLACE OF B... SERVICING... LANGUAGE EXPORT LIST

Page: 1 2

Results: **19**

COMPANY	PLACE OF BUSINESS	PRIMARY CONTACT	SERVICING MARKETS	SUPPORTED LANGUAGES
atsec (Beijing) Information Technology Co., Ltd	China, Germany, Sweden, USA	Yan Liu Yan@atsec.com +86-10-82893001	China	Chinese, English

资料来源：https://www.pcisecuritystandards.org/assessors_and_solutions/pci_forensic_investigators

PFI报告样例

PFI Preliminary Incident R

Appendix A: PCI DSS Overv

To assist in in identifying where compromised enti

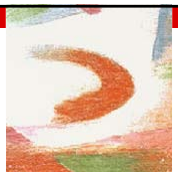
directly to PCI SSC via the portal. When completing this section do not include any information that identifies the potentially compromised entity.

PCI DSS Requirement	Was Requirement Fully Assessed?	In Place	Cause of breach?	Contribute to breach?	Findings/Comments (must be completed for all Requirements)
Build and Maintain a Secure Network					
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☒ No ☐ Not Assessed	☐ Yes ☐ No ☒ Unknown	☐ Yes ☐ No ☒ Unknown	No firewall device was deployed in current network environment, and need install a firewall and provide the security configuration to protect the network of cardholder data environment.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☒ No ☐ Not Assessed	☐ Yes ☒ No ☐ Unknown	☐ Yes ☒ No ☐ Unknown	It's suggested to set system passwords according to the requirement 8.5 of PCI DSS, and perform security hardening for all of servers according to PCI DSS requirement 2.
Protect Cardholder Data					
Requirement 3: Protect stored cardholder data	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☐ No ☒ Not Assessed	☐ Yes ☒ No ☐ Unknown	☐ Yes ☒ No ☐ Unknown	No any cardholder data was stored.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	☐ Yes ☒ No	☐ Yes ☐ Partial Yes ☐ No ☒ Not Assessed	☐ Yes ☐ No ☒ Unknown	☐ Yes ☐ No ☒ Unknown	Currently, the encryption transmission was implemented in the "shopping cart" part of whole website. Further QSA assessment would be needed and suggested.

A.1 PCI DSS Summary

Type of business entity	☒ Merchant (brick and mortar, e-commerce, or both)	☐ Acquirer processor	☐ Encryption Support Organization (ESO)
	☐ Prepaid issuer	☐ Issuer processor	☐ Payment application vendor
	☐ Issuer	☐ ATM processor	☐ Payment application reseller
	☐ Acquirer	☐ Third-party service provider (webhosting, co-location)	
	☐ Other (describe):		
Summary statement for findings, including factors that caused or contributed to the breach. (For example, memory-scraping malware, remote access, SQL injection, etc.)	Because almost all of the logs of system components requested by PCI DSS are missing, no clear evidences show a data breach happened, and no evidence shows that the sensitive data (including full track, CAV2, CVV2, CVC2, PINs) and the cardholder data were impacted during the completed investigation. Plenty of high risk vulnerabilities (XSS, HPP) and medium vulnerabilities (CSRF) were found in the website www.banggood.com. XSS vulnerability allows an attacker to send malicious code to another user, because a browser cannot know if the script should be trusted or not, and it could execute the script in the user context allowing the attacker to access any cookies or session tokens retained by the browser. HPP attacks consist of injecting encoded query string delimiters into other existing parameters, it makes that a malicious		

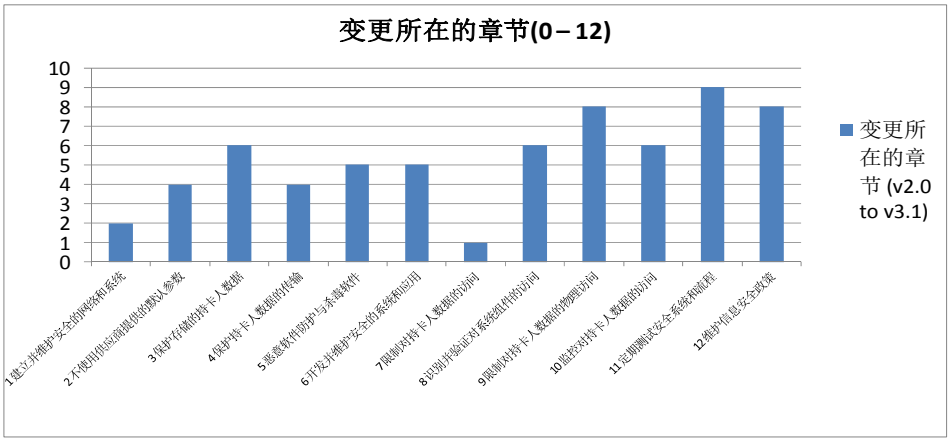
支付卡产业标准
及其相关指导的发展动态



面临风险持续增加的合规要求

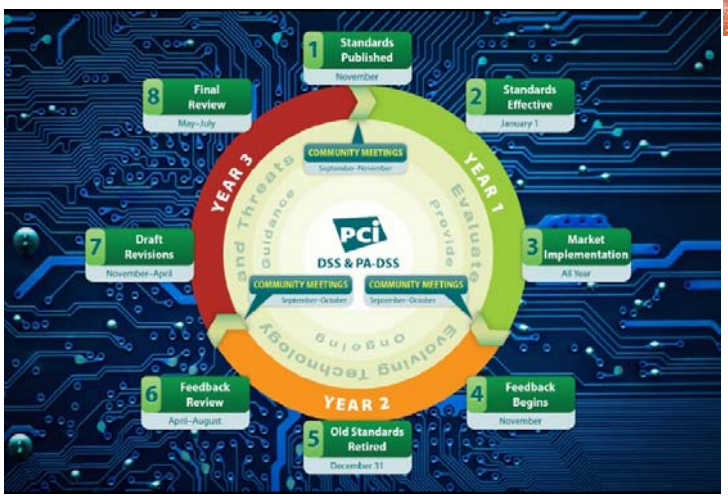
- 标准要求的数量增加且更复杂
- 评估质量和技术能力的增强
- 合规报告的标准化和质量提升

PCI产业标准的条目增加情况



Source from Verizon report

PCI标准传统的生命周期

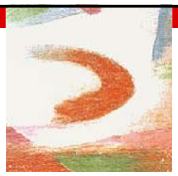


Source from PCI SSC

PCI DSS v3.2新版本即将发布

- PCI DSS v3.2版本预计2016年上半年发布。
- PCI SSC CTO Troy Leach反馈：
  - 调整针对SSL和早期版本TLS的最迟整改日期至2018年。
  - 标准成熟度，目前并不要求重大的变更和调整。
  - 敏感和谨慎地处理对于最新支付技术和形式的发展和重大变化，包括移动支付、EMV以及其他动态数据和认证的形式。

PCI DSS v3.2整合最佳实践

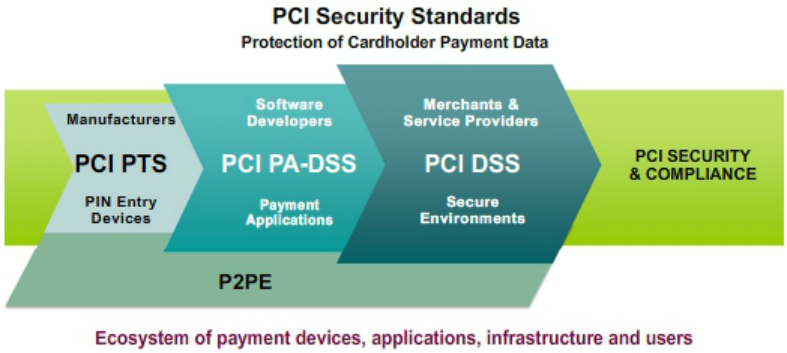


- 整合了产业的反馈，并紧密跟踪最新的威胁趋势，特别结合了来自支付产业数据泄露取证报告中涉及的事件发生原因的宏观统计。
- 更新要求：
  - 对持卡人数据环境运维中多因素认证的额外要求
  - 澄清了主帐号显示时的掩码规则
  - 集成了指定机构的补充验证（DESV）要求。
- 允许过渡周期，但建议尽快引入最佳实践。
- PA-DSS等其他标准和支持文档同步更新。

SSL和早期版本的TLS，您整改了吗？

- SSL和TLS v1.0长期使用历史
  需要立即停止使用这些协议进行传输保护，并立即进行整改。
- 风险！风险！风险！
  - 2014年年底被发现，参见CVE-2014-3566
  - POODLE (Padding Oracle On Downgraded Legacy Encryption)
  - 造成中间人攻击，使得传输不再可信
- 整改目标：TLS v1.2
- PCI DSS相关条目：
  - 2.2.3：针对不安全的服务、协议和/或进程实现安全特性
  - 2.3：采用强加密加密所有非控制台的管理访问
  - 4.1：公共开放网络传输需要采用强加密
- ASV是最有效的方式发现漏洞

PCI SSC管理PCI合规的统一标准



***2013年6月**
Card Production Logical and Physical Security Requirements
面向卡厂的逻辑和物理安全要求

***2014年12月**
PIN Security requirements v2.0
PIN Security requirements and test procedures

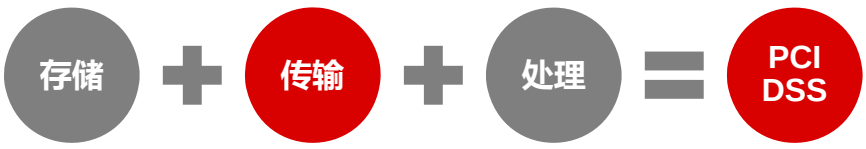
PCI DSS作为产业成熟的最佳实践

支付卡产业数据安全标准是一个被开发支持和提高持卡人数据安全和卡组织采用的全球化一致性的数据安全措施。

提供了一套保护持卡人数据的技术和操作的基线要求。

谁需要执行QSA评估

- 对大多数商户，该要求来自于上一级的银行或收单行。如果业务与多个卡品牌（包括万事达、VISA、JCB、美国运通和Discover ）相关，有较大可能需要满足要求。
- 机构自身出于信息安全考虑，执行标准的合规建设工作。



银行、支付公司……
超市、呼叫中心、航空公司、电子商城……

atsec PCI合规思路简介

建立和维护安全的网络

保护持卡人数据

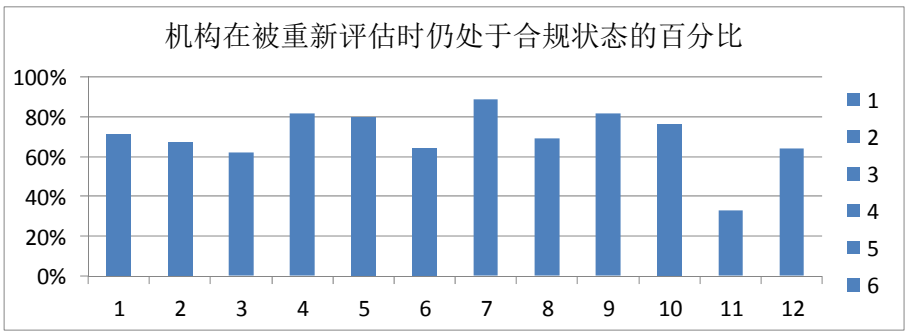
维护漏洞管理程序

实施访问控制措施

定期监控和测试网络

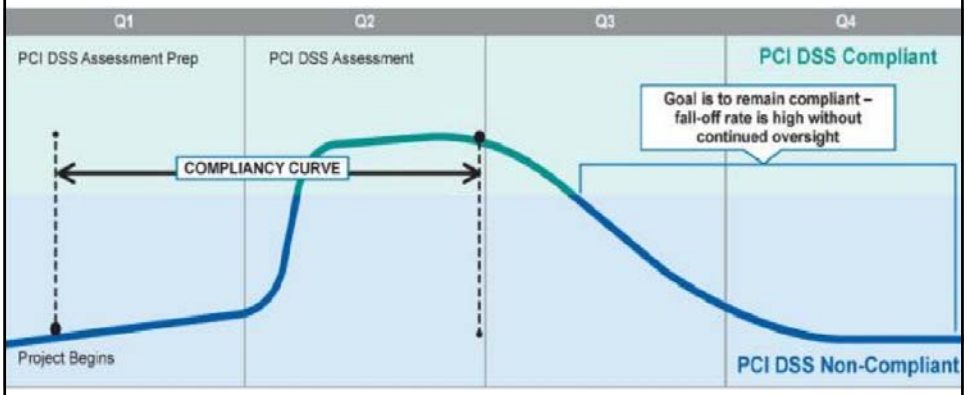
维护信息安全策略

合规比率情况



Source from Verizon report

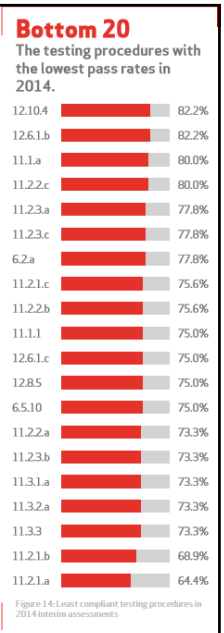
合规曲线 – 鼓励持续长期有效合规



Source from PCI SSC

合规难度持续增加

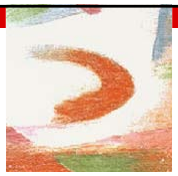
- **TOP1**：安全事件发生时进行应急相应的相关职责需要定期的培训；入职和定期的安全意识等培训。
- **TOP2**：无线接入点的巡检或者无线入侵检测。
- **TOP3**：ASV扫描，内部扫描。
- **TOP4**：补丁更新（本条要求产业已经降低了难度，根据机构自身的风险评估制定补丁的整改计划）。
- **TOP5**：渗透测试



支付应用PA：软件设计缺陷

- 差的敏感数据实践
- 没有将安全性要求纳入到最初的设计（Security through obscurity）
- 不安全的会话管理
- 日志和审计缺失
- 差的密码实现
- 依赖于硬编码的密码和密钥
- 不合适的访问控制措施
- 不经意的数据泄露

支付应用PA：不安全的配置和操作



- 默认账号的使用
- 默认/弱的密码或密钥的使用
- 差的远程访问配置
- 失败配置安全数据传输
- 失败配置安全更新功能
- 共享账号的使用
- 不合适或者不严格的安全设置
- 失败禁用没必要的特性
- 失败禁用不必要的端口和协议

PA QSA列表：
https://www.pcisecuritystandards.org/assessors_and_solutions/payment_application_assessors

PCI Security Standards Council

PAYMENT APPLICATION QUALIFIED SECURITY ASSESSOR

COMPANY | VALIDATION | DEPLOYMENT | REVALIDATION | EXPIRY | VALIDATED BY

Find a Payment Application Qualified Security Assessor Company

atsec (Beijing) Information Technology Co., Ltd

SUBMIT

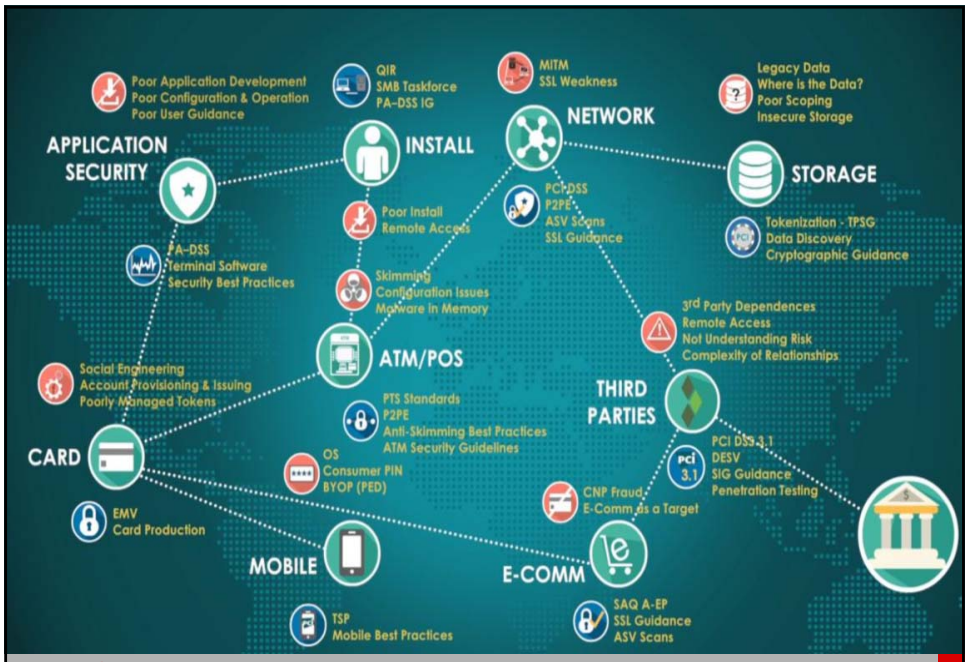
Filter by: PLACE OF B... | SERVICING... | LANGUAGE | EXPORT LIST

Page: 1

Results: 1

COMPANY	PLACE OF BUSINESS	PRIMARY CONTACT	SERVICING MARKETS	SUPPORTED LANGUAGES
atsec (Beijing) Information Technology Co., Ltd	China, Germany, Sweden, USA	Yan Liu yan@atsec.com	Asia Pacific	Chinese, English

customer of organization can use the mobile phone to transfer money, pay for goods and services, and distribute bulk payments such as salaries and welfare payments based on mobile technology (e.g. Unstructured Supplementary Service Data (USSD), SIM Application Toolkit (STK), mobile app, etc.). All the money changes on customer's CPS user account will be recorded into the CPS system and reflected on the organization's bank account. CPS system uses Electronic funds transfer (EFT) file to finalize the settlement with the bank in a pre-defined time period.



安全电子商务 – 防御措施

面对电子商务系统泄漏数据的风险

安全电子商务 – 发现与响应机制

- 渗透测试
- ASV和内部扫描
- 监控和日志
- 源代码审核
- 入侵检测
- 端口、用户和系统账号的定期审查
- 通知和响应流程
- 验证变更

电子商务欺诈的防护

防止其他位置偷取的数据进行电子商务欺诈

- 从其他非法渠道获得的卡号信息用于电子商务欺诈日趋增强
- 持卡人数据的认证是关键，可以考虑引入：
  - 由发卡机构和/或商户实现的身份认证；
  - 交易流程中引入额外的认证因素或者步骤
  - 3D安全
  - 依赖于认证机制的完整性
  - PCI DSS自评估SAQ

不同的第三方需要不同的控制，但是需要考虑…

- 该机构提供什么样的服务？
- 该第三方机构是否完成了PCI DSS合规？
- 是否访问被有效地限制？
- 是否需要贵机构参与到第三方的PCI合规中？

特别工作组SIG动态 – 当前正在工作中

- Effective Daily Log Monitoring
  有效的日志监控
- Managing Shared Responsibilities with Third Party Service Providers
  管理第三方服务供应商的共同责任

已经完成的SIG

虚拟化

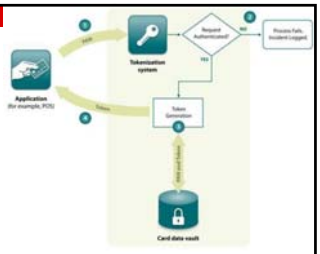
PCI DSS Virtualization Guidelines Jun 2011

移动

Mobile Payment Security Guidelines, Sep 2012

加密

Point-to-Point Encryption Technology and PCI DSS Compliance



P2PE standard (released in 2012) contains security requirements and testing procedures for application vendors and providers to ensure the data protection.

无线

PCI DSS 2.0 Wireless Guidelines Aug 2011

EMV

PCI DSS Applicability in an EMV Environment Oct 2010

令牌化

PCI DSS Tokenization Guidelines, Aug 2011

PCI长期谨慎关注移动支付的安全性

已经完成的SIG – 续

云
云计算指导
Feb 2013

电子商务指导
Jan, 2013

风险评估

PCI DSS风险评估指导
Nov 2012

- 第三方安全保障，Aug 2014
- PCI DSS V3.0维护PCI DSS合规的最佳实践，Aug 2014
- 渗透测试指导，Mar 2015
- 实现安全意识教育程序的最佳实践，Oct 2014

PCI安全标准委员会和国际监管机构体系

PCI SSC安全标准委员会

开放全球化的论坛

成立于2006

针对支付卡安全提供开放的标准指导

- 开发
- 管理
- 教育
- 意识

PCI安全标准委员会的职责

PCI Security Standards Council

PCI DSS, PCI PTS, PCI PA-DSS, P2PE, PIN Security and supporting documents

Roster of QSAs, ASVs, PA-QSAs, validated payment applications, PTS Devices, and P2PE solutions

PCI Security Standards Council FAQs

Education & Outreach Programs

Participating Organization Membership, Community Meetings, Feedback

PCI全球范

More than 72

ATMJ	Australia and New Zealand Banking Group Limited	Australian Postal Corporation	bnz
BBPOS Limited	中国银联 China UnionPay	Coles Group Limited	coomota
Cuscal Limited	Eastern Communications Co Ltd (Financial Division)	eway	ezidebit
F-REGI F-REGI Co.,Ltd	Feitian Technologies Co., Ltd	fjconsulting, INC.	LANDI
GMO PAYMENT GATEWAY	GROUNDLABS	HITACHI Inspire the Next Hitachi-Omron Terminal Solutions, Corp.	INTELLIGENT WAVE INC.
iNVENCO	Nautilus Hyosung	NEXUSGUARD	PAX Your Payment Partner of Choice
Premier Technologies Pty Ltd	QANTAS	Quest Payment Systems Pty Ltd	XED 新国都
SPECTRA Technologies Holdings Company Ltd	Strategic Payment Services	Sun Partners Co.,Ltd	SZZT 证通电子
IT'S HOW WE CONNECT	veritrans	XAC Automation Corporation	ZEUS Credit Payment Service

监管要求和各卡品牌安全体系

Security Program	URL
MasterCard Site Data Protection Program (SDP)	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html
Visa USA: Cardholder Information Security Program(CISP) Other Visa Regions: Account Information Security(AIS) Program	http://www.visa-asia.com/ap/sa/merchants/riskmgmt/ais_visanet.shtml#Requirements
American Express Data Security Operating Policy Compliance Program (DSOP)	https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=spinfo&ln=en&frm=US&tabbed=complienceRequirement
Discovery Discover Information Security & Compliance (DISC)	http://www.discovernetwork.com/merchants/data-security/disc.html
JCB	http://partner.jcbcard.com/security/jcbprogram/

VISA针对Service Provider的要求：

- http://www.visa.com/splisting/LearnMore.html
- **PCI DSS Validated Service Providers**
  - Service Providers that store, process or transmit cardholder data must be registered with Visa and demonstrate PCI DSS compliance. PCI DSS compliance validation is required every 12 months for all service providers. Inclusion on the registry indicates only that the service provider successfully validated PCI DSS compliance with an on-site assessment, based on the report of an independent Qualified Security Assessor (QSA), and has met all applicable Visa program requirements.
- **Annual Revalidation**
  - Service Providers that store, process or transmit Visa cardholder data must demonstrate PCI DSS compliance and provide the compliance validation to Visa every 12 months. The fine for non-compliance starts at 10,000 USD per service provider (assessed to the registering Visa member).
  - For service providers published on the Registry, if Visa does not receive the appropriate revalidation documents:
  - **Within 1 - 60 days** upon expiry of the validation documents, the service provider will be highlighted in Yellow on the Registry.
  - **Within 61 - 90 days** upon expiry of the validation documents, the service provider will be highlighted in Red on the Registry.
  - **After 91 days,** the service provider will be removed from the Registry.

来自国际卡组织VISA的要求

- http://www.visa.com/splisting/searchGrsp.do

COMPANY	SERVICE PROVIDER TYPE	VALIDATION TYPE	SERVICES	EXPAND ALL / COLLAPSE ALL	VALID THROUGH DATE	ASSESSOR	REGION OF OPERATION
Alipay CA, U.S.A.	AGENT	PCI DSS	PCI DSS Services		Jun 30, 2016	atsec (Beijing) Information	U.S., CAN
Alipay Hong Kong Limited HONG KONG, CHINA	AGENT	PCI DSS	PCI DSS Services		Jun 30, 2016	atsec (Beijing) Information	AP
Alipay.com.Co., Ltd CHINA	AGENT	PCI DSS	PCI DSS Services		Nov 30, 2016	atsec (Beijing) Information	AP
Century Heguang Technology Development (Beijing) Co.,Ltd. CHINA	AGENT	PCI DSS	PCI DSS Services		Oct 31, 2016	atsec (Beijing) Information	AP
China Unionpay Data Service Co., Ltd CHINA	ACS VENDOR	ACS	ACS Services		Dec 31, 2015	AGES	GLOBAL
	AGENT	PCI DSS	PCI DSS Services		Mar 31, 2016	atsec (Beijing) Information	AP
ePayLinks Technology Co., Ltd CHINA	AGENT	PCI DSS	PCI DSS Services		Dec 31, 2016	atsec (Beijing) Information	AP

Visa's Qualified Service Provider (QSP) Program

第三方支付公司认证

Launched in Aug
http://www.visa.c
ound.html

Facilitates co
more secure
China

Helps PSPs in C
grow their busi
and drive stro
performanc

1. 联款通电子科技（广州）有限公司 (ASIAPAY)
2. 深圳市钱宝科技服务有限公司 (GBPAY)
3. 迅付信息科技有限公司 (IPS)
4. 快钱支付清算信息有限公司 (99BILL)
5. 易智付科技（北京）有限公司 (PES)
6. 深圳市财付通科技有限公司 (TENPAY)
7. 深圳鼎付信息技术有限公司 (GPAY)
8. 深圳市富汇通信息网络有限公司 (FHT)
9. 世纪禾光科技发展（北京）有限公司 (DHGATE)
10. 上海乾汇信息科技有限公司 (MASAPAY)
11. 广州市易票联支付技术有限公司 **(EPL)
12. 上海银联电子支付服务有限公司 ** (CHINAPAY)
13. 重庆易极付科技有限公司 ** (YJF)
14. 深圳市财宝网络技术服务有限公司 ** (PFA)
15. 通联支付网络服务股份有限公司 ** (AIP)
16. 支付宝（中国）网络技术有限公司 (ALIPAY)
17. 启赟金融信息服务（上海）有限公司 **

tb

onal
to
ence

MasterCard

Alipay (Europe) Limited (Branded as "Alipay Europe")	Europe	06/03/2015	atsec (Beijing) Information Technology Co., L
Alipay.com Co., Ltd. (Alipay HangLv)	Asia Pacific	12/26/2015	atsec (Beijing) Information Technology Co., L
ChinaPay e-payment Service Co.,Ltd.	Asia Pacific	12/23/2015	atsec (Beijing) Information Technology Co., L
ePayLinks Limited (Branded as "ePayLinks")	Asia Pacific	12/25/2015	atsec (Beijing) Information Technology Co., L
Shenzhen FHTPay Information Network Co., Ltd. (Branded as "FHTPay")	Asia Pacific	12/19/2014	atsec (Beijing) Information Technology Co., L
Shenzhen GleePay Information Technology Co., Ltd. (Branded as "GleePay")	Asia Pacific	12/29/2015	atsec (Beijing) Information Technology Co., L
ShenZhen GlobeBill Technology CO., Ltd (Branded as "GBPAY")	Asia Pacific	01/11/2016	atsec (Beijing) Information Technology Co., L
Shenzhen Tenpay Technology Company Limited (Branded as "Tenpay")	Asia Pacific	01/27/2016	atsec (Beijing) Information Technology Co., L

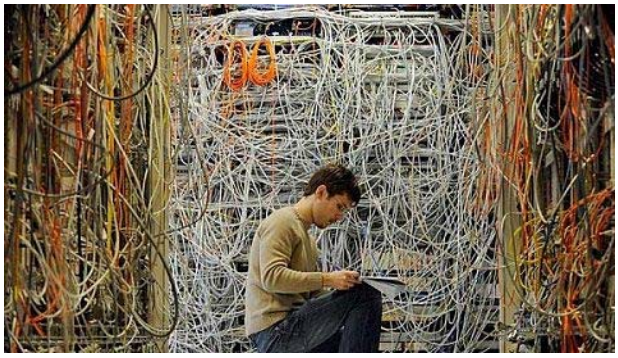
61-90 Days Past AOC Due Date

合规的价值 – 来自卡组织的强制性要求

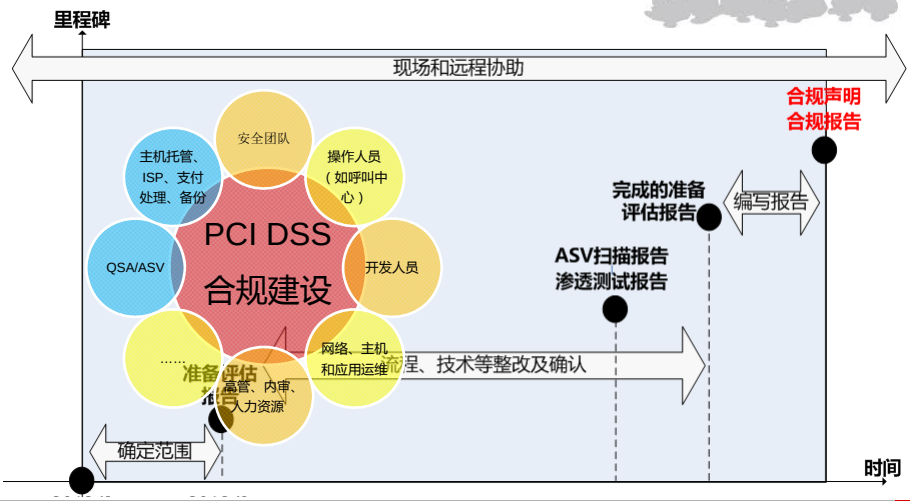
- 各个卡组织（VISA、MasterCard、JCB、American Express、Discovery）针对PCI DSS维护各自的验证要求。总体来讲，目前针对新上线系统卡组织要求收单机构和发卡机构通过PCI QSA合规评估。完整的PCI DSS合规是强烈推荐的。
- 支付应用的强制要求：
  - VISA组织要求新上线的机构必须使用PA-DSS合规的支付软件应用：生效日期: 7/1/2010；收单机构必须确保所有机构使用PA-DSS合规的支付应用：生效日期: 7/1/2012
  - Effective 1 July 2012, MasterCard SDP Program Standards require all merchants and Service Providers that use third party-provided payment applications to only use those applications that are compliant with the Payment Card Industry Payment Application Data Security Standard (PCI PA-DSS), as applicable.
  - Discover's PA-DSS mandate states that all Discover merchants and acquirers must ensure any new implementations of payment applications are compliant with the current version of the PA-DSS. Discover is also strongly encouraging all merchants and acquirers to upgrade existing implementations to payment applications that are PA-DSS validated.
  - Currently, American Express and JCB are evaluating the PA-DSS standard and may choose to fit it in with their compliance programs at a later date. Both brands strongly encourage that merchants and agents use PA-DSS validated applications.

atsec合规方法论分享

PCI DSS =



合规建设思路分享



PCI DSS合规结果


Payment Card Industry (PCI) Data Security Standard
Report on Compliance

机密

ZZZZ Payment Co., Ltd.


Payment Card Industry Data Security Standard
Attestation of Compliance

A QSA led assessment of compliance validation according to the Payment Card Industry Security Standards and Security Assessment Procedures version 3.0

ZZZZ Payment Co., Ltd.

Report Date: 2015-1-1
Initial Compliance Date: 2013/10/10
Report Number: CXXX-YY-2015-02
The assessment remains valid for 12 months

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, P.R. China, 102206
Tel: +86 10 5305 6679
Fax: +86 10 5305 6678
www.atsec.cn

PCI合规列表

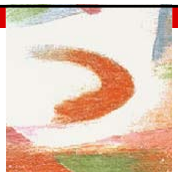
- PCI QSA Assessment List:
- http://www.atsec.cn/it-security-services/pci/pci-compliance/index.html

公司名称 COMPANY 合规标准 STANDARDS	创建日期 INITIAL DATE 发布日期 ISSUE DATE 失效日期 EXPIRY DATE	证书 ATTESTATION 编号 NUMBER
Accounting Centre of China Aviation PCI DSS v3.0	Initial Date: 2015-03-30 Issue Date: 2015-03-30 Expiry Date: 2016-03-29	atsec-2015-PCI-DSS-C.01156.05019
Air China Limited PCI DSS v3.1	Initial Date: 2015-11-06 Issue Date: 2015-11-06 Expiry Date: 2016-11-05	atsec-2015-PCI-DSS-C.19287.0124
Alipay.com Co., Ltd PCI DSS v3.1	Initial Date: 2014-11-14 Issue Date: 2015-11-13 Expiry Date: 2016-11-12	atsec-2015-PCI-DSS-C.01131.02007
Bank of China Limited. PCI DSS v3.1	Initial Date: 2016-02-05 Issue Date: 2016-02-05 Expiry Date: 2017-02-04	atsec-2016-PCI-DSS-C.01445.01067
Beijing Baidupay Science and Technology Co., Ltd PCI DSS v3.1	Initial Date: 2014-12-31 Issue Date: 2016-01-05 Expiry Date: 2017-01-04	atsec-2016-PCI-DSS-C.47271.0248
Beijing BoTongLianDa Technology Co., Ltd PCI DSS v3.0	Initial Date: 2014-07-21 Issue Date: 2015-08-31 Expiry Date: 2016-08-30	atsec-2015-PCI-DSS-C.75269.0219
BOC Services Company Limited Kunshan branch PCI DSS v3.1	Initial Date: 2012-12-06 Issue Date: 2015-12-06 Expiry Date: 2016-12-05	atsec-2015-PCI-DSS-C.69225.0255
CHASE Science Co., Ltd PA DSS v2.0	Initial Date: 2012-07-27 Issue Date: 2012-07-27 Expiry Date: 2016-10-28	Refer to SSC official website
Hainan New Generation Technology Company Limited. PCI DSS v3.1	Initial Date: 2016-02-20 Issue Date: 2016-02-20 Expiry Date: 2017-02-19	atsec-2016-PCI-DSS-C.01233.03005
HE RONG TONG Technology Co., Ltd PCI DSS v3.0	Initial Date: 2013-03-15 Issue Date: 2015-04-24 Expiry Date: 2016-04-23	atsec-2015-PCI-DSS-C.09263.0122
HotSauce Technologies PA DSS v2.0	Initial Date: 2013-10-18 Issue Date: 2013-10-18 Expiry Date: 2016-10-28	Refer to SSC official website
Industrial and Commercial Bank of China Limited PCI DSS v3.0	Initial Date: 2013-08-02 Issue Date: 2015-07-31 Expiry Date: 2016-07-30	atsec-2015-PCI-DSS-C.62226.0236
International Payment Solutions (China) Limited PCI DSS v3.1	Initial Date: 2015-02-05 Issue Date: 2016-02-05 Expiry Date: 2017-02-04	atsec-2016-PCI-DSS-C.01118.04016
iPayLinks Financial Information Service (Shanghai) Co., Ltd PCI DSS v3.0	Initial Date: 2015-04-15 Issue Date: 2015-04-15 Expiry Date: 2016-04-14	atsec-2015-PCI-DSS-C.01399.01021
JD.com Co., Ltd PCI DSS v3.1	Initial Date: 2015-10-10 Issue Date: 2015-10-10 Expiry Date: 2016-10-09	atsec-2015-PCI-DSS-C.24241.0131

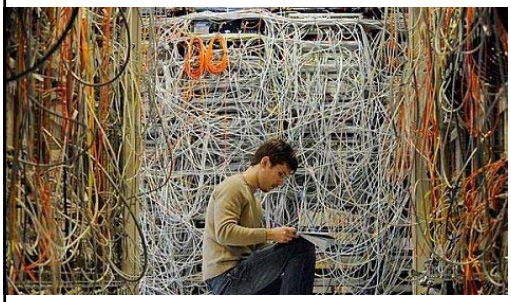
合规的价值

- **达到外部监管机构强制性要求，比如VISA、MasterCard、相关客户等；**
- **塑造形象增强机构往来的信心**
  - 监管机构或者权威部门的批准；
  - 客户，合作伙伴，供应商
  - 机构内部组织和部门之间
- **进一步加强机构内部管理和控制**
  - 加强公司管理高级别的安全性，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；
  - 全员提高安全意识，全员深刻体会企业文化；
  - 加强投资信心。

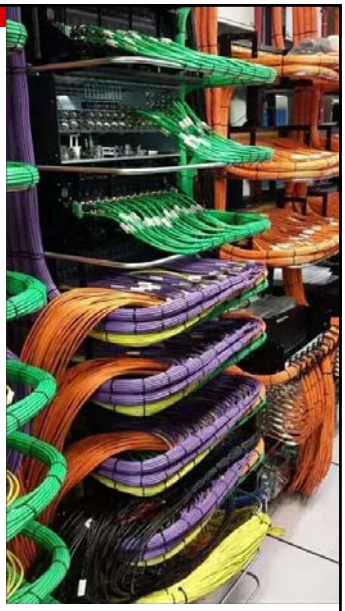
合规的价值-续



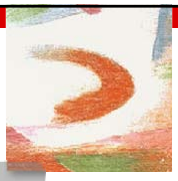
- **降低诸多的成本和费用**
  - 有效的管理和降低安全事件的影响，减小处理风险的投资，完整的风险管理，业务连续性和应急响应等细节的完善更是直接降低了重大事件发生的风险；
  - 通过符合性的审计和认证，可以减少其他各个领域的外部审查或调研，比如西方客户或者法律领域经常发生的尽职调查等；
  - 可以减少保险相关费用，通过符合性建设直接带来长期的必要保险费用的减低，或者保险额、保险范围的增加；
  - 通过管理体系职责明确，可以与相关人员分担安全工作。
  - 符合性建设和认证具有市场价值，在同行业同领域对手面前占据绝对的优势，提高自身竞争力；
  - 符合性建设和认证可以为全球信息交流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。

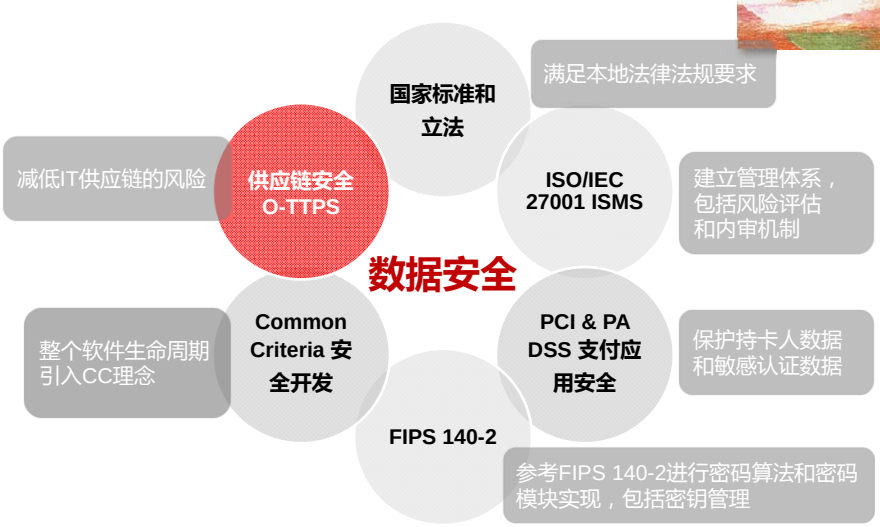


PCI DSS =



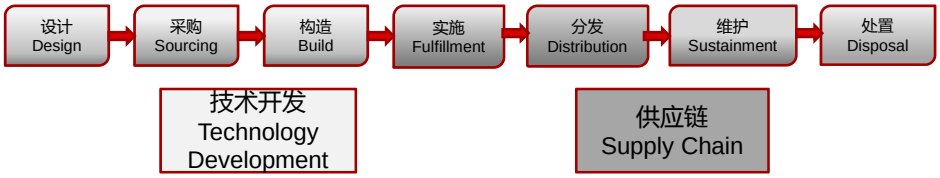
atsec整合统一的管理体系方法论





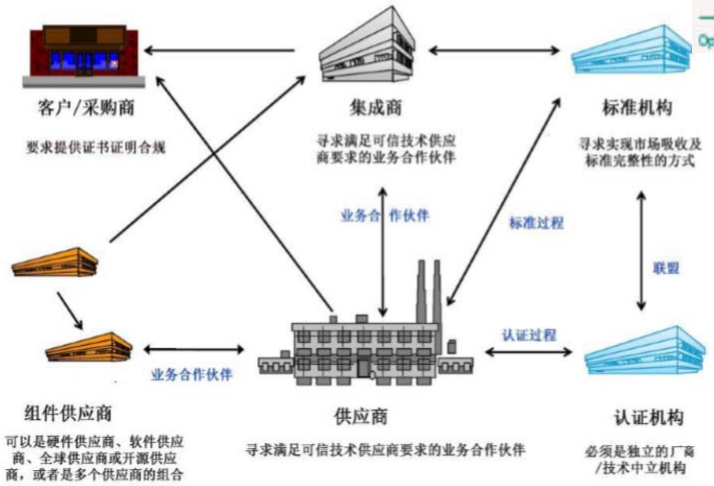
O-TTPS：降低恶意污染和伪造的供应链来源产品（组件）

- The Open Trusted Technology Provider Standard (O-TTPS) 2013年4月正式发布，atsec从最初参与该最佳实践的编写和开发。
- 3年的持续努力，产业合作。
- 贯穿于整个生命周期。
- 两个要求的领域 – 通常会根据产品和提供商有所重合：
  - 技术发展Technology Development – 一般是提供商内部监管
  - 供应链活动 – 一般关注于与该提供商交互的第三方



Source from OTTPS

参考O-TTPS降低商业环境供应链安全风险



Source from OTTPS

谢谢!
www.atsec.cn