




2014 Asia-Pacific Community Meeting



Payment security in China

Coauthors: Yan Liu, Gary Gu, Tao Chen

- 
- Disclaimer: atsec (Beijing) Information Technology Co.,Ltd is an independent lab specializing in IT security evaluations.
The authors do not represent any Chinese government agency or Chinese government-controlled lab. All information used for this presentation is publicly available on the Internet, despite the fact that most of them are in Chinese.

Introduction



- **Best practise from a QSA – atsec China**
- **Security Risk Management Practice from a service provider – 99bill**
- **PCI Compliance experience sharing from a merchant – Air China**



Background: Rapid Growth in China's Electronic Payment Space

269

Number of non-financial payment organizations continue to grow.

62.36%

E-payment penetration rate keeps rising.

1,800,000,000,000

Internet retail volume grows rapidly.

94%

E-payment sector remains highly concentrated.

Background: Payment Innovations with Underlying Risk Factors

Mobile POS



Virtual Currency



Bio-Tech



Insurance

众安保险



O2O



Credit Business

BIG-DATA
+
Credit Business



Background: Payment Innovation Patterns in China

A	Customer Interface	<i>M-POS、 Self-Service Terminals</i>
B	Functionality	<i>KJ Payment、 Fingerprint Payment</i>
C	Product Grouping	<i>e-Wallet、 e-Banking、 Credit Card Repayment</i>
D	Channel	<i>Payment As A Channel for Financial Products</i>
E	Service Addition	<i>Marketing、 Data、 Risk Service</i>
F	Business Mix	<i>Payment + Credit、 Wealth Management、 E-Commerce, etc.</i>



Background: Payment Risk Profile Trends in China

- 1** Security risk around mobile payment becomes increasingly critical.
- 2** Surge of CNP risk is hitting domestic & cross-boarder e-commerce.
- 3** Data-Leakage-Protection continues as a challenge to the industry.
- 4** Cyber-Crime becomes more organized and sophisticated.

Challenge: Security Risk Management Focusing Areas



**Product
Security**

**Data
Security**

**Transaction
Security**

**Fund
Security**



Case 1: Attack on Credit Card Vulnerability

- Merchant: ABC Motel
- Budget Hotel, established on 2013/12/27
- Payment Service: POS Terminal

Merchant	Transaction Time	Transaction Type	Amount
ABC Motel	2013-12-31 11:50:21	Pre-Auth	1.00
ABC Motel	2013-12-31 11:51:20	Pre-Auth Complete	1.00
ABC Motel	2013-12-31 12:16:26	Pre-Auth	1.00
ABC Motel	2013-12-31 12:20:19	Pre-Auth Complete	1.00
ABC Motel	2014-01-02 16:18:25	Pre-Auth	1.00
ABC Motel	2014-01-02 16:19:40	Pre-Auth Complete	1.00

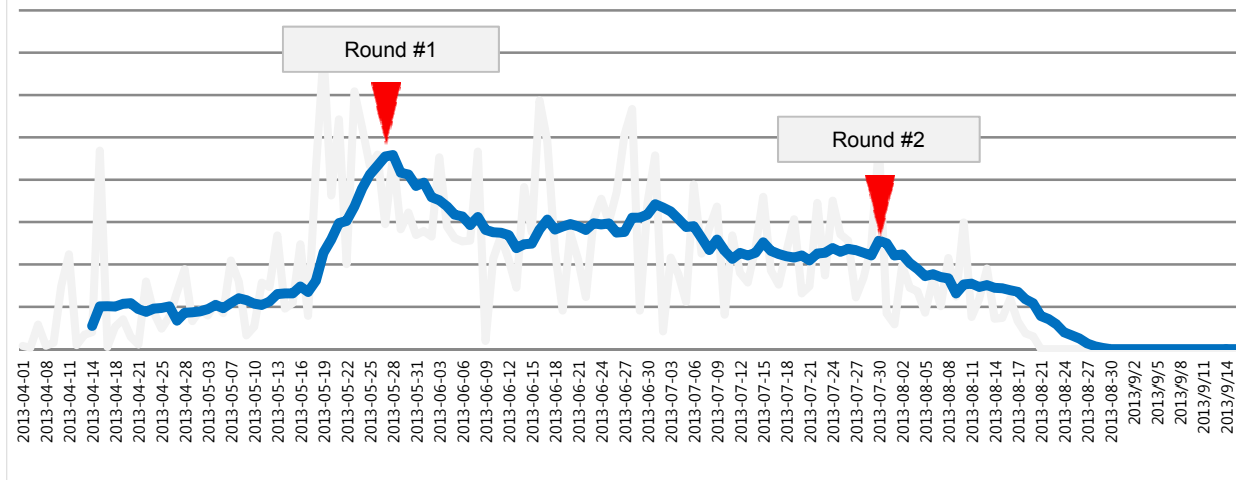
Merchant	Transaction Time	Transaction Type	Amount
ABC Motel	2014-01-03 01:44:38	Pre-Auth	69,000
ABC Motel	2014-01-03 01:53:25	Pre-Auth Complete	79,350
ABC Motel	2014-01-03 18:56:16	Pre-Auth	57,500
ABC Motel	2014-01-03 19:01:50	Pre-Auth Complete	66,125
ABC Motel	2014-01-04 10:59:09	Pre-Auth	75,000
ABC Motel	2014-01-04 11:04:28	Pre-Auth Complete	86,250

Highlights

- ▲ Small amount card testing
- ▲ Transaction amount abnormal
- ▲ Transaction time abnormal
- ▲ 115% Pre-auth percentage abnormal
- ▲ Massively impact on issuers and acquirers
- ▲ Regulatory sanctions

Case 2: CNP Risk on Airline Ticketing

CNP Risk Trend in An Airline Ticketing Merchant



Highlights

- ▲ Vast CNP attack airline ticketing companies
- ▲ Suspicious credit card data leakage
- ▲ Work with merchant to successfully suppressed the attack in 2013
- ▲ Assisted in arresting crime organization members

Background: About Air China



Connected to
32 countries
1,62 cities



Official airline in
China, and afford
special tasks



512 airplanes

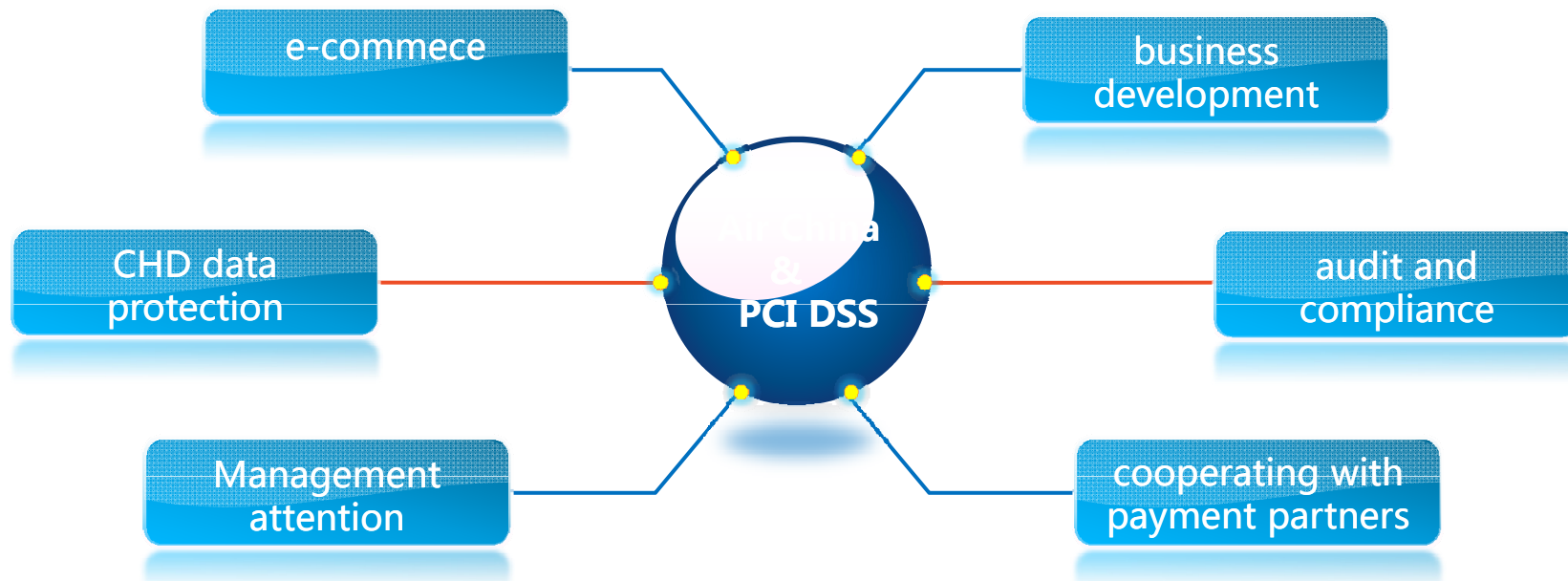


323 airlines



Passenger traffic
volume 77.974
million in 2014

Background: Motivation from Air China





Background: Assessors' Place in Payment Industry

atsec's Vision and Mission

Promote the effort of establishing a set of well-thought out, consistent standards for IT security evaluation worldwide.

Prevent re-inventing the wheel or making the same kind of mistakes repeatedly.

Enable western clients to deliver their products/solutions to the Chinese market by facilitating compliance to the Chinese requirements.

Help Chinese organizations to enter the global market or reach global standards requirements by achieving internationally recognized certificates and/or validation (e.g. PCI, CC, FIPS 140-2).



* CNAS: (China National Accreditation Service for Conformity Assessment) Laboratory Accreditation (based on ISO/IEC 17025)



2014 Asia-Pacific
Community Meeting

Background (from 99bill): Data Security Management

PCI-DSS Compliant since 2009 by atsec

Other Data Security Compliance Programs

PBOC	ISO/IEC	Ministry of Public Security	CUP
Payment Organization System Attestation Certificate	ISO/IEC 27001	Security Level-3 Certificate	ADSS

Background: Key national standards in China

GB 17859 -1999, "Classified Criteria for Security Protection of Computer Information System"

- Classifies the security protection capability of Computer Information Systems into five levels:
 - Level 1 - Discretionary Protection
 - Discretionary Access Control
 - Level 2 - System Audit Protection
 - Mandatory Access Control
 - Level 3 - Security Flag Protection
 - Labels
 - Level 4 - Structure Protection
 - Identification and Authentication
 - Level 5 - Access Verification Protection
 - Object reuse
 - Audit
 - Data Integrity
 - Covert Channel
 - Trusted Path
 - Trusted Recovery
- Outlines the incremental requirements for each security protection level from security functions in ten aspects:

GB/T 20271-2006, "Information Security Technology - Common Security Technology Requirements for Information Systems"

GB/T 18336.1-2008, GB/T 18336.2-2008, GB/T18336.3-2008

- the Chinese translations of Common Criteria Part 1, Part 2, and Part 3

Background: Surveillance and authority organizations in China

- The People's bank of China
 - was established on December 1, 1948. In September 1983, the State Council decided to have the PBC function as a central bank.
 - Starting from Sep 2010, PBC issued licenses for payment organizations in China after the assessment (including requirements regarding information security, but also business , performance, etc) according to the "non-financial institutions payment service management measures"(the Chinese name is 非金融机构支付服务管理办法); See the list as following:
<http://www.pbc.gov.cn/publish/zhengwugongkai/3580/index.html>
 - Under the schemas, 2 major certification bodies and a few labs
- Payment & Clearing Association of China
 - *PCAC was founded on May 23, 2011, upon the approval of the State Council and the Ministry of Civil Affairs of China. Registered at the Ministry of Civil Affairs as a national non-profit organization, PCAC serves as a self-regulatory body of the payment and clearing service industry of China, and operates under the business guidance and oversight from the People's Bank of China.*
 - In Feb 2014, payment security workshops were organized by cooperating with VISA, and atsec in China.



Background: Surveillance and authority organizations in China

■ Global card brands in China

- Facilitates collaboration with industry and builds a more secure and trusted payment network in China
- For example, Visa's QSP (Qualified service provider) program was started from 1 April 2013. See the list who has passed the QSP certification by VISA:
<http://www.visa.com.cn/merchants/riskmanagement/accountsecurity.shtml>
- PCI QSA validation is one of the requirements for QSP. In addition to that VISA will do audits with respect to the requirements related to risks management and GBPP, etc.
- Acts as an additional oversight layer to acquirer due diligence



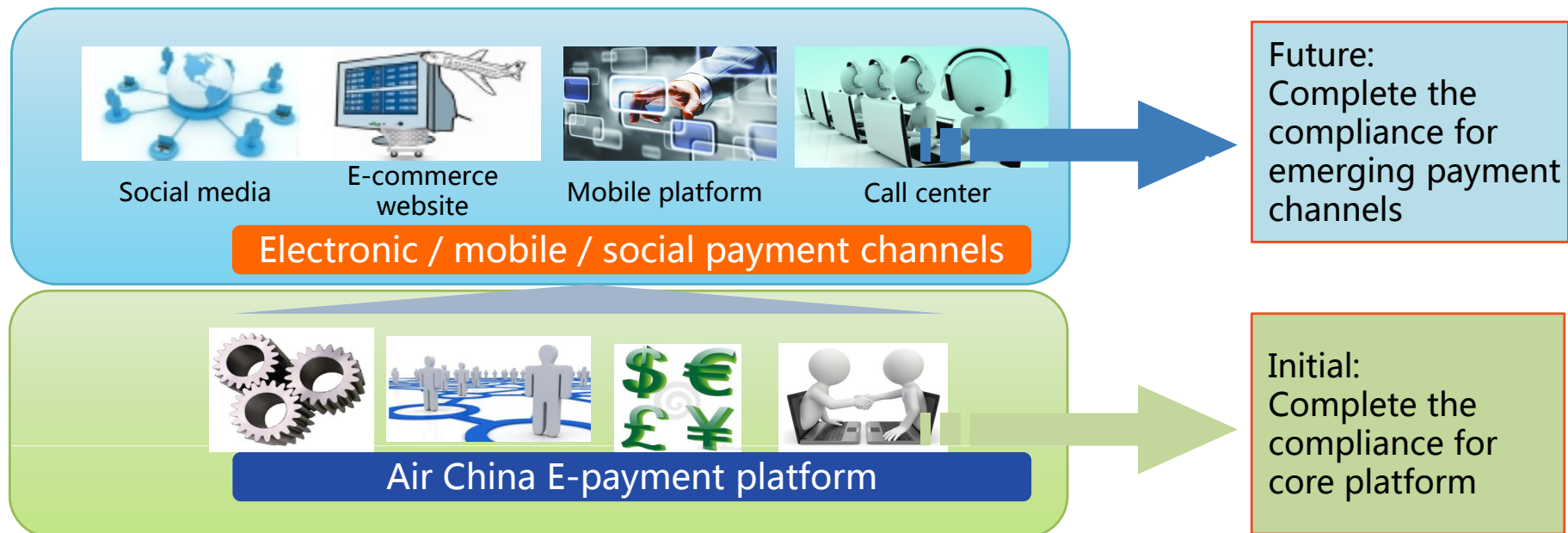
- ### ■ China Unionpay: Issued Account Data Security Standard (full Chinese name of the standard: 银联卡收单机构账户信息安全管理标准) initially in 2008 (similar security requirements with PCI DSS).



Looking forward, Challenges faced by China Payment Sector

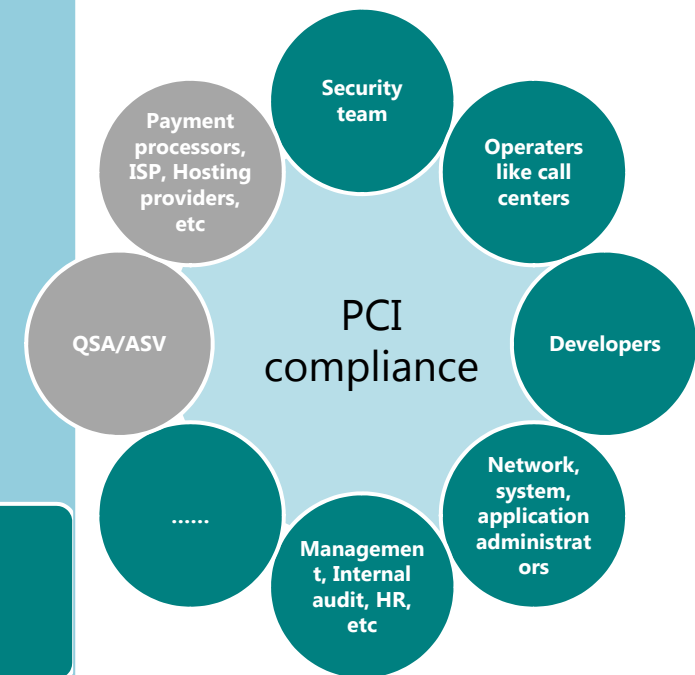
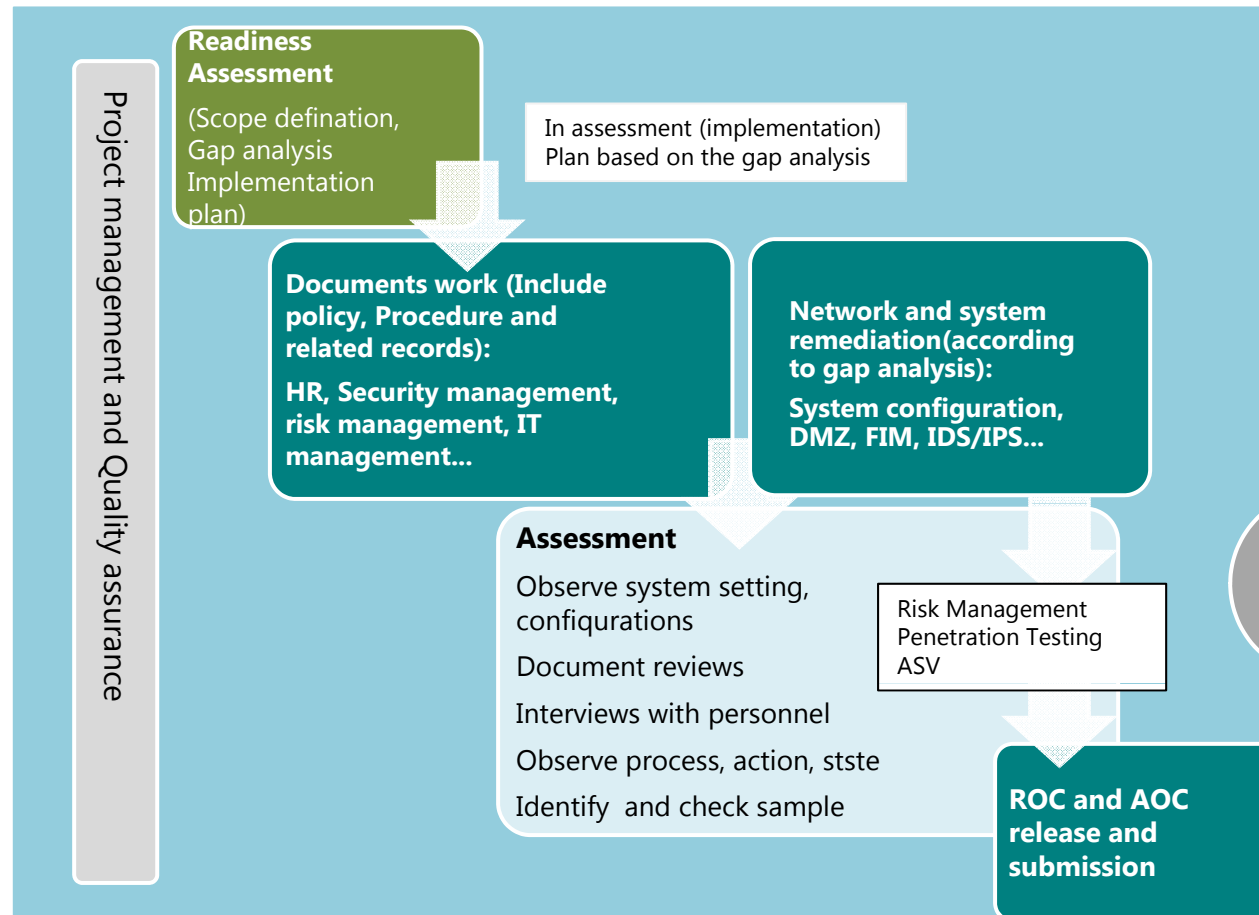
Competition	Regulation	Operation
1 New rivals, domestic and abroad	5 Compliance	7 Risk Management
2 Product Innovation		8 Technology
3 Talent	6 Legal System	9 Operation Efficiency

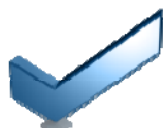
Challenge: Compliance and certification plan



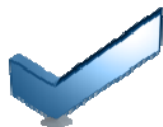
CHD discovery and network segmentation are challenging

Approach: PCI DSS Implementation Milestone

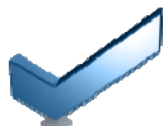




Optimizing data: clean up and protect the payment data



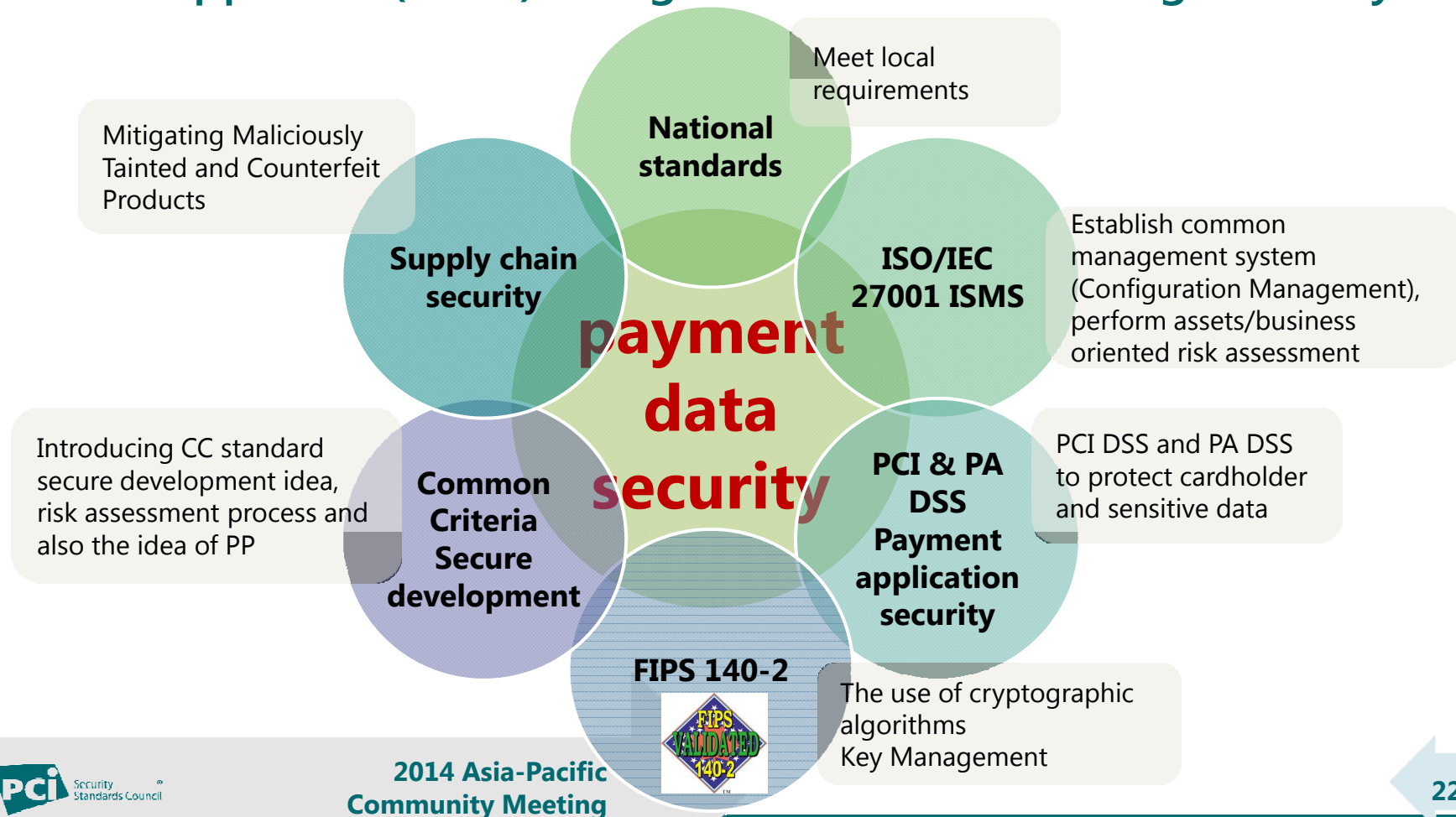
Improving business: establish stable and reliable payment environment



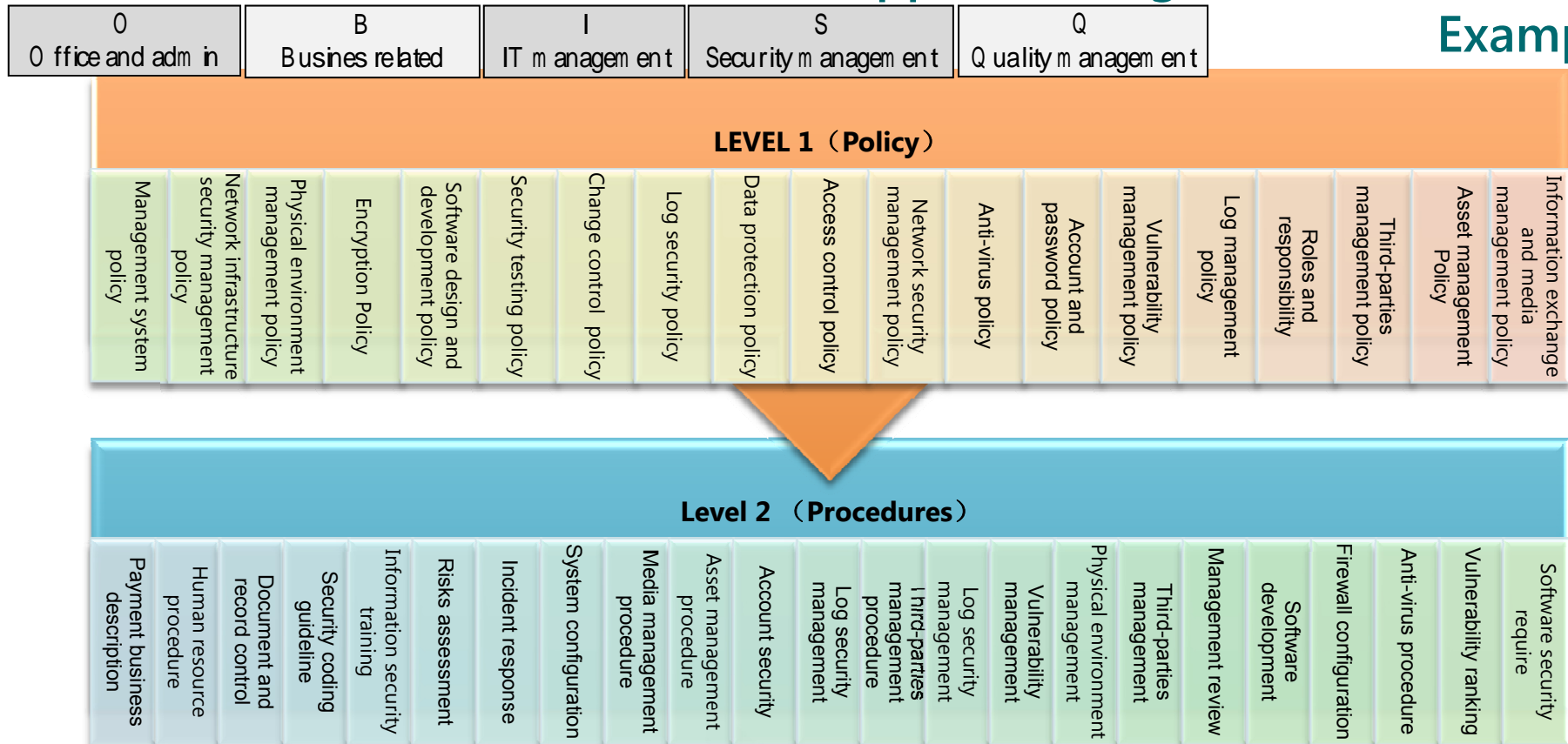
Improving technology: Improve security control measurement comprehensive



Approach (atsec): Integrated & unified Management System



Approach: Organizational Security Example



Approach: Consideration and plan after the initial compliance

Based on PCI DSS, Air China's methodology on data security in the future:

Two steps, five phases

Step one: data integration

Integration first



- What data we have;
- Where the data located;
- Who use the data;
- What about risks;
- What levels;
-

Step two: Implementation

Technology implementation



- Establishment of terminal security management ability;
- Establishment of data breach prevention ability;
- Establishment of database audit ability;
- Establishment of document centralized management ability
-

Five phases

1. Aviation business and the passenger data analysis

2. Risks assessment for critical data

3. Make the classification and control strategy of aviation business data and passengers data

4. Foundation protection of data security

5. Improve Air China overall data security management system

Why security compliance?

Meet the mandatory requirements defined by external cooperating organizations, like card brands, related customers;

Increase confidence during the business cooperation

- Surveillance organizations or authority organizations;
- Customers, partners, suppliers;
- Internal organizations or departments

Further improve internal management and control

- Improve security management, and integrate high level policy into the business process effectively;
- Establish measurable method for management and technology;
- Enhance the assurance of security control within the organization;
- Enhance the security awareness, and benefit for corporation culture;
- Enhance the investment confidence

Reduce cost

- Reduce the cost and investment for security incident and risks; improve processes on risk management, business continuity and incident response;
- Reduce the cost on the audit or assessment in other area, like due diligence;
- Reduce the insurance cost;
- Clarify the security roles and responsibility;
- Improve competitiveness;
- Establish trust and recognition globally

Recommendations



- **Harmonization with national standards and global standards**
- **Industry collaboration**
- **CDE Scope and implementation plan**
- **Risk-based approach**

Thanks You!

Yan Liu, Principal Consultant, atsec China

Tel : +86-139-1072-6424

E-mail : yan@atsec.com

Gary Gu, Vice President, 99Bill Corporation

Tao Chen, PCI Project Manager, Air China

