

CONTROLCASE™ INTRODUCTION

Agenda



PCI DSS
For Retail
Industry

1

ControlCase – Who we are, What we do, How we can help you

2

PCI DSS – What is it, Why is it needed, How to get it

ControlCase – Who we are, what we do, how we can help you

ControlCase™ Corporate Overview

- .. Founded in 2004 by former Ernst & Young/PwC professionals
- .. Offices in McLean, VA and Mumbai, India ,Dubai, UAE with additional resources in Japan, Korea, Philippines and multiple US locations
- .. 100 + clients worldwide
- .. Pioneers in Managed Compliance which includes:
 - .. PCI DSS Certification Services
 - .. IT GRCM Software
 - .. Data Discovery Software
 - .. Managed Security Services



ControlCase™ Corporate Overview

- Rated 'Promising' by Gartner in the recent market scope
- Single largest pool of PCI qualified professionals (QSAP) in US, Middle East & Asia-Pacific. First PCI empanelled company in India
- Rated as top 25 percentile of all American companies by Dun & Bradstreet, D&B DUNS Number 36-285-3769
- One of the 5 companies selected by State Government of Virginia for assistance in overseas growth.



Current Sample Customers (more than 100 customers across 20 countries)

North America

- Intersections
- Washington Metro
- NCR
- TravelClick
- Large US Banks

Middle East

- National Bank of Kuwait
- Commercial Bank of Qatar
- AlRajhi Bank - KSA
- Bank Saudi Fransi
- Arab Bank

India

- ICICI Bank
- Vodafone
- Cap Gemini
- WNS
- FSS

Africa

- Bank Misr
- Coop Bank
- Kenya Commercial Bank
- HLP
- Bank DuCaire

Asia/Pacific

- Vevo Systems, Thailand
- Dai Nippon Printing, Japan
- Equitable Computers, Philippines
- BNI Bank, Indonesia
- Paygate, S.Korea

Current Sample Customers (more than 100 customers across 20 countries)



Differentiations / Why us

- .. PCI is a core focus of the company in Asia-Pacific
- .. A PCI focused IT GRC portal and card search software
- .. Got AINMA bank certified (which is one of the first banks globally to get certified)
- .. Multi region operations in US, CEMEA, APAC
- .. Experience in BFSI sectors including some of the largest banks:
 - .. National Bank of Kuwait
 - .. Large US Banks
 - .. Al Rajhi Bank
 - .. Commercial Bank of Dubai
 - .. ICICI Bank
 - .. Bank Misr

Differentiations / Why us

- .. Experience with merchants:
 - .. Ridecharge
 - .. Salt lake city plaza hotel
 - .. Washington metro
 - .. Blockbuster network
 - .. Alshaya
 - .. Kudzu
 - .. Traveclick
 - .. Southern Sun Hotels

Offerings Portfolio



IT GRC Software (includes Data Discovery Software)



ControlCase GRC — Compliance Manager - PCI

- .. Single and centralized repository for all compliance related data
- .. Deploy questionnaires to evaluate manual controls
- .. Dashboards and reports
- .. Remediation tracking
- .. Test password strength of domain and databases

ControlCase GRC — Compliance Scanner

- .. Pinpoint credit card or sensitive data within databases, file systems, desktops and servers
- .. External vulnerability scans
- .. Analyze firewall rule sets
- .. Perform vulnerability scans and integrate with existing vulnerability scanners
- .. Integrate with web application scanners

Compliance Manager Screenshots

Assessment Admin - Risk Rating

● Low
● Medium
● High

Remediation - Remediation Status

■ Total tasks
■ Waiting for approval
■ Closed

Database Credentials

Step 11 of 17: Databases

Provide credential details of the databases. Data Search tool will scan the databases for cardholder data. In case any enterprise databases are not manually entered, they will be auto discovered at a later point. You can add additional database servers after the auto-discovery process.

Uploaded Record :

Database Server	Non-Default Port Number	Type	User Name	Authentication Type	Added By	Added On	
10.1.3.9		POSTGRES	pgadmin	SQLAuth	admin	Apr 20, 2009	Delete
10.1.3.9		POSTGRES	pgadmin	SQLAuth	admin	Apr 20, 2009	Delete
10.1.3.7		SYBASE	sybaseadmin	SQLAuth	admin	Apr 20, 2009	Delete
10.85.203.23		SQLServer	sa	SQLAuth	admin	Apr 20, 2009	Delete
10.85.203.22		SQLServer	sa	SQLAuth	admin	Apr 20, 2009	Delete

Database Types:
 Authentication Type:
 User Name:
 Password:
 Non-Default Port Number:
 IP Addresses:

(Enter multiple IP addresses / Database Server Name separated by comma.)

OR

Scan Result: (Upload CSV or DMP file only)

PCI DSS – What is it, Why is it needed, How to get it

What is PCI (Payment Card Industry)

- PCI is a family of data security standards that is intended to secure processing infrastructure of payment industry.
- Processing Infrastructure of payment industry includes all organizations, processes and systems that handle, store, process or transmit sensitive information like credit card information, PIN or cryptographic keys directly or indirectly.
- PCI as a term is generally never used alone. The key standard in PCI is PCI Data Security Standard, or PCI DSS.

PCI DSS – Historical Perspective

Individual Card Association Security Programs:

- Visa Card Information Security Program
 - MasterCard Site Data Protection
 - American Express Data Security Operating Policy
 - Discover Information and Compliance
 - JCB Data Security Program
-
- PCI Security Standards Council formed in 2006
responsible for the development, management, education, and awareness of the PCI Security Standards

PCI Family of Standards



- .. PIN Transaction Security: Vendors manufacturing Pin Entry Devices
- .. PCI PA DSS: Software vendors who develop commercial secure payment applications
- .. PCI DSS: If a Primary Account Number (PAN) is stored, processed, or transmitted.

PCI DSS - Facts

- Not a Law
- Data Security Standard adopted by major card processing networks (Visa, MasterCard, etc.) to combat fraud and promote secure processing of payment card transactions
- Unified standard for security associated with card data storage, transmission, and processing
- PCI DSS Compliance is recommended / mandatory as per the organizations levels that deals with card data.

Core of PCI DSS

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	Primary Account Number (PAN)	YES	YES	YES
	Cardholder Name*	YES	YES*	NO
	Service Code*	YES	YES*	NO
	Expiration Date*	YES	YES*	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2/CVV2/CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

Brief Introduction to PCI DSS Requirements

Build & Maintain a Secure Network

1. Install & Maintain a Firewall Configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

1. Protect Stored Data
2. Encrypt Transmission of cardholder data and sensitive information across public networks.

Maintain a Vulnerability Management Program

1. Use and regularly update anti-virus software.
2. Develop and Maintain Secure Systems and Applications.

PCI DSS Requirements (Contd.)

Implement Strong Access Control Measures

1. Restrict Access to Data by business need-to-know.
2. Assign a unique id to each person with computer access.
3. Restrict physical access to cardholder environment.

Regularly Monitor and Test Networks

1. Track and Monitor all access to network resources and cardholder data.
2. Regularly test security systems and processes.

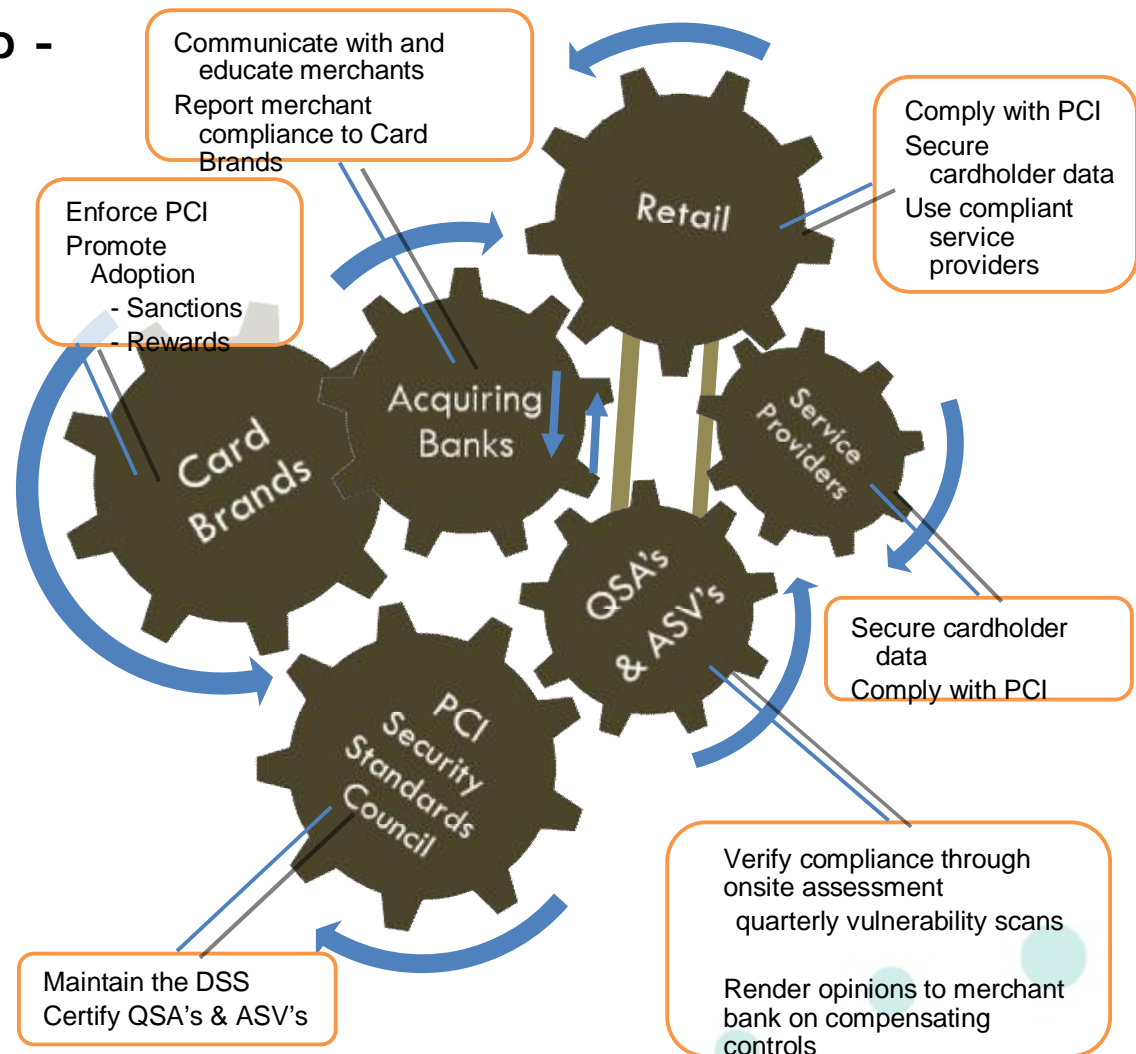
Maintain a Information Security Policy

1. Maintain a policy that addresses information security.

Definitions

Roles and Responsibilities Under PCI

Owned and maintained by the PCI Security Standards Council
Promoted and enforced by the card brands
Administered by acquiring banks
Interpreted by Qualified Security Assessors (QSA's)
Observed by merchants
Assessed by merchants or QSA's and by Approved Scan Vendors (ASV's)



Why PCI DSS is needed?

- Negative media coverage
- Damage to reputation
- Impacts to consumer confidence
- Counterfeit cards and fraud
- Significant chargeback risk
- Penalties, fines, losses
- Legal wrangling

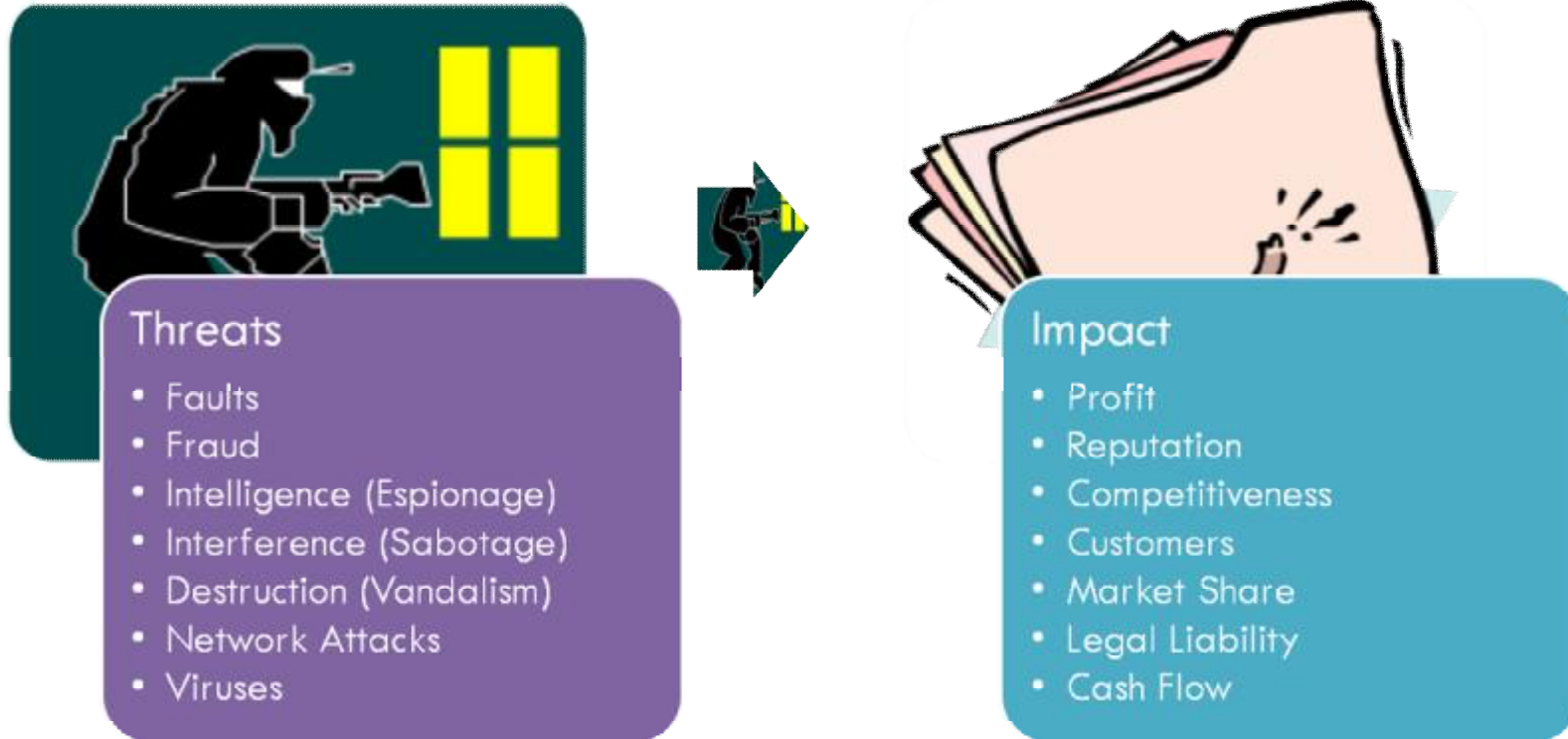
Pit falls of PCI DSS

- .. Storage of prohibited data like CVV, PIN, Track data
- .. Storage of PAN information in clear format
- .. Incorrect network architecture and usage of insecure wireless networks
- .. Lack of patch management and vulnerability management process
- .. Usage of non PA-DSS certified third party applications
- .. Inadequate Log Monitoring & Incident Response Process
- .. Missing Secure Software Development Life-cycle with focus on application security

Brief PCI DSS Certification Methodology



PCI DSS Challenges



Failure to comply with PCI DSS is a breach of contract & can potentially result in fraud / monetary fines and/or actions taken by card brands on a case by case basis

PCI DSS Challenges - Technical

- What is data classification and why do you need to care?
- Do you know where your Confidential, PCI data is located?
- Do you know what your sensitive data is?
 - What users and groups have access to sensitive data?
 - What users and groups are accessing sensitive data?
 - Where is sensitive data most at risk?
 - Which of my sensitive data is not being used and can be archived or simply deleted?
 - General Guidelines for employee access to cardholder data:
 - If you don't need it, you should not have access to it.
 - If you need it, there should be justification and strong access controls.
 - If you have to store it, it must be encrypted.
 - If you use it, then its use should be controlled and monitored.
 - If you have to print it, then the printed cardholder information must be accessed, stored and disposed of securely, in line with Information Security Policies and Standards
 - Network Segmentation and Isolation
 - IT operations and maintenance of systems with cardholder data
 - Documentation and demonstration of compliance (evidence)
 - Training and user awareness

PCI DSS Challenges - Management

- A challenge to change the attitude of the organization towards security and card data
- Time, Resource and Budget
- Prioritization of Remediation activities
- Keep the PCI Certification as a goal for everyone to achieve.

Questions & Contact Information

Suresh Dadlani
sdadlani@controlcase.com
+91-9820293399

Ketal Sheth
ksheth@controlcase.com
+91-9324548363

Afy Merchant
amerchant@controlcase.com
+91-9833264520

www.controlcase.com

