# Credit Cards and Oracle: How to Comply with PCI-DSS

Stephen Kost

Integrigy Corporation

Session #600

# Background

## Speaker

### Stephen Kost

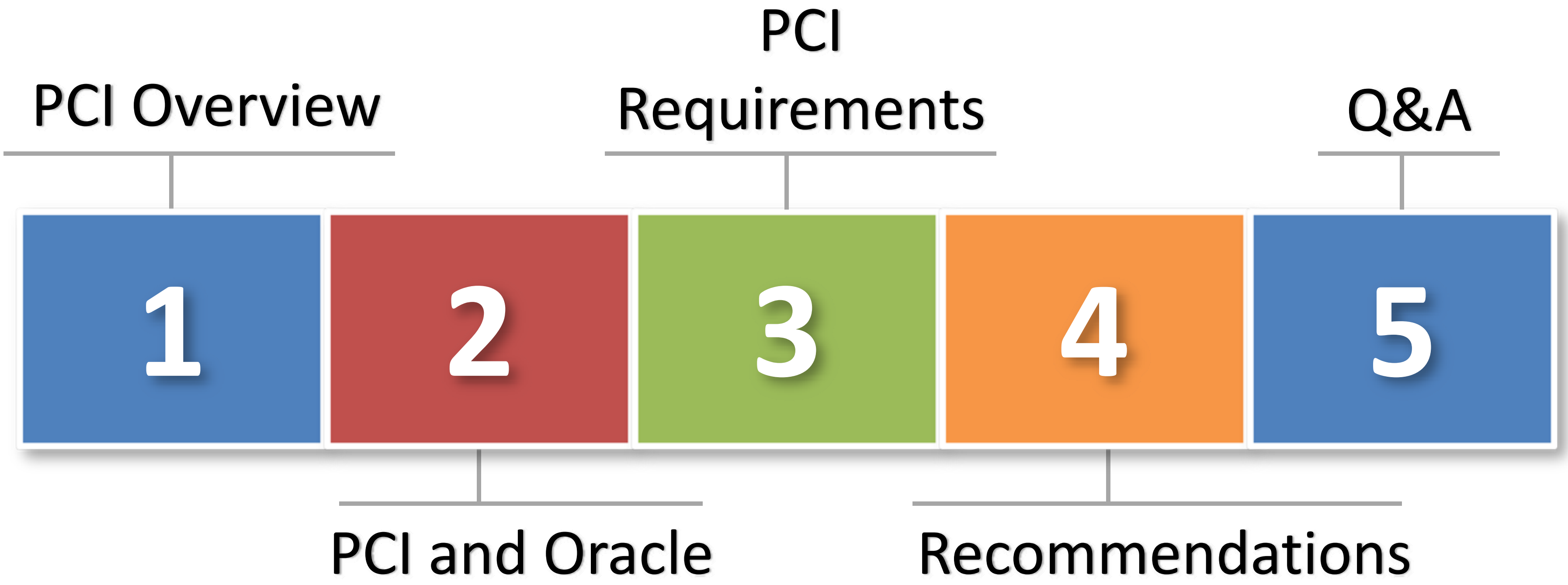
- CTO and Founder
- 16 years working with Oracle
- 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, …

## Company

### Integrigy Corporation

- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool

# Agenda



1 PCI Overview

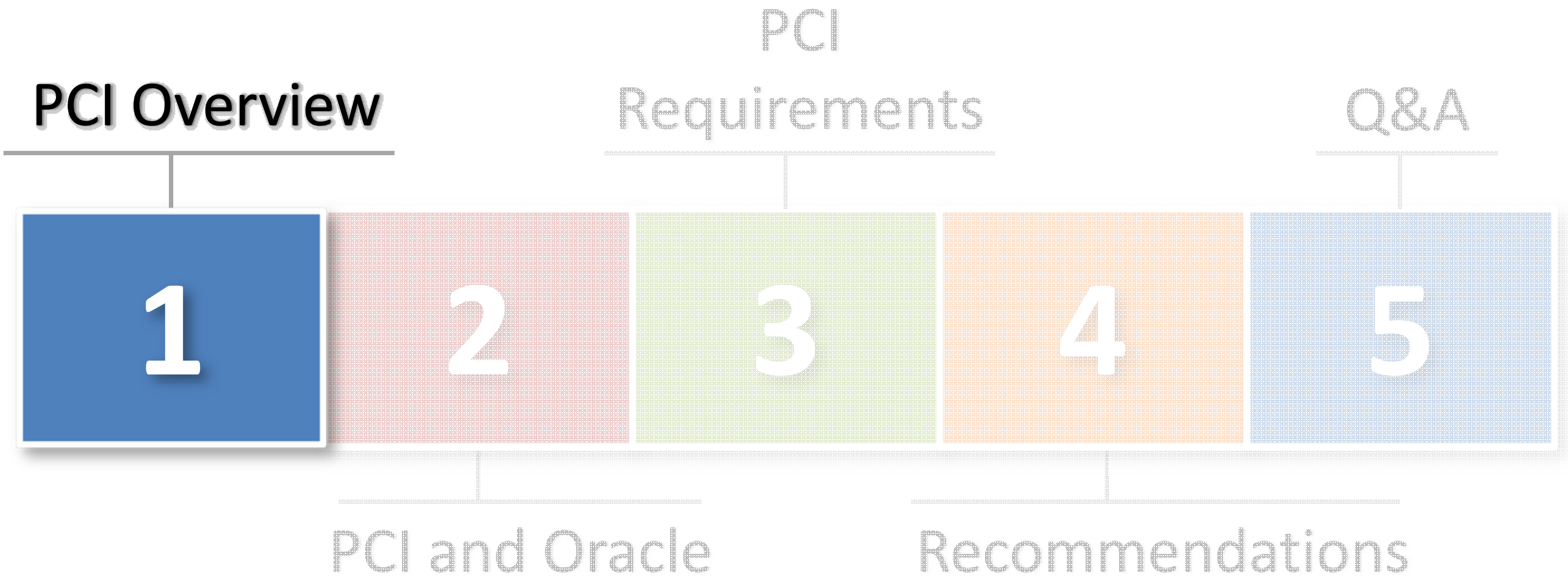
2 PCI and Oracle

3 PCI Requirements

4 Recommendations

5 Q&A

# Agenda



1 PCI Overview

2 PCI and Oracle

3 PCI Requirements

4 Recommendations

5 Q&A

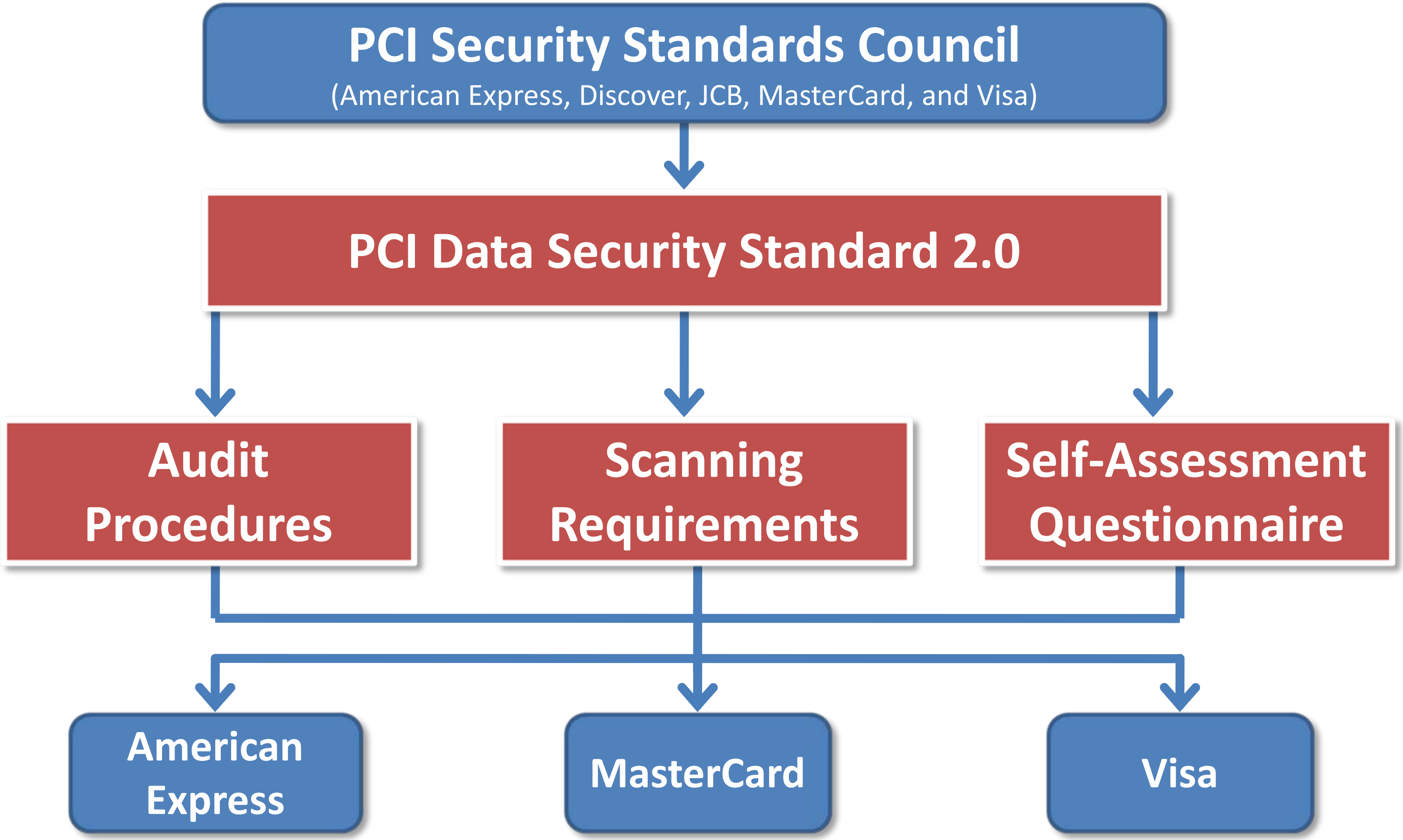
# Payment Card Industry

- **PCI Security Standards Council** is a single organization that consolidated the multiple credit card security programs
  - American Express, Discover, JCB, MasterCard, Visa
- Publishes “Data Security Standard” and related documents
- Manages third-party “Qualified Security Assessors (QSA)” and “Approved Scanning Vendors (ASV)”

# PCI Data Security Standard 2.0

- A set of 12 stringent security requirements for networks, network devices, servers, and applications
- Specific requirements in terms of security configuration and policies and all the requirements are mandatory
- Focused on securing credit card data
- **Significant emphasis on general IT security and controls**

# PCI DSS



PCI Security Standards Council

(American Express, Discover, JCB, MasterCard, and Visa)

PCI Data Security Standard 2.0

Audit Procedures

Scanning Requirements

Self-Assessment Questionnaire

American Express

MasterCard

Visa

# PCI Compliance

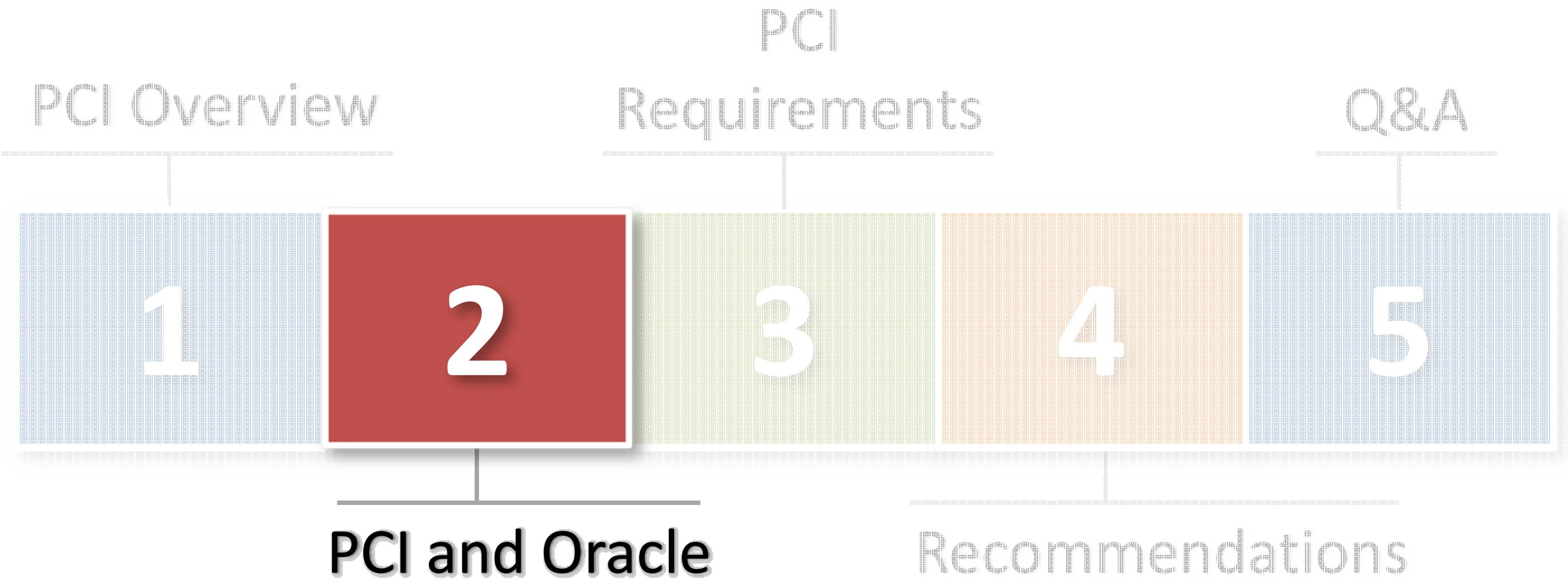
- **Compliance is dependent on card brand, merchant type (ecommerce), and transactions**
  - On-site assessment
  - Quarterly external scans
  - Self-assessment questionnaire (through Acquirer)
  - Depending on card brand, may be required to submit documentation
- **In case of a data breach, compliance is assessed by team of forensic auditors**
  - Audit result determines liability

# PCI Merchant Levels*

| Transactions per Year | Level | Compliance Requirement |
|---|---|---|
| **6,000,000+** | **1** | ▪ Annual on-site security assessment by QSA<br>▪ Quarterly Internet-facing network scan by ASV |
| **1,000,000 to 6,000,000** | **2** | ▪ Annual PCI self-assessment (SAQ)<br>▪ Quarterly Internet-facing network scan by ASV |
| **20,000 to 1,000,000 e-Commerce (only)** | **3** | ▪ Annual PCI self-assessment (SAQ)<br>▪ Quarterly Internet-facing network scan by ASV |
| **< 20,000 e-Commerce<br>< 1,000,000 Total** | **4** | ▪ Annual PCI self-assessment (SAQ) |

* Varies by card brand (VISA, MasterCard, American Express)

# Agenda



1 PCI Overview

2 PCI and Oracle

3 PCI Requirements

4 Recommendations

5 Q&A

# PCI and Oracle

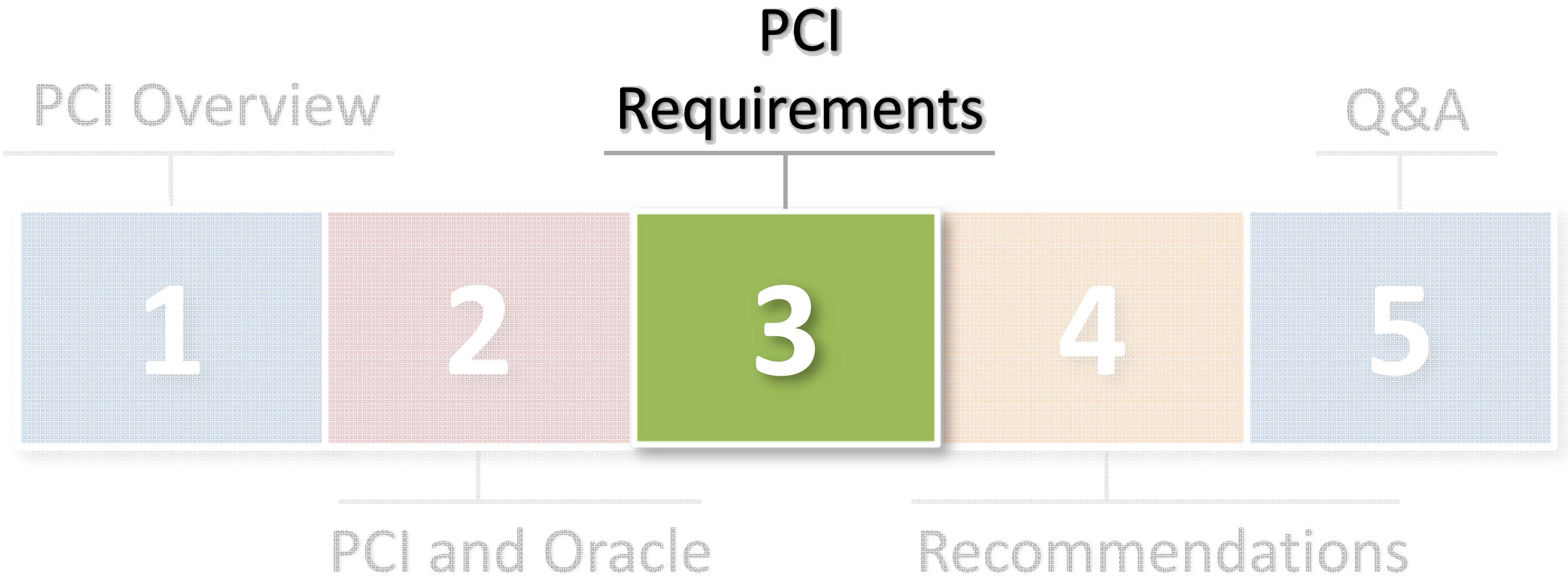
All Oracle databases that **"store, process, or transmit cardholder data"** must comply with the Data Security Standard regardless of size or transaction volume.

# PCI Oracle Scope

PCI scope for an Oracle database is –

- Entire sever
- All databases on server

# Agenda



PCI Overview

PCI Requirements

Q&A

1

2

3

4

5

PCI and Oracle

Recommendations

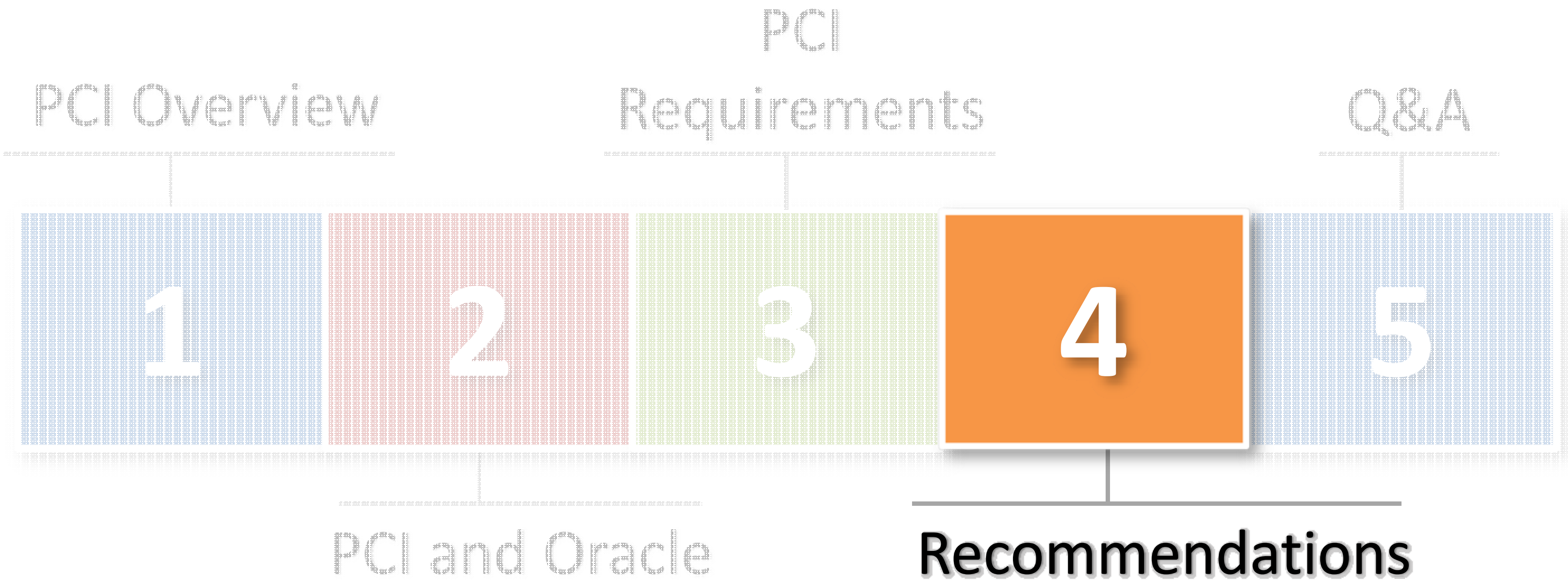
# PCI Requirements

| # | Requirement | Network | Server | Database | App | Policy |
|---|---|---|---|---|---|---|
| 1 | Use Firewall to protect data | ✓ | | | | ✓ |
| 2 | Do not use vendor-supplied defaults | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3 | Protect stored cardholder data | | ✓ | ✓ | ✓ | ✓ |
| 4 | Encrypt across open, public networks | ✓ | | | | |
| 5 | Use Anti-virus software | | ✓ | | | ✓ |
| 6 | Develop and maintain secure applications | ✓ | ✓ | ✓ | ✓ | ✓ |
| 7 | Restrict access to cardholder data | | ✓ | ✓ | ✓ | ✓ |
| 8 | Assigned unique IDs for access | | ✓ | ✓ | ✓ | ✓ |
| 9 | Restrict physical access to data | ✓ | ✓ | | | ✓ |
| 10 | Track and monitor access | ✓ | ✓ | ✓ | ✓ | ✓ |
| 11 | Regularly test security | ✓ | ✓ | ✓ | ✓ | ✓ |
| 12 | Maintain information security policy | | | | | ✓ |

# PCI Definition of Bad Things to Do

1. Storage of CVV/CV2 or magnetic strip data
   - Not normally stored in applications
   - CVV/CV2 is 3 digits on back of card or 4 digits above number on front of card
2. Storage of card number (PAN) **unencrypted**
3. Weak "General IT Controls"
   - IT processes such as passwords, patching, change management, and development

# Agenda



1 PCI Overview

2 PCI and Oracle

3 PCI Requirements

4 Recommendations

5 Q&A

# #2 - Do not use vendor-supplied defaults

- Change all default database passwords
- Implement standard database recommendations in best practices such as Oracle’s, Center for Internet Security (CIS), Department of Defense (DOD STIG), or SANS
- **All administrator network traffic must be encrypted, consequently, all network traffic must be encrypted**
  - SSL, SSH, SQL*Net encryption

# #3 - Protect stored cardholder data

- **Card number MUST be encrypted**
  - Several options for encryption
  - Application must also mask display of card number
  - Key management policies and procedures are critical
- **Storing of card data in logs is a major issue**
  - Look at other log files such as Apache or reporting
- **Review existing data archiving and purging**
  - Credit card data retention should be less than 18 months
  - Do not mean entire transaction, just card number
- **Must find <u>ALL</u> locations of credit card data**

# #6 - Develop and maintain secure apps

- ★ **Oracle Critical Patch Updates (CPU) should be applied within 30 days!**

  ***"Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release."***

- All sensitive data must be scrambled or removed during cloning, **including encrypted and hashed data**

# #8 - Assigned unique IDs for access

- **No generic accounts or all usage must be tied to an individual**
  - How to handle SYS, SYSTEM, …?
  - No generic accounts for read-only
  - Generic management accounts must be controlled
- **Strong password controls must be implemented for database and application**
  - Need to use database profiles to enforce database passwords
  - Must have a custom password validation function
  - Length => 7, password complexity, expire every 90 days, no reuse > 450 days, failure limit <= 6
- **Session time-out = 15 minutes**

# #10 - Track and monitor access

- **PCI has strong focus on logging, auditing, and monitoring**
  - Need to have logs and audit trails to forensically determine what happened in case of an incident
  - Daily review of critical logs required
- **Auditing and logging is problematic for Oracle due to the design and complexity**
  - Use of the generic, privileged accounts (SYS, etc.)
  - DBA can manipulate the audit trail
  - High volume of audit data with limited value
  - Many key audit fields can be spoofed

# #10 - Track and monitor access

- **10.1 Establish a process for linking all access to system components to each individual user (especially access done with administrative privileges)**
  - ***oracle/applmgr, SYS, SYSTEM, generic application accounts***
- **10.2 Audit Trails**
  - All individual accesses to cardholder data - ***Performance***
  - All actions taken by any individual with root or administrative privileges – ***SYS, SYSTEM***
  - Access to all audit trails
  - Invalid logical access attempts
  - Use of identification and authentication mechanisms
  - Initialization of audit logs
  - Creation and deletion of system-level objects
- **10.5 Secure audit trails so they cannot be altered**
  - ***SYS.AUD$ - no DBA access***
- **10.7 Retain audit trail history for at least one year**

# Database Audits and Estimated Volumes

| Audit | PCI # | Description | Daily Volume |
|---|---|---|---|
| Session | 10.2.1<br>10.2.4<br>10.2.5 | Connections to the database including failed logins (ora-1017) | 10,000+ |
| User | 10.2.2 | Creation, altering, and dropping of database user accounts | 0 |
| System audit | 10.2.3 | Changes to the database auditing | 0 |
| System grant | 10.2.2 | Grants to system privileges and roles, does not include object grants | 0 |
| Create role, alter any role, drop any role | 10.2.2 | Creation, altering, and dropping of database roles, does not include SET ROLE | 0 |
| Profile | 6.X | Creation, altering, or dropping of database profiles used for password controls | 0 |
| Public database link | | Creation, altering, or dropping of public database links, which should not be used | 0 |
| Database link | | Creation, altering, or dropping of database links | 0 |
| Sysdba, sysoper | 10.2.2<br>10.2.6 | Actions taken by DBAs | 100+ |

# #11 - Regularly test security

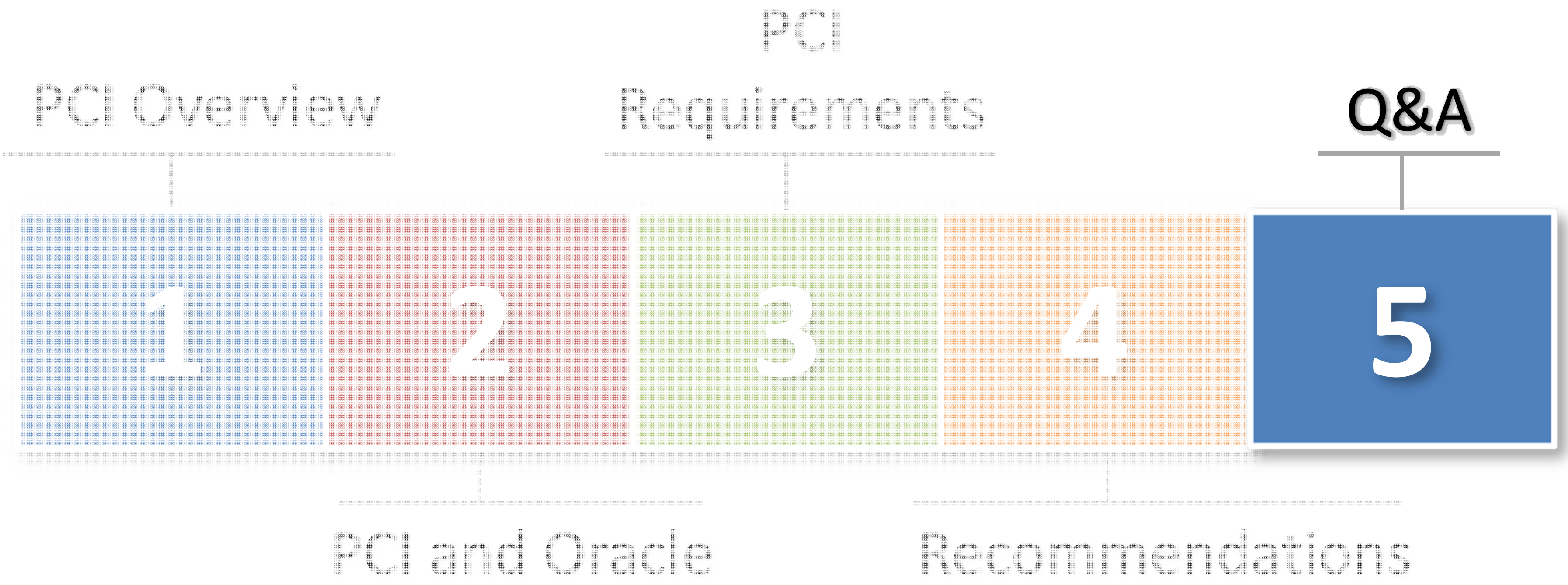
- **Periodic penetration tests should be performed annually, especially for Internet-facing applications**

- **“Deploy file integrity monitoring software”**
  - A standard ORACLE_HOME has 40,000+ files
  - Multiple configuration files and logs can make deploying file integrity monitoring challenging

# PCI PA-DSS

- Oracle PA-DSS Consolidated Patch for 12.1
  - Reduces complexity of PCI DSS compliance
  - Fixes multiple functional weaknesses when processing and viewing credit card data
  - Does not eliminate significant manual configuration for PCI DSS
  - Only 12.1 is PA-DSS compliant
  - See Metalink Note ID 984283.1
- 11i and 12.0 will not be PA-DSS compliant
  - See Metalink Note ID 1101213.1

# Agenda



1 PCI Overview

2 PCI and Oracle

3 PCI Requirements

4 Recommendations

5 Q&A

# *Credit Cards and Oracle: How to Comply with PCI-DSS Session #600*

**Stephen Kost**
**Chief Technology Officer**
**Integrigy Corporation**

**e-mail: info@integrigy.com**
**blog: integrigy.com/oracle-security-blog**

**For information on -**

- Oracle Database Security
- Oracle E-Business Suite Security
- Oracle Critical Patch Updates
- Oracle Security Blog

**www.integrigy.com**