INTEGRIGY

PCI-DSS 3.0 Compliance
and the Oracle E-Business Suite

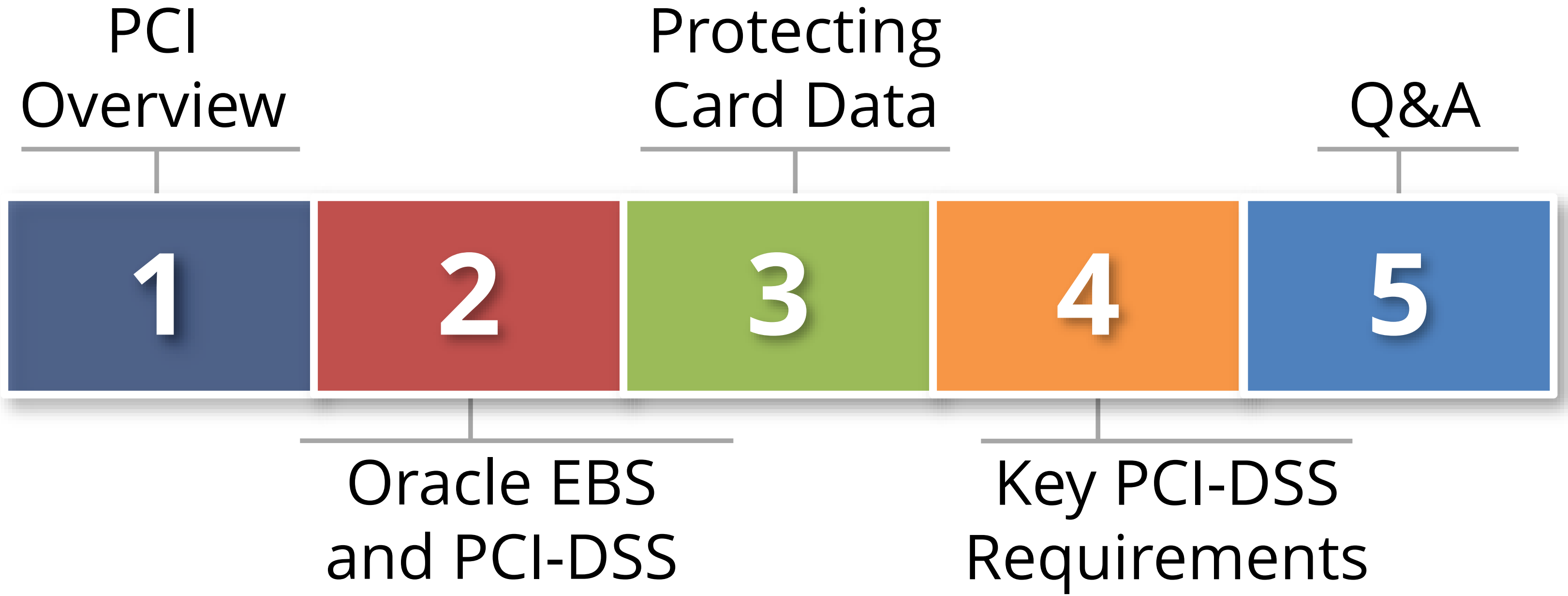
January 23, 2014

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Mike Miller
Chief Security Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



1 PCI Overview

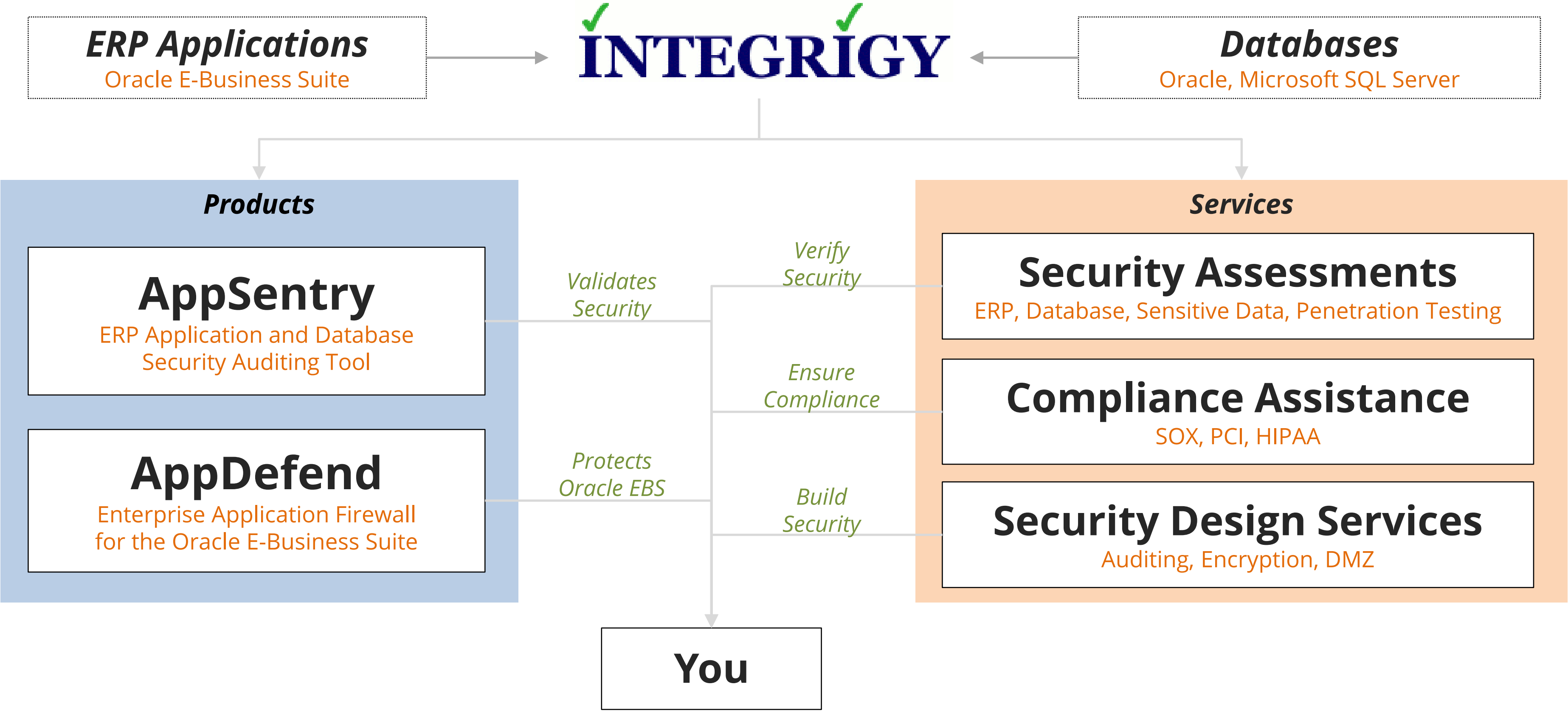
2 Oracle EBS and PCI-DSS

3 Protecting Card Data

4 Key PCI-DSS Requirements

5 Q&A

About Integrigy



ERP Applications

Oracle E-Business Suite

INTEGRIGY

Databases

Oracle, Microsoft SQL Server

Products

AppSentry

ERP Application and Database Security Auditing Tool

AppDefend

Enterprise Application Firewall for the Oracle E-Business Suite

Validates Security

Protects Oracle EBS

Verify Security

Ensure Compliance

Build Security

Services

Security Assessments

ERP, Database, Sensitive Data, Penetration Testing

Compliance Assistance

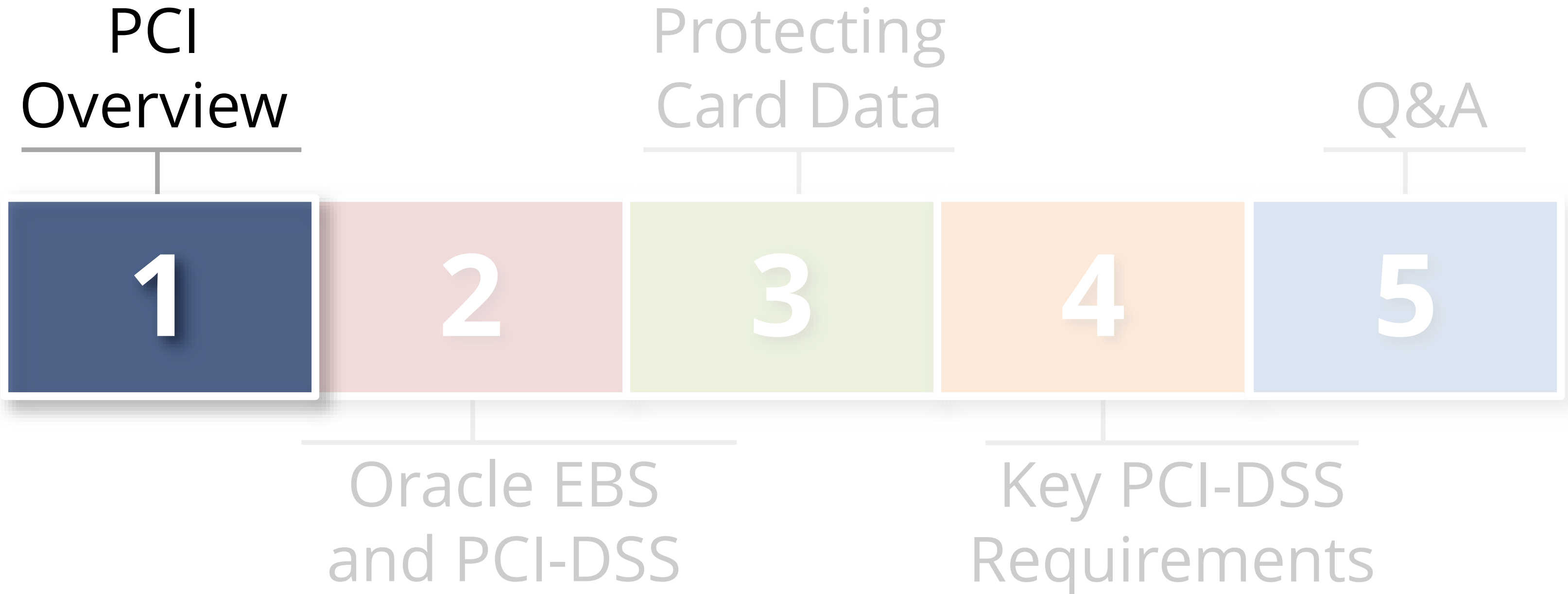
SOX, PCI, HIPAA

Security Design Services

Auditing, Encryption, DMZ

You

Agenda



1 PCI Overview

2 Oracle EBS and PCI-DSS

3 Protecting Card Data

4 Key PCI-DSS Requirements

5 Q&A

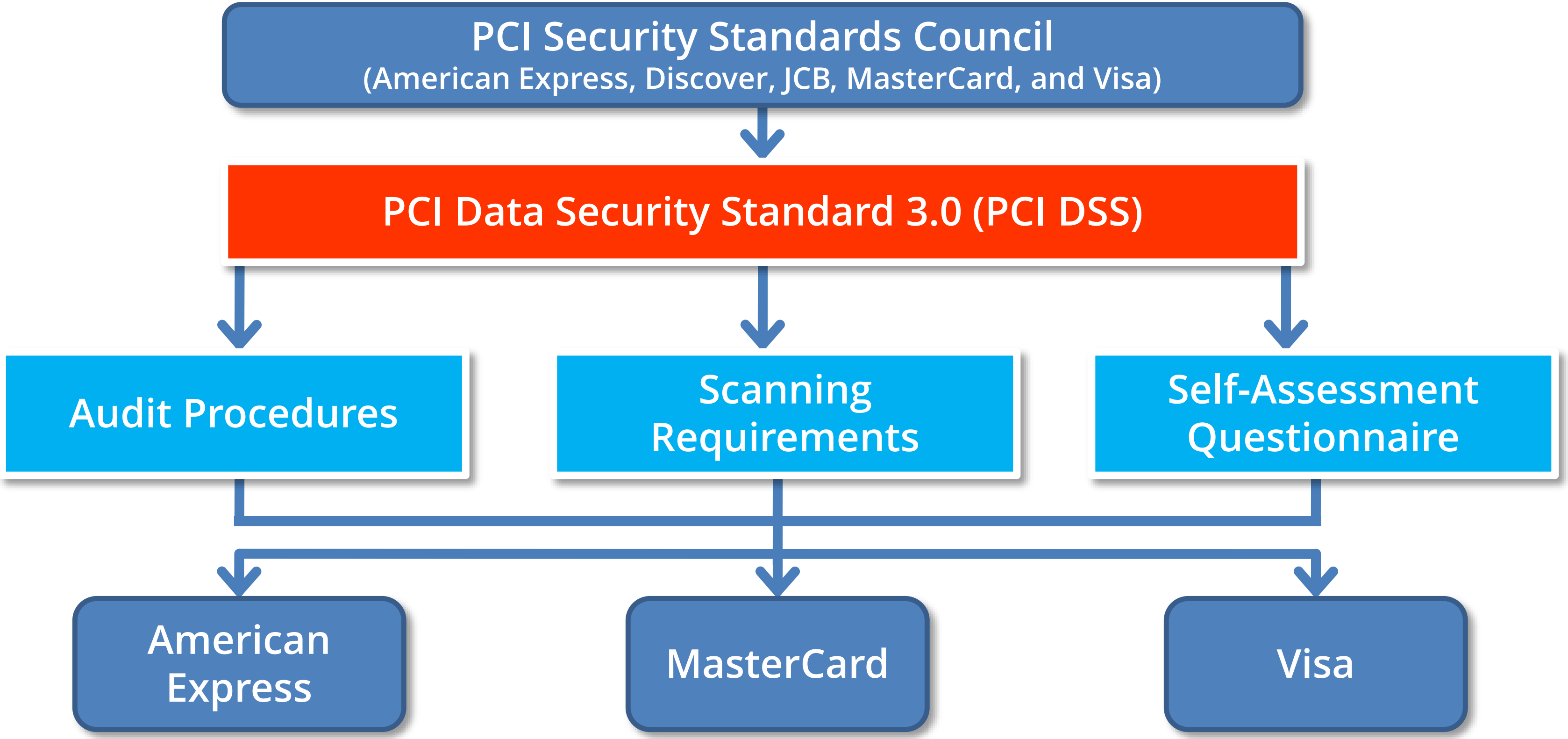
Payment Card Industry (PCI)

- **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 (DSS)** and related documents

- Manages third-party **Qualified Security Assessors** (QSA) and **Approved Scanning Vendors** (ASV)

PCI DSS Structure



PCI Security Standards Council
(American Express, Discover, JCB, MasterCard, and Visa)

PCI Data Security Standard 3.0 (PCI DSS)

Audit Procedures

Scanning Requirements

Self-Assessment Questionnaire

American Express

MasterCard

Visa

PCI Data Security Standard 3.0

- A set of **12 stringent security requirements** for networks, network devices, servers, and applications
  - 200 sub-requirements

- 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 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

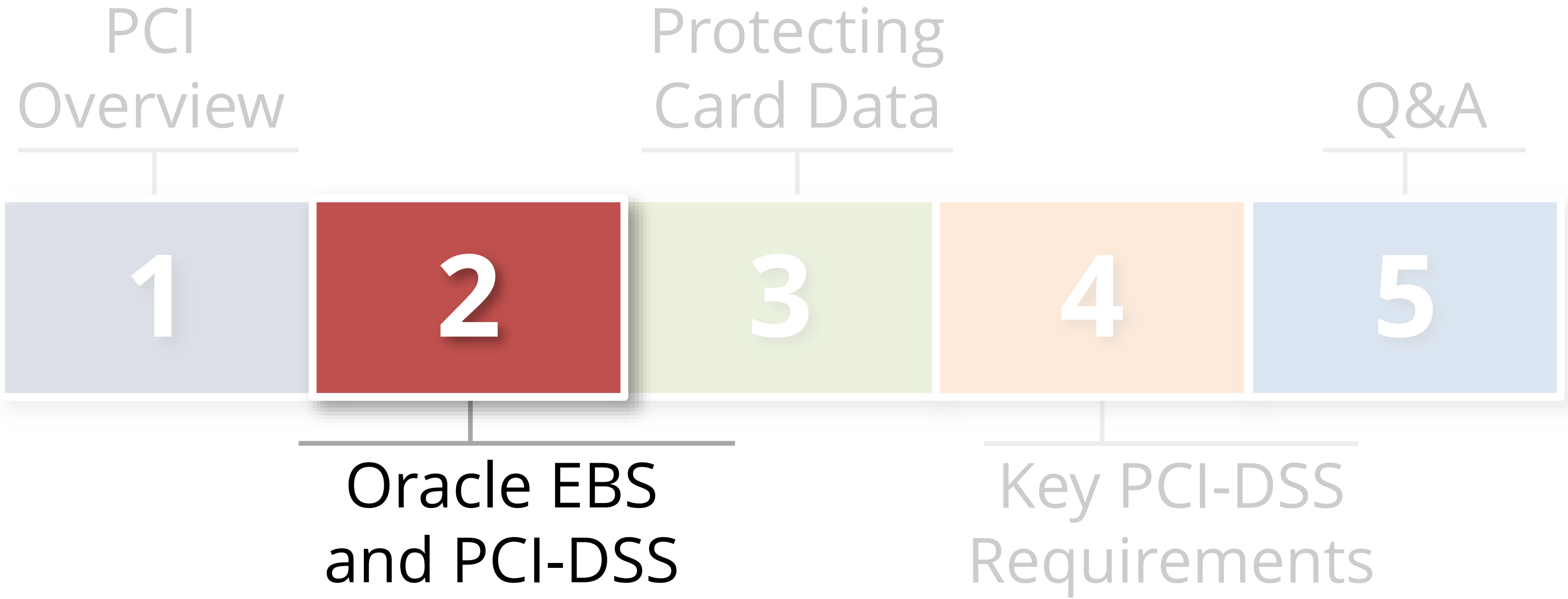
PCI Merchant Compliance Levels

Transactions per Year	Level	Compliance Requirement
6,000,000+	**1**	▪ Annual on-site security assessment ▪ Quarterly Internet-facing network scan
1,000,000 to 6,000,000	**2**	▪ Annual PCI self-assessment (SAQ) ▪ Quarterly Internet-facing network scan
20,000 to 1,000,000 **e-Commerce (only)**	**3**	▪ Annual PCI self-assessment (SAQ) ▪ Quarterly Internet-facing network scan
< 20,000 e-Commerce **< 1,000,000 Total**	**4**	▪ Annual PCI self-assessment (SAQ) and/or quarterly network scan if required by acquiring bank

Determine merchant compliance level with acquiring bank. Exact transaction per year requirements vary by card brand (VISA, MasterCard, Amex)

All 12 PCI DSS requirements are mandatory regardless of merchant compliance level.

Agenda



1

PCI Overview

2

Oracle EBS and PCI-DSS

3

Protecting Card Data

4

Key PCI-DSS Requirements

5

Q&A

All Oracle E-Business Suite environments that **"store, process, or transmit cardholder data"** must comply with the Data Security Standard 3.0 (PCI DSS) regardless of size or transaction volume.

PCI DSS 3.0 – EBS Requirement Mapping

#	Requirement	Network	Server	Database	Oracle EBS	Policy
1	Use Firewall to protect data	✓				✓
2	Do not use vendor-supplied defaults	✓	✓	✓	✓	✓
3	Protect stored cardholder data		✓	✓	✓	✓
4	Encrypt data 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 DSS 3.0 – EBS Compliance Effort

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

🟥 High 🟧 Medium 🟨 Low

PCI DSS Prioritized Approach Milestones

#	Milestone	Key Requirements
1	**Remove sensitive authentication data and limit data retention**	▪ Do no store prohibited data ▪ Purge card data periodically
2	**Protect the perimeter, internal, and wireless networks**	▪ Firewalls, network controls ▪ Secure configurations
3	**Secure payment card applications**	▪ Implement web application firewall ▪ Security patching
4	**Monitor and control access to your systems**	▪ Access control ▪ Logging and monitoring
5	**Protect cardholder data**	▪ Encrypt credit card data
6	**Finalize and ensure all controls in place**	▪ Everything else

Integrigy Recommended EBS PCI Approach

In the context of an overall PCI compliance effect, EBS PCI compliance should address highest security risks and lowest effort PCI DSS requirements first.

#	Approach Phase	PCI DSS Requirements
1	**Encrypt Credit Card Data (3.4)**	▪ Enable native Oracle EBS encryption
2	**Harden EBS Configuration (2.x)**	▪ Secure config for app, db, and app server
3	**Apply Security Patches (6.2)**	▪ Get and stay current with Oracle CPUs
4	**Logging and Monitoring (10.x)**	▪ Enabling auditing and send to logging server
5	**Purge and Scramble (3.1)**	▪ Develop purging and scrambling
6	**Complete EBS PCI Compliance**	▪ Everything else

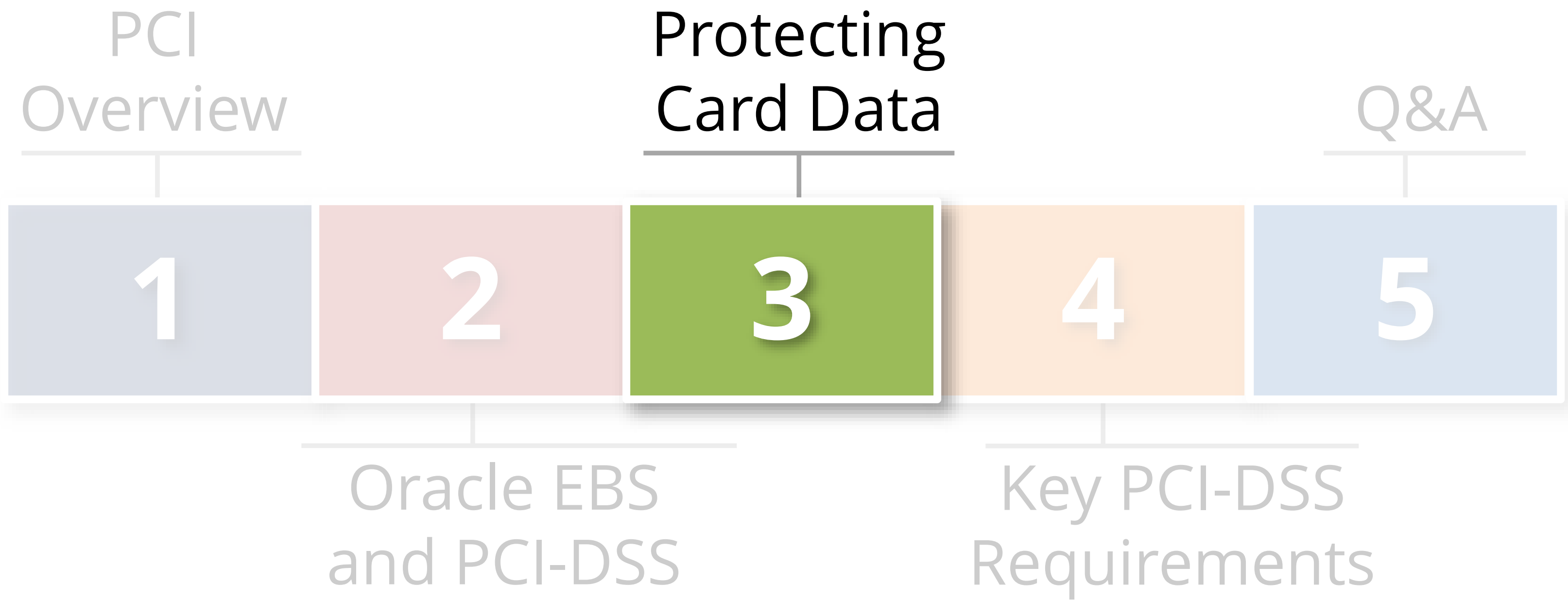
Oracle E-Business Suite and PCI Compliance

- **Standard installation is NOT COMPLIANT**

- **R12 provides new PCI DSS functionality**
  - Supersedes 11i functionality
  - **Disabled by default**

- **PCI compliance in Oracle EBS is not a one-time setup**
  - Maintenance and on-going monitoring required

Agenda



1 PCI Overview

2 Oracle EBS and PCI-DSS

3 Protecting Card Data

4 Key PCI-DSS Requirements

5 Q&A

3. Protect stored cardholder data

"3.4 Render PAN unreadable anywhere it is stored …"

- **By default, PAN stored in clear-text in Oracle EBS**
- **Oracle Payments – Secure Payments Repository – must be enabled to encrypt PAN**
  - Application level encryption using Oracle Wallet
  - Much better option than using Oracle Transparent Data Encryption (TDE)

R12 Oracle Payments

- **Oracle Payments** – new R12 module consolidates all payment activity within Oracle Financials
  - Including processing and storage of credit cards

- **Secure Payments Repository** – part of Oracle Payments
  - Consolidates storage of TCA party external accounts
  - Provides PCI encryption and masking – disabled by default

Oracle Financial Modules Using Secure Payment Repository

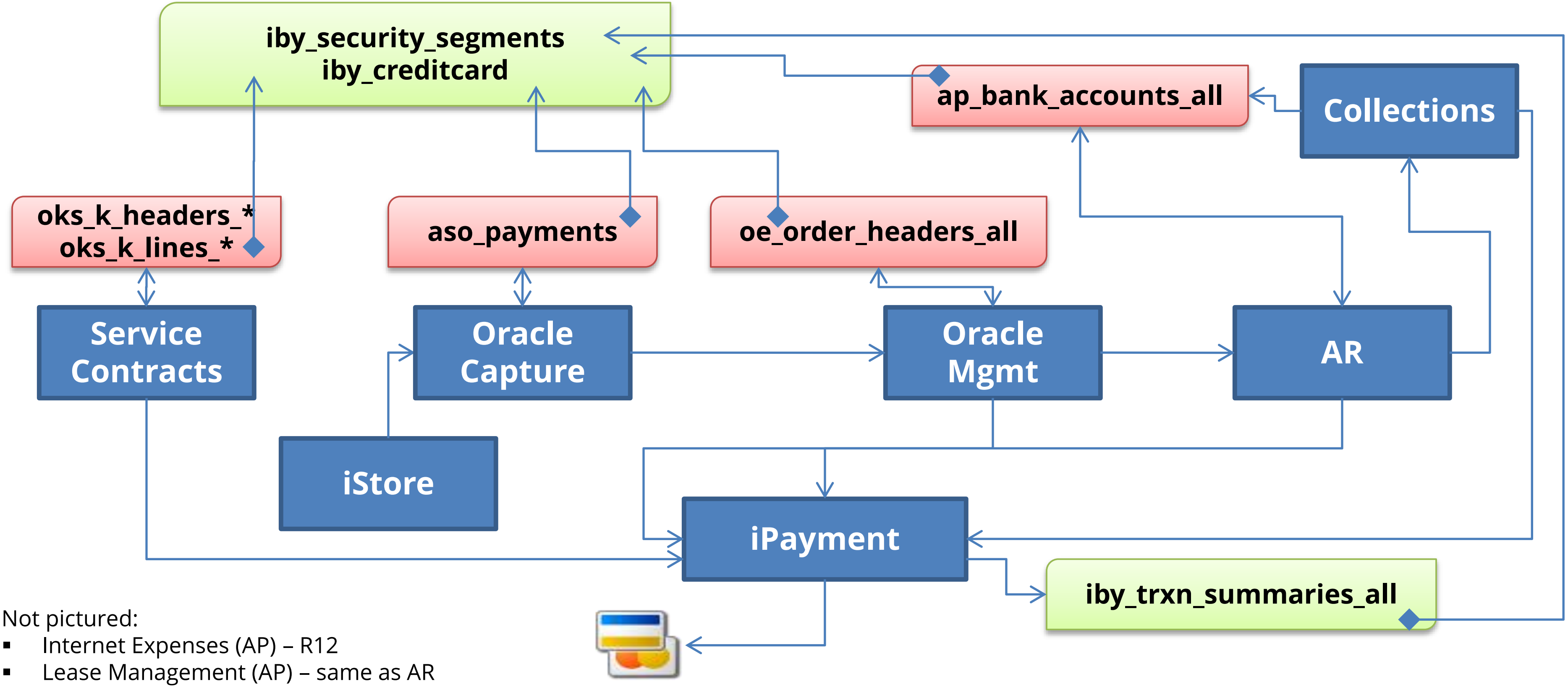
- Oracle Advanced Collections
- Oracle iExpenses
- Oracle iReceivables
- Oracle iStore
- Oracle Order Capture
- Oracle Order Management
- Oracle Partner Management
- Oracle Payables
- Oracle Payments
- Oracle Quoting
- Oracle Service Contracts

Corporate Cards

- **Recommended but not required to be in the scope of PCI DSS compliance**
  - Seek opinion from legal counsel, security and card Issuer

- **iExpense uses Secure Payment Repository as it is part of Payables**
  - Corporate Cards are protected

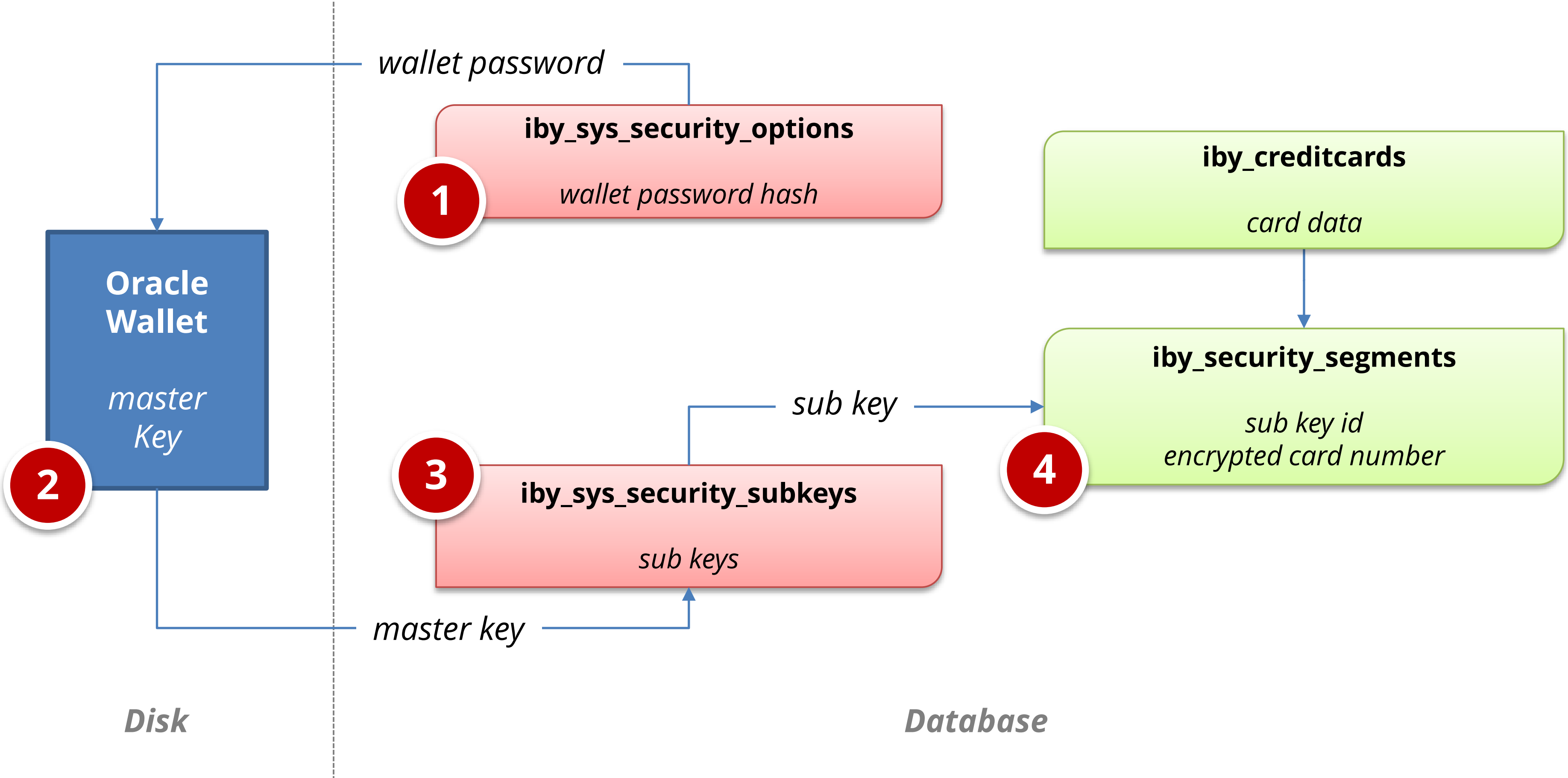
R12 Credit Card Protection (logical)



Not pictured:

- Internet Expenses (AP) – R12
- Lease Management (AP) – same as AR
- Student System (IGS) – IGS patch

R12 Encryption Keys (logical)



Enabling E-Business Credit Card Protection

Three step process to enable encryption

1. Create Payment wallet
2. Set protection configuration options
3. Encrypt existing cardholder data

Step 1 – Create the Payment Wallet

- **Primary PCI requirement is encryption**
  - Creation, use and protection of wallet is critical

- **Considerations**
  - Uses Oracle Wallet technology
  - Can be self-signed or use third party CA
  - Must be placed in a secure location
  - Do not share wallets
  - Restrict access to the Payment wallet password
  - Backup separately and securely

Step 2 – Set Configuration Options

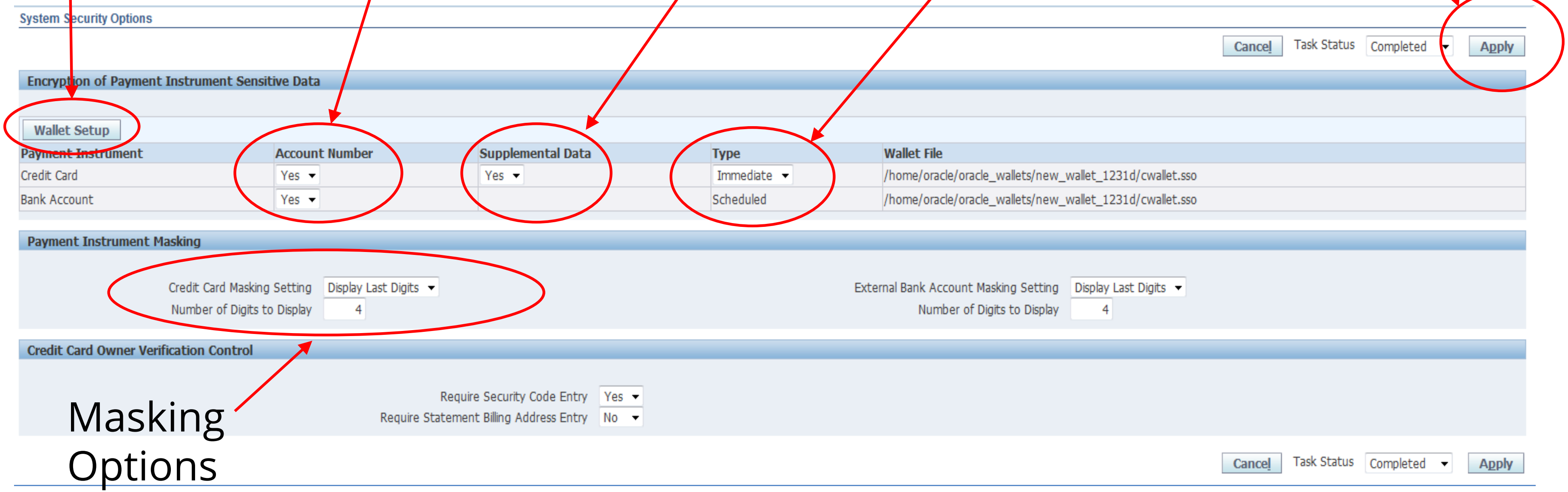
Set Wallet location and password

“Yes” to Encryption

Full or Partial Encryption

Immediate or Scheduled Encryption

Remember to Click Apply



System Security Options

Cancel   Task Status: Completed   Apply

Encryption of Payment Instrument Sensitive Data

Wallet Setup

Payment Instrument	Account Number	Supplemental Data	Type	Wallet File
Credit Card	Yes	Yes	Immediate	/home/oracle/oracle_wallets/new_wallet_1231d/cwallet.sso
Bank Account	Yes		Scheduled	/home/oracle/oracle_wallets/new_wallet_1231d/cwallet.sso

Payment Instrument Masking

Credit Card Masking Setting: Display Last Digits
Number of Digits to Display: 4

External Bank Account Masking Setting: Display Last Digits
Number of Digits to Display: 4

Credit Card Owner Verification Control

Require Security Code Entry: Yes
Require Statement Billing Address Entry: No

Cancel   Task Status: Completed   Apply

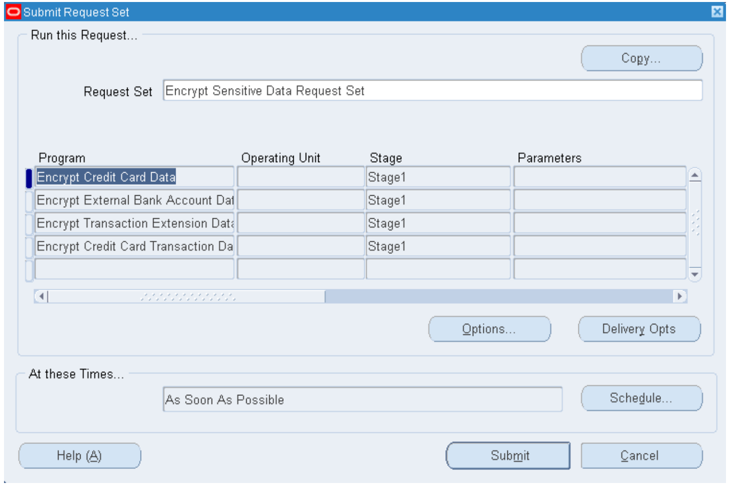
Masking Options

Step 3 – Encrypt Existing Cardholder Data

- Existing cardholder data will not be automatically encrypted

- To encryption run request set ‘Encrypt Sensitive Data Request Set”

- If using full encryption must also run “Upgrade Encrypted Credit Cards’



Request Set: Encrypt Sensitive Data Request Set

Program	Operating Unit	Stage	Parameters
Encrypt Credit Card Data		Stage1	
Encrypt External Bank Account Dat		Stage1	
Encrypt Transaction Extension Data		Stage1	
Encrypt Credit Card Transaction Da		Stage1	

As Soon As Possible

3. Protect stored cardholder data

- **3.4 – Must find ALL locations of credit card data**

- **3.4 – Storing of card data in logs is a major issue**
  - Look at other log files such as Oracle Payments and Apache

- **3.1 – Review existing data archiving and purging**
  - Credit card data retention should be less than 18 months
  - No Oracle supported purging available -- custom solution required
  - Do not mean entire transaction, just card number

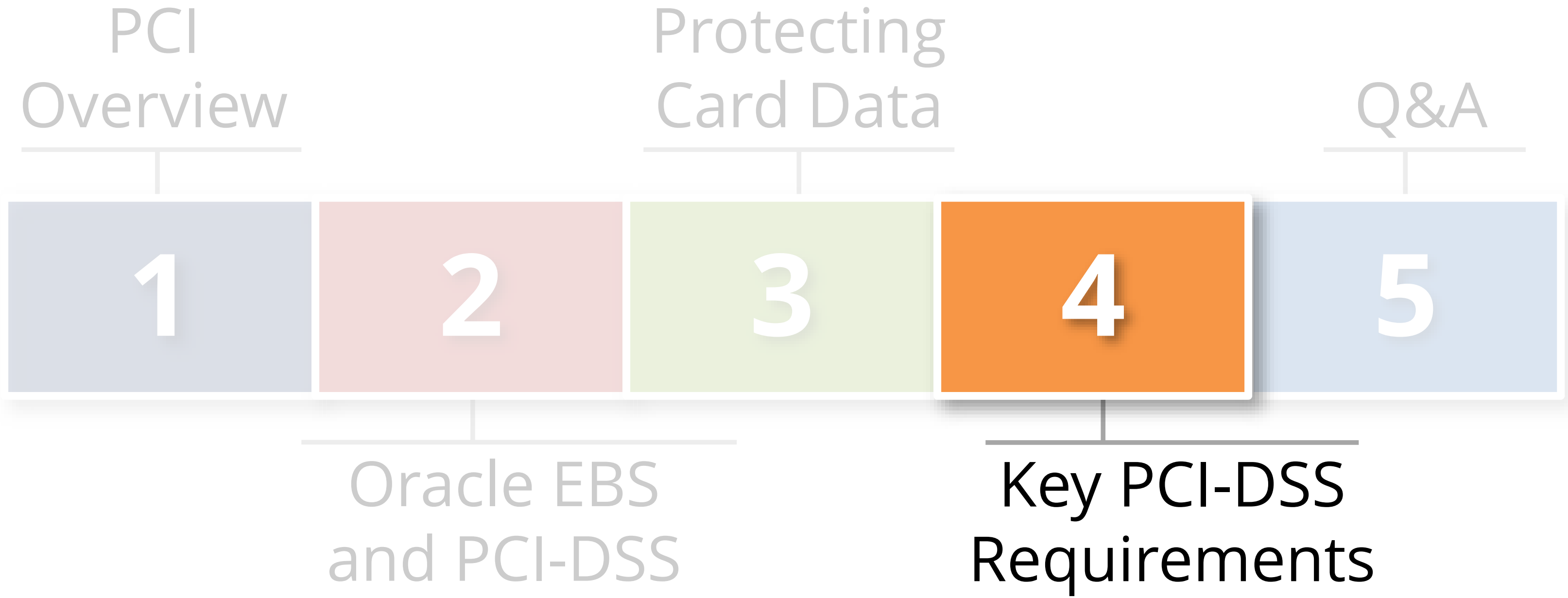
Where else might be Credit Card Data?

- **Custom tables**
  - Customizations may be used to store or process credit card data
- **“Maintenance tables”**
  - DBA copies tables to make backup prior to direct SQL update
  - iby.iby_security_segments_011510
- **Interface tables**
  - Credit card numbers are often accepted in external applications and sent to Oracle EBS
- **Interface files**
  - Flat files used for interfaces or batch processing
- **Log files**
  - Log files generated by the application (e.g., Oracle Payments)

Test and Development Instances

- **6.4.3** – No production or “live” cardholder data allowed for test or development
- **3.5** – Protection of encryption keys
- **Building non-production instances**
  1. Production payment wallet rotated and securely wiped
  2. Location of Payment wallet reset
  3. Remove, purge and/or scramble production cardholder data

Agenda



1 PCI Overview

2 Oracle EBS and PCI-DSS

3 Protecting Card Data

4 Key PCI-DSS Requirements

5 Q&A

2. Do not use vendor-supplied defaults

- **2.1 – Change all default settings**
  - Default database passwords
  - Default seeded application passwords

- **2.2 – A configuration standard is required**
  - Use Oracle's Secure Configuration Guide for Oracle EBS

- **2.3 – All administrator network traffic must be encrypted, consequently, all network traffic must be encrypted**
  - SSL, SSH, SQL*Net encryption

6.2 Develop and maintain secure apps

- **Oracle Critical Patch Updates (CPU) should be applied within 30-90 days!**

"6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches <u>within one month of release</u>."

"Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months)."

6.6 Protect EBS Internet Modules

- **External Oracle EBS modules (iSupplier, iStore, iRecruitment, iSupport) must be protected by –**
  - Annual penetration tests or
  - Web application firewall (WAF)

- **Significant cost to deploy WAF just for Oracle EBS**
  - Existing WAF not optimized for Oracle EBS and not specific rules
  - WAF rules must be developed for Oracle EBS

- **Integrigy AppDefend WAF**
  - WAF highly optimized for Oracle EBS
  - Satisfies PCI-DSS 6.6 requirements
  - Provides support for application logging requirements (10.x)

8. Assign 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 EBS due to the design and complexity**
  - Use of the generic, privileged accounts (APPS, 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, APPS, 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, APPS***
- 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 10.2.4 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 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 EBS install has 500,000+ files
  - Multiple configuration files and logs can make deploying file integrity monitoring challenging
  - R12 $INST_TOP improves monitoring situation

Periodic PCI DSS Tasks

Task	Requirement
Daily Log Review	10.6
Monthly Card Expiration Status Update (If Using Full Encryption)	3.4
Every 90 Days Disable Inactive Users and Change User Passwords	8.2.4 8.1.4
Quarterly Internal and External Vulnerability Scans	11.2
Purge PAN Data regularly	3.1
Rotate Wallet Keys Annually	3.6
Annual Application Penetration Test	11.3

On Going PCI DSS Tasks

Task	Requirement
Backups and Payment Wallet Protection	3.5
Remove production cardholder data and encryption keys from non-production instances	6.4.3 3.5
Restrict Access to and Manage Wallet Keys	3.5
Masking and Viewing Cardholder data in Clear Text	3.3
Keep Cardholder data out of Log Files	3.4
Disable and Monitor Decryption Concurrent Programs	3.4
Monitor for PCI Configuration Changes and Decryption	3.4 3.3
Review customizations for PCI security	6.3/6.4.4

Agenda

1 PCI Overview

2 Oracle EBS and PCI-DSS

3 Encrypting Card Data

4 Key PCI-DSS Requirements

5 Q&A

Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**