INTEGRIGY

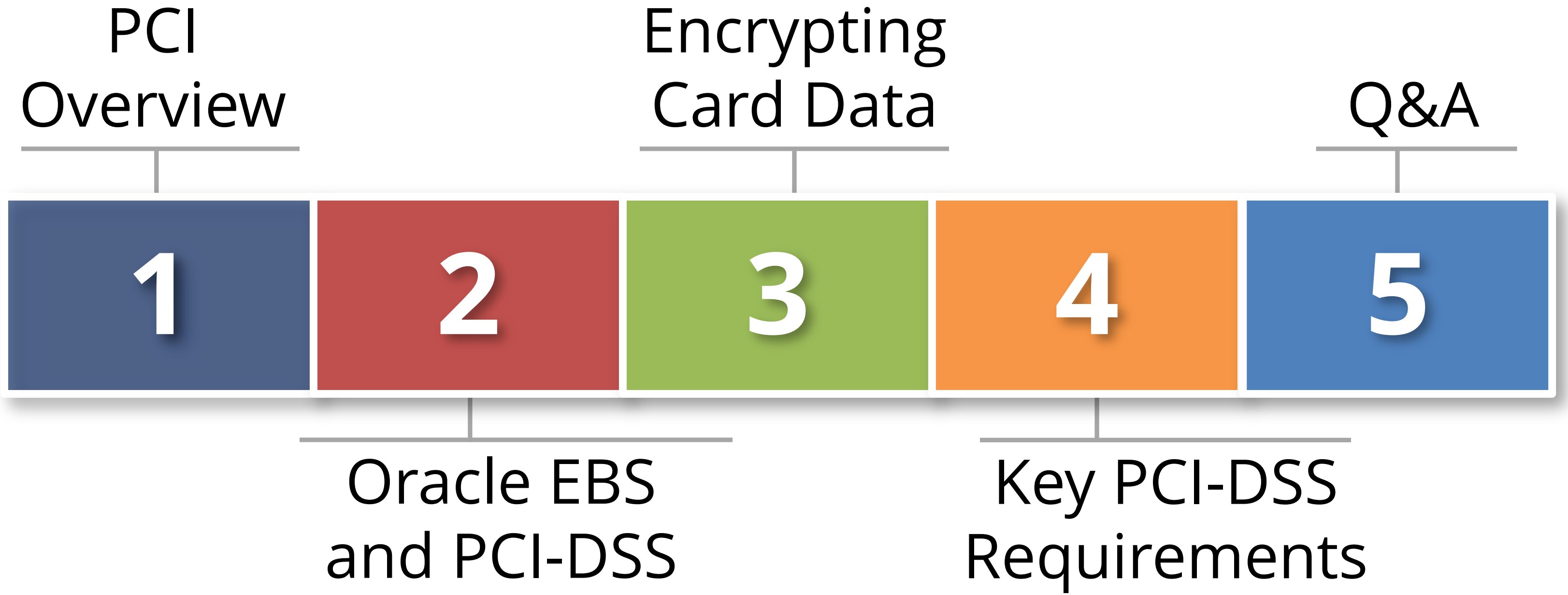
Credit Cards and Oracle E-Business Suite
Security and PCI Compliance Issues

August 16, 2012

Stephen Kost
Chief Technology Officer
Integrigy Corporation

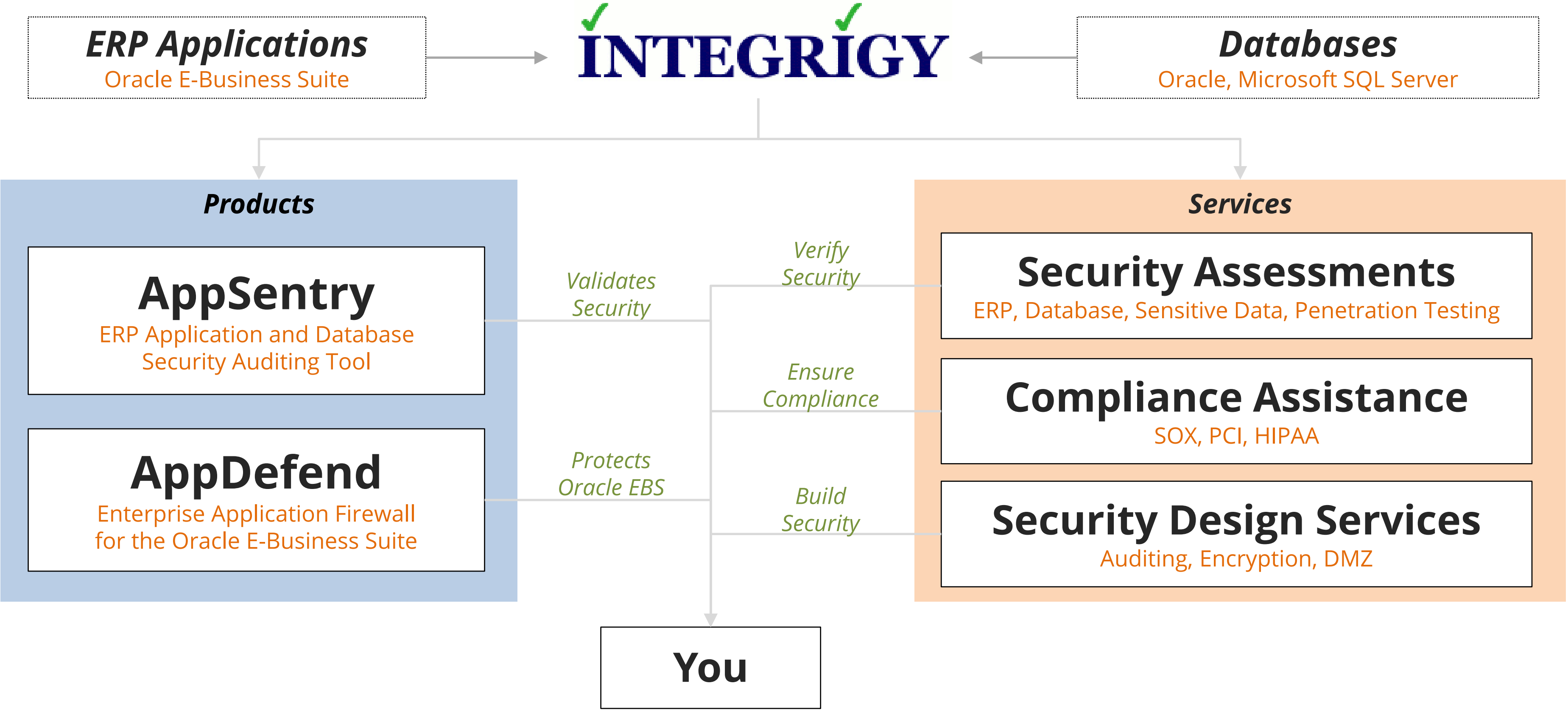
Phil Reimann
Director of Business Development
Integrigy Corporation

Agenda



1. PCI Overview
2. Oracle EBS and PCI-DSS
3. Encrypting 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

Services

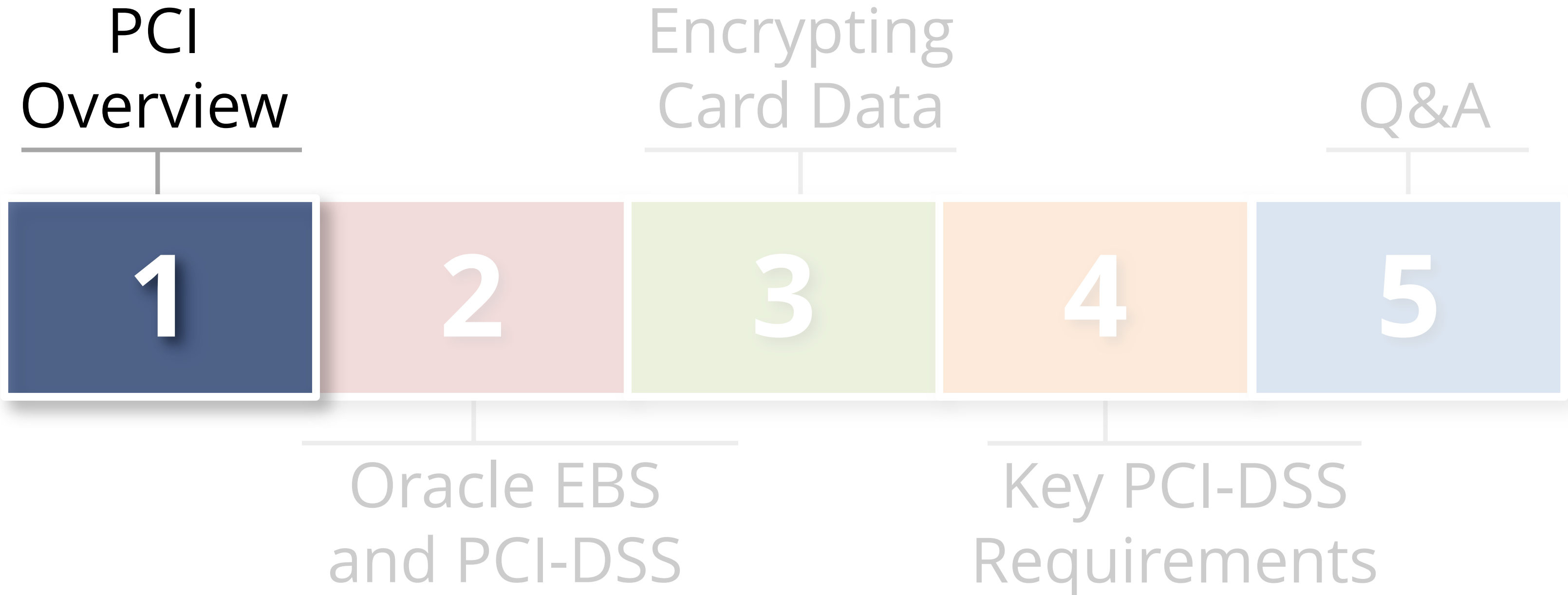
Security Assessments
ERP, Database, Sensitive Data, Penetration Testing

Compliance Assistance
SOX, PCI, HIPAA

Security Design Services
Auditing, Encryption, DMZ

You

Agenda



1 PCI Overview

2 Oracle EBS and PCI-DSS

3 Encrypting 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

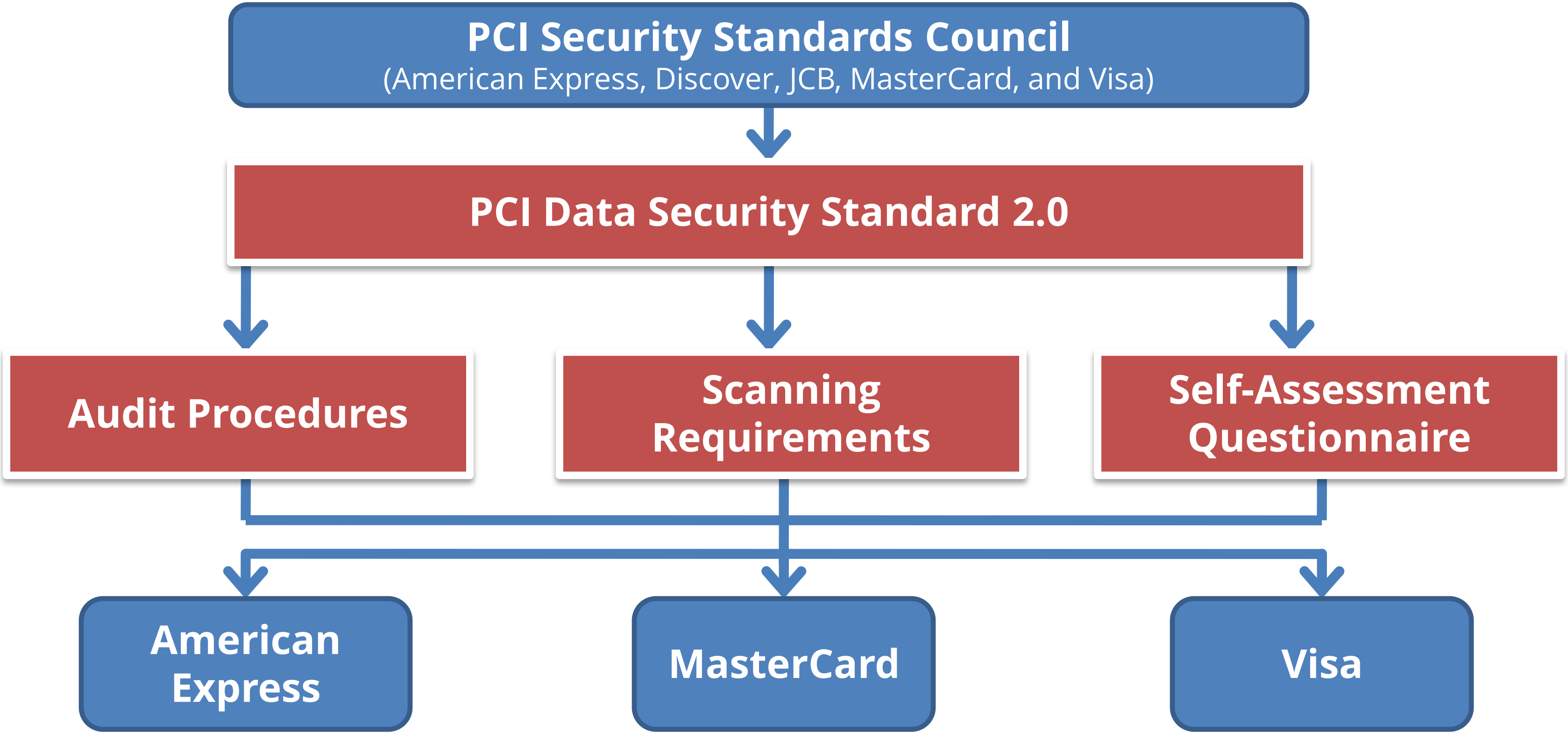
- Publishes "**Data Security Standard (DSS)**" and related documents

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

PCI Data Security Standard 2.0

- 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 DSS Structure



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

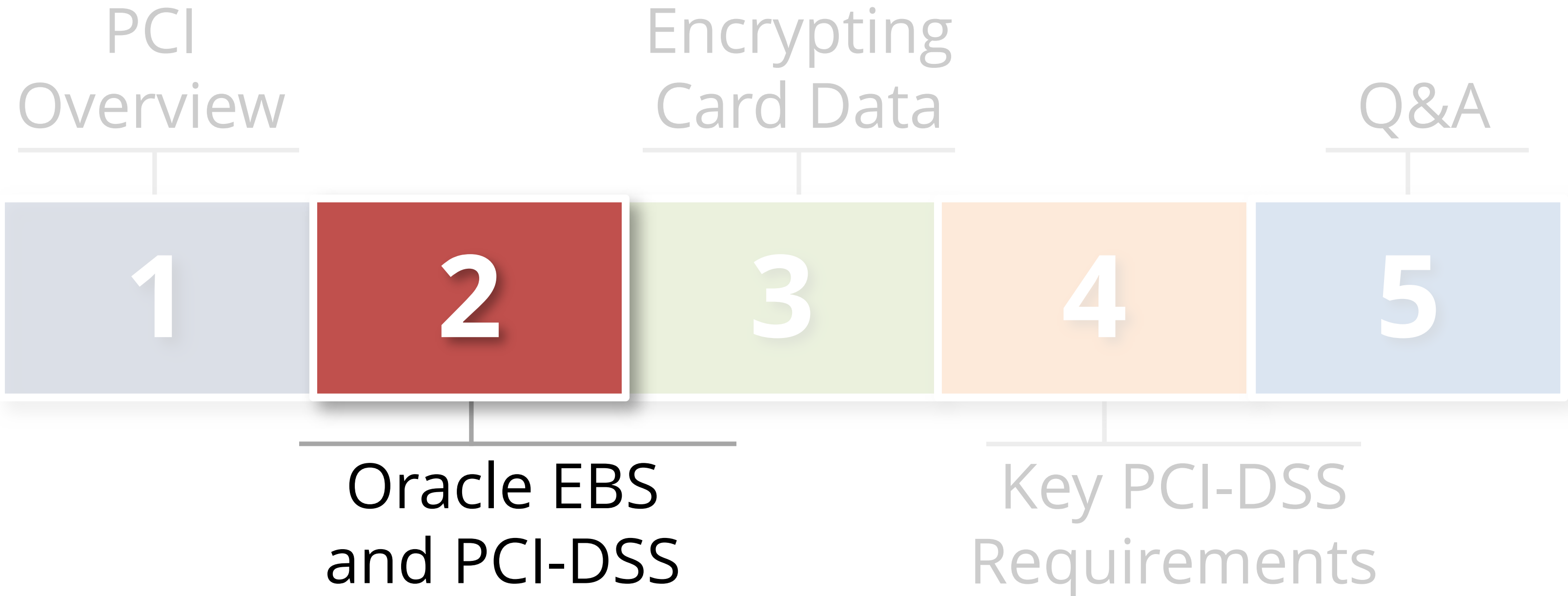
- **Compliance is dependent on card brand, merchant type (ecommerce), and transactions**
  - On-site assessment
  - Quarterly external scans
  - Self-assessment questionnaire (through Acquirer)
  - Depending on card brand, may be required to submit documentation
- **In case of a data breach, compliance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

PCI 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 ▪ Quarterly Internet-facing network scan
20,000 to 1,000,000 e-Commerce (only)	**3**	▪ Annual PCI self-assessment ▪ Quarterly Internet-facing network scan
< 20,000 e-Commerce < 1,000,000 Total	**4**	▪ Annual PCI self-assessment

Exact transaction per year requirements vary by card brand (VISA, MasterCard, American Express)

Agenda



1 PCI Overview

2 Oracle EBS and PCI-DSS

3 Encrypting 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 2.0 (PCI-DSS) regardless of size or transaction volume.

PCI-DSS 2.0 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 2.0 – 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

Credit Cards and Oracle E-Business Suite

- Standard installation is **NOT COMPLIANT**

- Storage of credit card data is by module
- Card number stored un-encrypted
- Masking of card numbers controlled by module specific profile options
- iPayment is payment gateway
  - Oracle Payments in R12

PCI Definition of Bad Things to Do

1. Storage of CVV/CV2 or magnetic strip data
   - Not normally stored in Oracle E-Business Suite
   - 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

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 – Not yet on approved list
  - See Metalink Note ID 984283.1
- **11i and 12.0 will not be PA-DSS compliant**
  - See Metalink Note ID 1101213.1

PCI-DSS Prioritized Approach (1-6)

1 – Do not store prohibited data

2 – Secure configuration

3 – Web application firewall

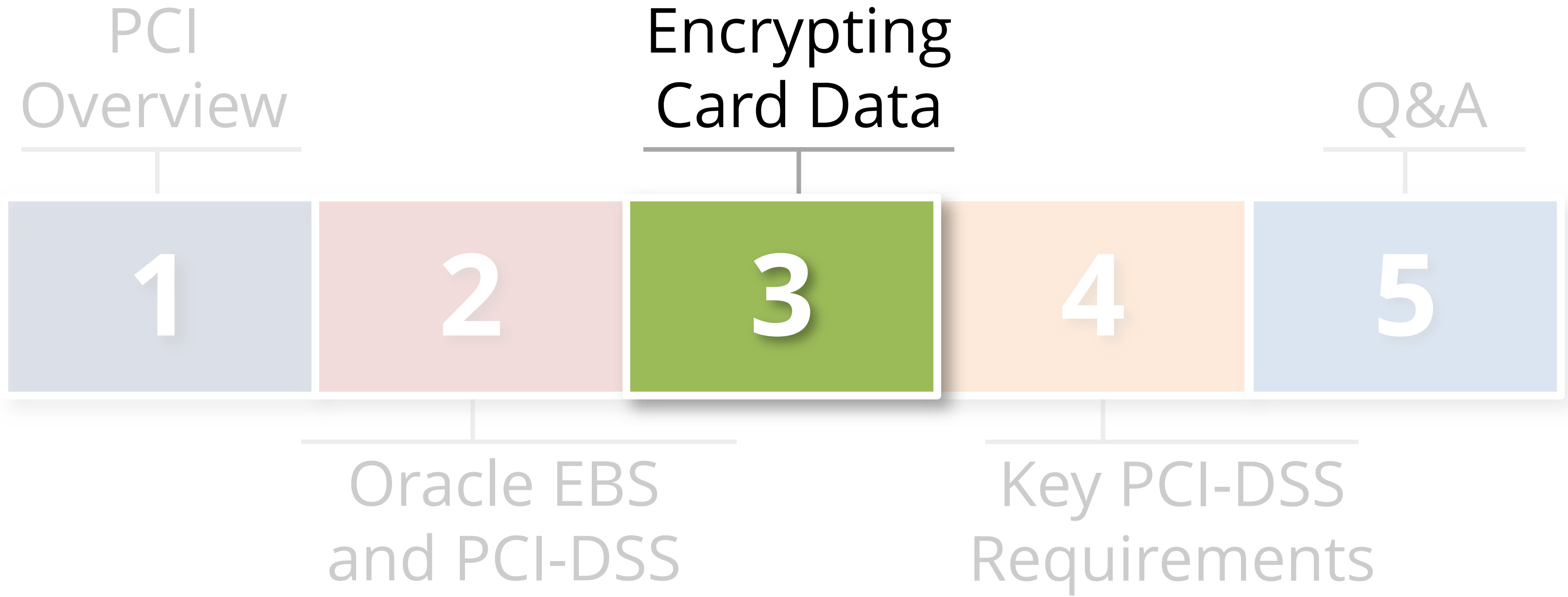
3 – Security patching

4 – Access Control

4 – Logging and monitoring

5 – Encrypt credit card data

Agenda



1 PCI Overview

2 Oracle EBS and PCI-DSS

3 Encrypting Card Data

4 Key PCI-DSS Requirements

5 Q&A

Credit Card Number Encryption

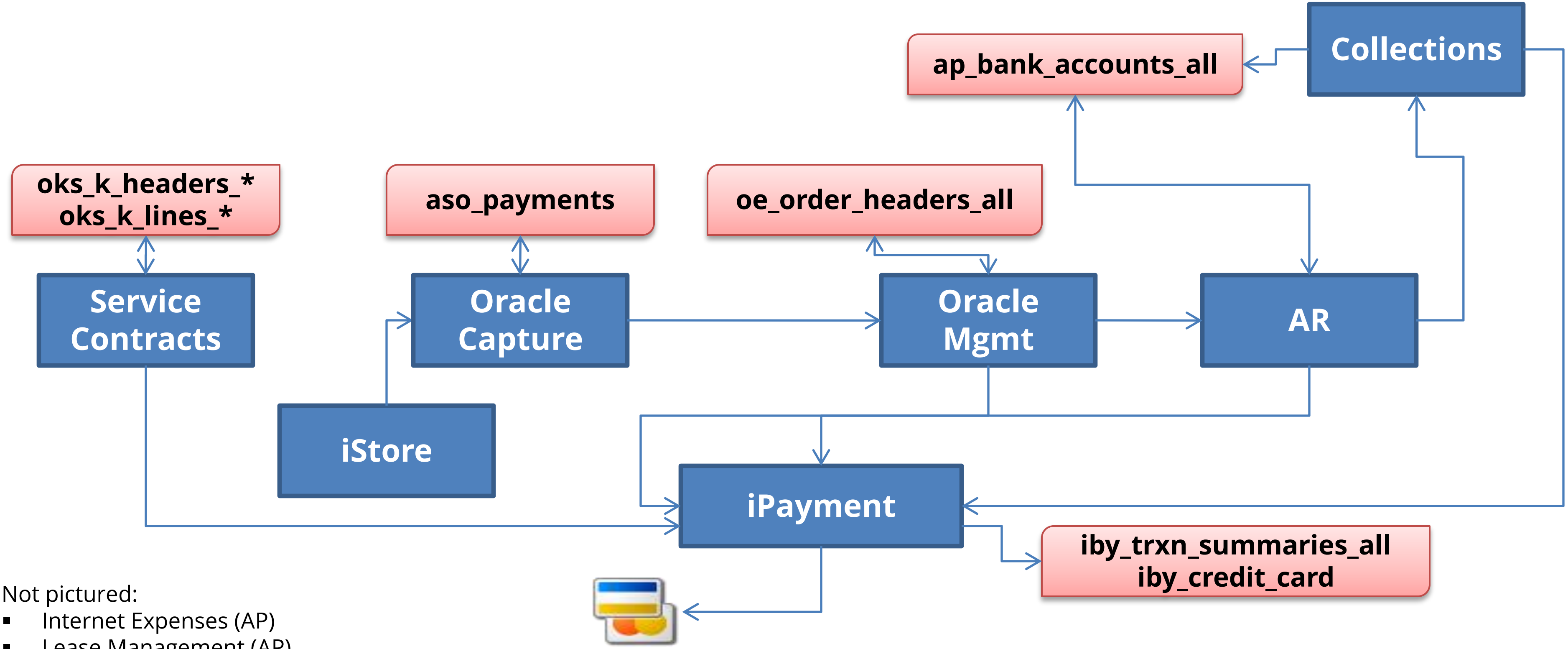
- **Use the Oracle E-Business Suite encryption**
  - Application-level encryption
  - Better solution than other technologies such as Oracle Transparent Data Encryption (TDE)

- **Metalink Note ID 338756.1, Patch 4607647**
  - Consolidates card numbers into IBY_SECURITY_SEGMENTS table
  - Encrypts card numbers in IBY_SECURITY_SEGMENTS
  - Uniform masking of card numbers
  - Significant functional pre-requisites (11.5.10.2)

Oracle Credit Card Encryption Solution

- **Implementation of “FND Vault” for secure data storage**
  - Key chain used (FND Vault Key -> Application Generated Key -> Data)
- **Consolidation of credit card numbers into a single table**
- **All access to credit card number replaced with one of the following –**
  1. Package to decrypt/encrypt card number
  2. Hashes used for searching/matching card numbers

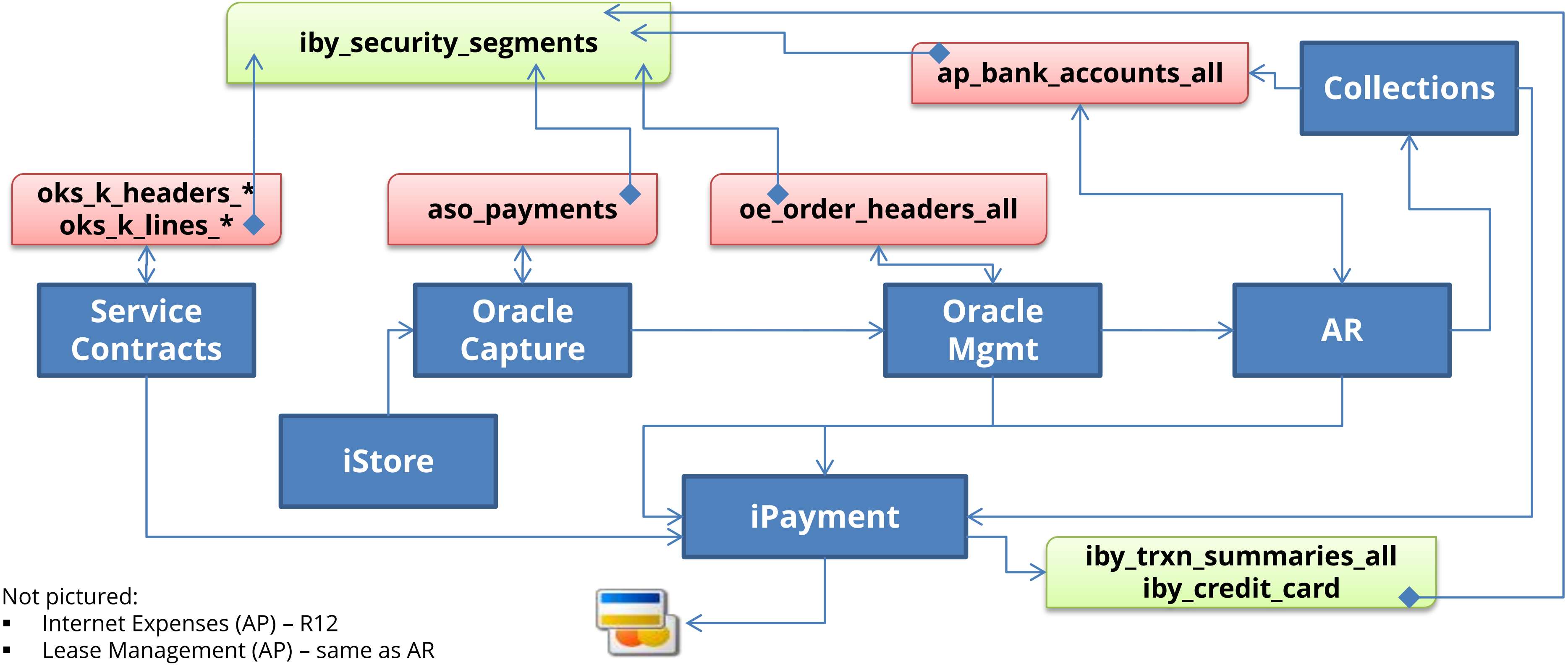
Oracle E-Business Suite and Credit Cards



Not pictured:

- Internet Expenses (AP)
- Lease Management (AP)
- Student System (IGS)

Credit Card Encryption Patch



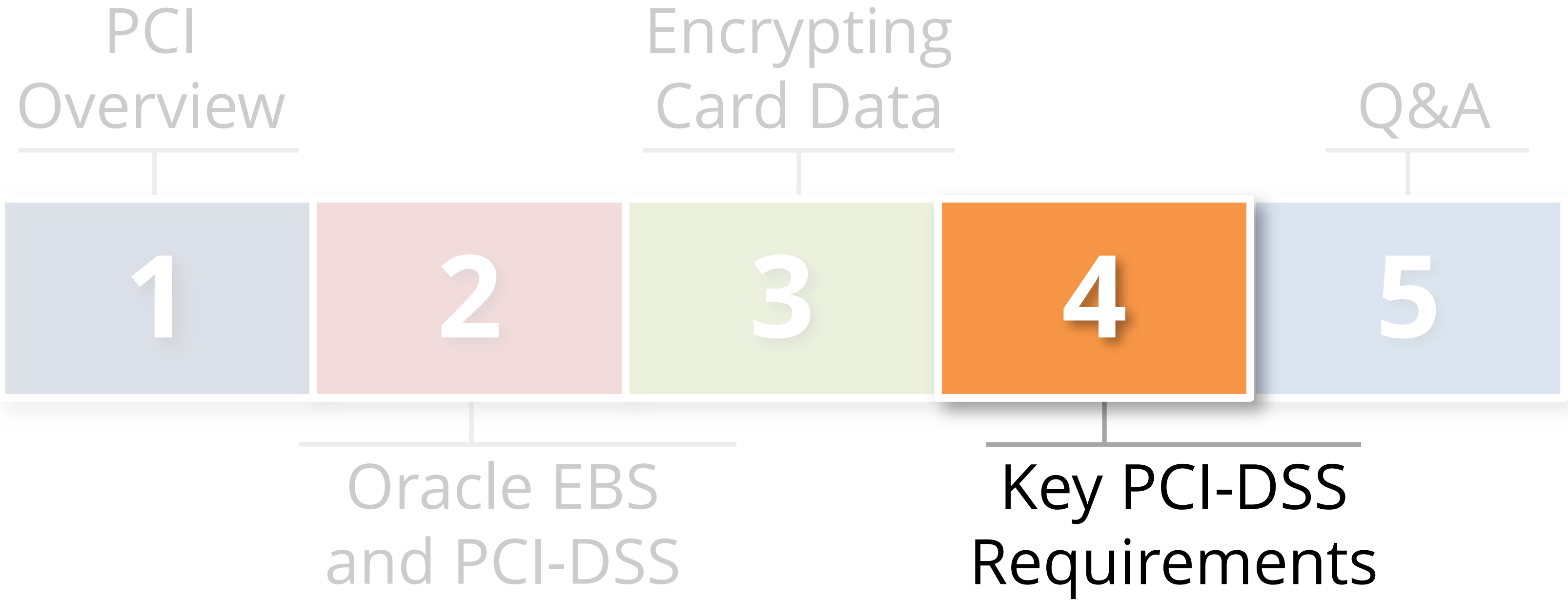
Not pictured:

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

Where else might be Sensitive Data?

- **Custom tables**
  - Customizations may be used to store or process sensitive 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., iPayment)
- **Oracle EBS Flexfields**
  - It happens – very hard to find

Agenda



1 PCI Overview

2 Oracle EBS and PCI-DSS

3 Encrypting Card Data

4 Key PCI-DSS Requirements

5 Q&A

2. Do not use vendor-supplied defaults

- **Change all default settings**
  - Default database passwords
  - Default seeded application passwords
- **A configuration standard is required**
  - Use Oracle's Secure Configuration Guide for Oracle EBS
- **All administrator network traffic must be encrypted, consequently, all network traffic must be encrypted**
  - SSL, SSH, SQL*Net encryption

3. Protect stored cardholder data

- **Must find ALL locations of credit card data**
- **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
  - No Oracle supported purging available
  - Custom solution required
  - Do not mean entire transaction, just card number
- **Must scramble card data in development and test**
  - Even if encrypted or hashed, must be scrambled
  - No Oracle supported scrambling available

6.1 Develop and maintain secure apps

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

"6.1 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."

6.6 Protect Internet-facing Applications

- **iSupplier, iStore, iSupport, etc. must be protected by one of the following -**
  - Annual penetration tests
  - 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

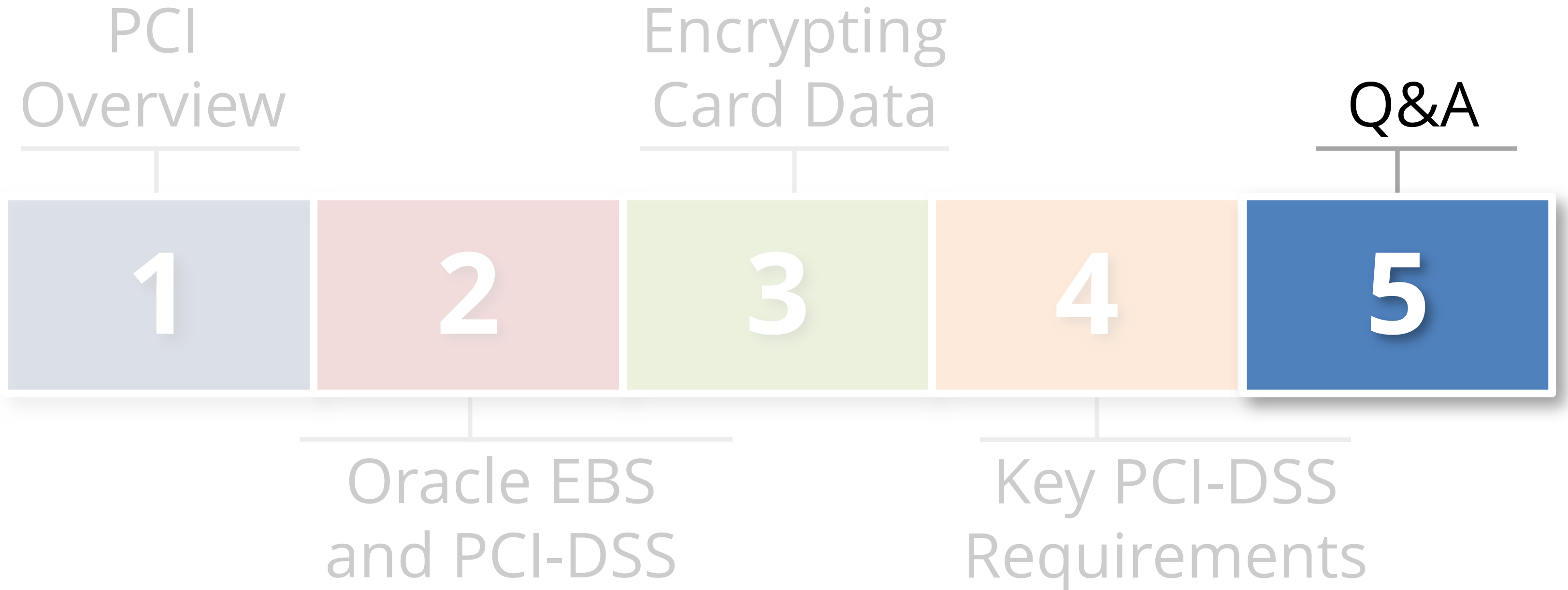
Audit	PCI #	Description	Daily Volume
Session	10.2.1 10.2.4 10.2.5	Connections to the database including failed logins (ora-1017)	10,000+
User	10.2.2	Creation, altering, and dropping of database user accounts	0
System audit	10.2.3	Changes to the database auditing	0
System grant	10.2.2	Grants to system 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

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**