



Oracle Applications  
Technologies *Experts.* dba

# Considerations for PCI Compliance in Oracle Application R12

Fred DeAngelis  
Managing Partner, ORAdba LLC

401-965-6202, [fred.deangelis@oradba.com](mailto:fred.deangelis@oradba.com)

# Agenda

- Introductions
- Defining The Problem
- What You Should Get From This
- Presentation Approach
- PCI Requirements and Responses
- Summary

# Defining the Problem

Securing Payment Card Information  
Stored on disk, tape, thumb drives  
Printed and displayed  
Cloned to other instances  
Processed by humans

# Defining the Problem

## Scope

Enterprise policies

Business unit applications, processes and procedures

Technology including operations

Data presentation, retention and handling

# What You Should Get From This

Understanding of seeded PCI compliance capabilities in R12

Appreciation for implementation effort

Direction on how to plan for implementation

# What You Should Get From This

Note: Not all requirements or responses are discussed

# Presentation Approach

Review applicable Payment Card Industry (PCI) Data Security Standard (DSS)

Identify seeded R12 capabilities that can satisfy requirements

Note: Some responses will involve configuration of the technology stack

# PCI Requirements and Responses

## Build and Maintain a Secure Network

### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

**1.1.5 Documented list of services and ports necessary for business**

**Provide the list of all ports used by the Oracle Applications instance and its technology stack to your network administrator. These ports can then be added to the allowed port list and the network configured to accept connections for allowed ports.**

**The complete installation, including the list of all ports assigned to an Oracle Applications instance, can be found in the config.txt file created by the Universal Installer. The location and name of this file is specified during the Installer session.**

**For example**

**`/u01/app/oracle/PROD/config.txt`**

# PCI Requirements and Responses

## Build and Maintain a Secure Network

### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

1.1.6 Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)

Oracle Applications Protocols include

TNS

IP

TCP/IP

HTTP

HTTPS

TCF

Oracle Net Services (integration)

FTP (development, integration)

SSH (integration)

Telnet

JDBC

IIOF

See Security Fundamentals for Oracle E-Business Suite, John Abel, 226 276-1,

[www.oracle.com/technology/books/pdfs/ebs-security-ch1.pdf](http://www.oracle.com/technology/books/pdfs/ebs-security-ch1.pdf)

# PCI Requirements and Responses

## Build and Maintain a Secure Network

### Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

1.1.7 Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented

FTP – is identified as a possible protocol that could be used to transfer files between Oracle and an external system (e.g. interfaces). Consider other utilities (e.g. Secure File Transfer Protocol) instead of FTP.

# PCI Requirements and Responses

## Build and Maintain a Secure Network

### Requirement 2: Don't Use Vendor Supplied Defaults - System Passwords, Other Security

2.1 Always change vendor-supplied defaults before installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).

During installation specify ports other than those provided as defaults (e.g. port pool). After installation port change is more complicated but possible.

Use FNDCPASS to change default database and Oracle Applications passwords.

Use 'alter user <username> identified by <new password>' to change a database user's password directly.

Drop/expire unused default database and Oracle Applications accounts (e.g. Scott/Tiger)

Oracle locks and expires default accounts and passwords during installation. Passwords for administration accounts are prompted for during installation.

# PCI Requirements and Responses

## Build and Maintain a Secure Network

Requirement 2: Don't Use Vendor Supplied Defaults - System Passwords, Other Security

**2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the devices' specified function)**

**Disable or prohibit from starting all unused Oracle services such as the following:**  
**Forms Metric Server**  
**Forms Metric Client**  
**Discoverer Server**  
**JTF**

# PCI Requirements and Responses

## Build and Maintain a Secure Network

Requirement 2: Don't Use Vendor Supplied Defaults - System Passwords, Other Security

**2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.**

**Only licensed and used Oracle Applications products are installed and configured.**

**Unnecessary installation logs, backed up files and other byproduct from the installation and patching are removed.**

**Oracle Database custom installation allows specific components to be installed or removed.**

# PCI Requirements and Responses

## Protect Cardholder Data

### Requirement 3: Protect Stored Cardholder Data

3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches:

Strong one-way hash functions (hashed indexes)

Truncation

Index tokens and pads (pads must be securely stored)

Strong cryptography with associated key management processes and procedures.

The **MINIMUM** account information that must be rendered unreadable is the PAN.

#### Primary Account Number (PAN)

iPayment, beginning with a patch available in 11i, encrypts credit card data. Reference Note: 338756.1, *Oracle Applications Credit Card Encryption, Release 11i*, 24-Aug-2007

# PCI Requirements and Responses

## Protect Cardholder Data

### Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

4.1 Use strong cryptography and security protocols such as secure sockets layer (SSL) / transport layer security (TLS) and internet protocol security (IPSEC) to safeguard sensitive cardholder data during transmission over open, public networks.

**Metalink Note: 391248.1, *Encrypting Oracle E-Business Suite Release 11i Network Traffic using Advanced Security Option and Advanced Networking Option*, 16-Jul-2008**, specifies how to setup encryption for network traffic using Transparent Network Substrate (TNS) protocol. For R21 only the sqlnet.ora configuration is required.

Add the following 3 lines to the sqlnet.ora files:  
SQLNET.ENCRYPTION\_SERVER=REQUIRED  
SQLNET.CRYPTO\_SEED =  
'About72charactersOfSuperSecretSeed'  
SQLNET.ENCRYPTION\_TYPES\_SERVER= (AES256,  
AES192, 3DES168)

**Metalink Note: 376700.1, *Enabling SSL in Release 12*, 03-Nov-2008 in *Appendix A***, provides information on setting up SSL.

# PCI Requirements and Responses

## Maintain a Vulnerability Management Program

### Requirement 6: Develop and Maintain Secure Systems and Applications

**6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of their release.**

**Policy: Oracle delivers Critical Patch Updates (CPUs) quarterly. Apply these within 30 days of their release. Follow similar procedure for OS, network, backup systems.**

# PCI Requirements and Responses

## Maintain a Vulnerability Management Program

### Requirement 6: Develop and Maintain Secure Systems and Applications

**6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.**

**Policy: Examine Metalink for 'High/Security' patches for all installed products weekly and apply them within 30 days.**

**Subscribe to the 'Electronic Subscriptions' section on OTN and be sure to check the box next to the Oracle Security Alerts and click 'Continue' to confirm.**

# PCI Requirements and Responses

## Implement Strong Access Control Measures

### Requirement 8: Assign a Unique ID to Each Person with Computer Access

**8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use**

**By default the user is required to change their password after it has been reset by an administrator.**

**Create Oracle database account with password expired.**

# PCI Requirements and Responses

## Implement Strong Access Control Measures

Requirement 8: Assign a Unique ID to Each Person with Computer Access

**8.5.9 Change user passwords at least every 90 days**

**Password expiration can be set in Oracle Applications in the Users screen accessed with the System Administrator responsibility.**

# PCI Requirements and Responses

## Implement Strong Access Control Measures

Requirement 8: Assign a Unique ID to Each Person with Computer Access

**8.5.10 Require a minimum password length of at least seven characters**

The following system profile option can be used.

**Signon Password Length** – sets minimum password length (default 5)

# PCI Requirements and Responses

## Implement Strong Access Control Measures

Requirement 8: Assign a Unique ID to Each Person with Computer Access

**8.5.11 Use passwords containing both numeric and alphabetic characters**

The following system profile option can be used.

**Signon Password Hart to Guess** – requires at least 1 letter and 1 number, cannot contain the username, and does not contain any repeating characters.

# PCI Requirements and Responses

## Implement Strong Access Control Measures

Requirement 8: Assign a Unique ID to Each Person with Computer Access

**8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts**

The following system profile option can be used.

**Signon Password Failure Limit** – sets limit on maximum failed login attempts before account is disabled

# PCI Requirements and Responses

## Implement Strong Access Control Measures

Requirement 8: Assign a Unique ID to Each Person with Computer Access

**8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal**

**The following system profile option can be used.**

**ICX:Session Timeout – specified allowed idle time before causing a timeout**

# Summary

Address compliance beginning with the enterprise and work down to business units, technology, and then data

Consider seeded R12 capabilities as a fast, easy, partial response

Use the PCI Data Security Standard (DSS) as a guide through implementation

# References

*Oracle Retail Point-Of-Service payment Card Industry (PCI) Compliance Issues*, Oracle Note: 415363.1

Oracle Technology Network document *Oracle Database Security and the Payment Card Industry Data Security Standard (10g and 11g)*

Oracle Corporation Document *Best Practices for Securing Oracle E-Business Suite Release 12, Version 1.0.0*

PCI Security Standards Council document *Payment Card Industry (PCI) Data Security Standard, Version 1.2*



Oracle Applications  
Technologies *Experts.* dba