INTEGRIGY

WHITE PAPER

# Oracle E-Business Suite: Credit Cards and PCI Compliance

APRIL 2016

# ORACLE E-BUSINESS SUITE: CREDIT CARDS AND PCI COMPLIANCE

Version 1.1.0 - January 2007
Version 1.1.1 – October 2009
Version 1.1.2 – March 2010
Version 2.0.0 – April 2011
Version 3.0.0 – January 2014
Version 3.0.1 – January 2014
Version 3.0.2 – May 2014
Version 3.0.3 – April 2016

Authors: Stephen Kost and Mike Miller, CISSP, CISSP-ISSMP, CCSK

If you have any questions, comments, or suggestions regarding this document, please send them via e-mail to info@integrigy.com.

*PCI validation assessments must be performed by a "Qualified Security Assessor" and PCI quarterly network scans must be performed by an "Approved Scanning Vendor". Integrigy Corporation is not a PCI Qualified Security Assessor nor an Approved Scanning Vendor as our services and products are limited to databases and ERP applications. Integrigy Consulting and our security auditing product, AppSentry, can assist you in identifying PCI compliance issues in your Oracle E-Business Suite implementation, however, Integrigy cannot provide any determination as to your compliance with the PCI Data Security Standard nor issue a Report on Compliance. You should consult with a PCI Qualified Security Assessor the individual credit card brands if you have any questions regarding PCI compliance or for independent validation and a Report on Compliance of your organization's overall PCI compliance effort.*

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise. Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice. The Payment Card Industry Data Security Standard is updated on a periodic basis and the information contained in this document is specific to version 3.0 and may not be applicable to other versions of the standard.

# Table of Contents

# Overview

***"Payment Card Industry Data Security Standard requirements are applicable if credit card numbers are stored, processed, or transmitted."***

## Introduction

All Oracle E-Business Suite implementations that "store, process, or transmit cardholder data" must comply with Payment Card Industry (PCI) Data Security Standard regardless of size or transaction volume. The PCI Data Security Standard (DSS) is a set of stringent security requirements for networks, network devices, servers, and applications. PCI DSS details specific requirements in terms of security configuration and policies and all the requirements are mandatory. PCI DSS is focused on securely handling credit card data, but also has a significant emphasis on General IT security controls.

To meet PCI DSS requirements for an environment, even though credit card processing may be only one minor feature of the application, the entire application installation and the entire environment must be fully PCI DSS compliant. In a large global implementation that may include financials, manufacturing, projects, sales/CRM or human resources, PCI compliance can be a daunting endeavor and will impact operations and management of the non-card processing modules as well as the underlying supporting environment.

This paper will review the credit card processing features of Oracle E-Business Suite and will provide general guidance for Oracle E-Business Suite implementations in complying with relevant PCI DSS requirements. As Oracle E-Business Suite is a complex application environment, compliance with PCI DSS will differ for each organization in terms of architecture, configuration, and third-party security solutions.

## PA DSS Compliance

The PCI standard for software vendors developing applications processing or storing card data is the Payment Application Data Security Standard (PA DSS). PA DSS is a separate security standard published from PCI DSS. Currently, Oracle E-Business Suite is not listed by the PCI Security Standards Council as being a validated PA DSS application. Even though it is not a validated application, Oracle Corporation with Release 12 provides new standard functionality that meets several of the key PA DSS requirements. Most of this new functionality is by default not enabled and, as one of the steps to build a PCI DSS environment, this functionality must be enabled.

## PCI DSS Compliance

The focus for the Oracle E-Business Suite is PCI DSS compliance not PA DSS compliance – if an application is not a validated payment application, then PCI DSS compliance is required. PCI DSS focuses on the entire environment in which card processing occurs. PCI DSS describes PCI scope as follows –

> *"... requirements apply to all system components. System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. ... Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain*

> *name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications."*

All Visa, MasterCard, and American Express merchants or service providers that "store, process, or transmit cardholder data" must comply with PCI DSS regardless of size or transaction volume. Even if a merchant is not required to have annual on-site audits, perform quarterly scans, complete annual self-assessment questionnaires, or submit compliance documentation, "nevertheless must comply with, and are subject to liability under, all other provisions of" the then-current Payment Card Industry Data Security Standard.

### *Basic Guidelines for PCI DSS*

- Do not store sensitive authentication data
- Do not store cardholder data unless it's absolutely necessary
- Use strong cryptography to render unreadable cardholder data that you do store
- Do not permit any unauthorized people to access stored cardholder data
- Understand the data flow for the entire transaction process

## Corporate Cards and PCI DSS

Corporate Cards, credit cards held by employees for corporate purposes, are not usually subject to the scope of PCI DSS compliance. Corporate Cards are classified as internal accounts and PCI DSS applies only to external accounts. The full definition of internal vs. external accounts is discussed later in this paper. The Oracle E-Business Suite's functionality for protecting external accounts does, however, includes protection for Corporate Cards. When the functionality is enabled to protect external accounts, Corporate Cards are also protected.

While it is highly recommended by both Integrigy Corporation and the PCI Council to appropriately protect Corporate Cards, specific guidance and requirements for the protection of corporate cards should be sought from legal counsel and compliance teams as well as the issuer of the Corporate Card.

## PCI DSS Risk and Liability

This paper will only provide a brief synopsis of the risk and liability associated with either non-compliance or in the event of a security breach. For specific information on potential non-compliance fees, fines, liability, and actions, refer to your agreements with card companies, service providers, and/or processors. American Express, MasterCard, and Visa (and affiliated acquirers and processors) have fees and fines associated with non-compliance (a minimum of $50,000), which may also result in termination of your merchant services.

In the event of a data breach, you should assume that direct liability is at least $50 per identity based on FTC data and data breach notification surveys and litigation may result in significantly higher financial risk. For planning purposes, simply multiply the number of unique credit card numbers in your database by $50 to obtain a rough estimate of minimum potential liability.

## Scope and Purpose

The purpose of this paper is to provide general guidance for your PCI compliance effort specifically related to Oracle E-Business Suite Release 12, but not to be an authoritative reference in terms of Oracle E-Business Suite and PCI compliance. Integrigy Corporation is not a PCI Qualified Security Assessor, rather we assist merchants and assessors in identifying and remediating PCI compliance issues specifically in Oracle E-Business Suite environments.

You should consult with the individual credit card brands or a PCI Qualified Security Assessor if you have any questions regarding PCI compliance or for validation of your organization's overall PCI compliance effort. Ultimately, you as the merchant (and the signing corporate officer) are responsible for ensuring PCI DSS compliance and adherence to any credit card processing agreements.

# PCI DSS Summary

The PCI Data Security Standard (DSS) is an evolving set of requirements. It is updated every three years based on feedback, market evolution, and findings from previous breaches. The latest version of PCI DSS, version 3.0, becomes effective on January 1, 2014. To ensure organizations have sufficient time to transition, version 2.0 will overlap by one year with version 3.0 by being active until December 31, 2014.

For the purpose of PCI DSS compliance of Oracle E-Business Suite environments, there are only a few minor changes between PCI DSS versions 2.0 and 3.0 that will impact the existing compliance of an Oracle E-Business Suite environment.

## Key Terms

As American Express, MasterCard, Discover, and VISA have different names for the various credit card data elements, this paper will use the PCI DSS terminology of Primary Account Number (PAN) and Card Verification Number (CVN) consistently to refer to the key elements. Information related to magnetic stripe data and PIN block data will not be discussed in depth as Oracle E-Business Suite does not natively support or store these credit card elements.

| Definition | Description |
|---|---|
| **Primary Account Number (PAN)** | This is the credit card number. It may be also referred to as Account Number or Payment Card Number. The PAN may be 13 to 19 digits in length. Generally, American Express card numbers are 15 digits and MasterCard and Visa card numbers are 16 digits. |
| **Card Verification Number (CVN)** | This is the 3 or 4 digit code printed on the front or back of the card used to verify the purchaser is in possession of the card when the card is not physically presented. Each payment card brand refers to this code differently as follows –<br>▪ CAV2 = Card Authentication Value 2 = JCB<br>▪ CID = Card Identification Number = American Express<br>▪ CID = Card Identification Number = Discover<br>▪ CVC2 = Card Validation Code 2 = MasterCard<br>▪ CVV2 = Card Verification Value 2 = Visa |
| **Personal Identification Number (PIN)** | This is the secret numeric password known only to the user and a system to authenticate the user to the system. PINs are typically used with automated teller machines for cash advance transactions. For cards with EMV chips, the PIN replaces the cardholder's signature. |
| **Sensitive Authentication Data (SAD)** | This is the combination of the full track data from the magnetic stripe, chip or elsewhere along with the pin/pin block and the CVN. |
| **Service Code** | Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various purposes including defining service attributes, international transactions and usage restrictions. |

For more information on credit card number formats, see "Anatomy of Credit Card Numbers".

## CARDHOLDER DATA REQUIREMENTS

The table below graphically depicts the PCI DSS 3.0 core requirements for cardholder and sensitive authentication data, whether storage of each data element is permitted or prohibited, and if permitted, if it must be protected.

PCI DSS Requirements 3.3 and 3.4 apply only to the PAN. If PAN is stored with other elements of cardholder data, only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4. Sensitive data must not be stored after authorization, even if encrypted. This requirement applies even where there is no PAN stored in the environment.

| | | Data Element | Storage Permitted | Render Stored Data Unreadable per 3.4 (Protected) |
|---|---|---|---|---|
| **Account Data** | **Cardholder Data** | Primary Account Number (PAN) | Yes | Yes |
| | | Cardholder Name | Yes | No |
| | | Service Code | Yes | No |
| | | Expiration Date | Yes | No |
| | **Sensitive Authentication Data (SAD)** | Full Track Data – from magnetic stripe, chip or elsewhere | No | Cannot store per 3.2 |
| | | CVN, CAV2, CVC2, CVV2/, CID | No | Cannot store per 3.2 |
| | | Pin/Pin Block | No | Cannot store per 3.2 |

# ORACLE E-BUSINESS SUITE AND PCI DSS

Any Oracle E-Business Suite implementation that stores, processes, or transmits a customer's or a vendor's cardholder data is clearly in the scope of PCI DSS compliance.

Though encryption plays a large part in meeting PCI DSS requirements, the scope of PCI DSS is much larger than encryption of cardholder data. The use of hardware encryption solutions or the use of Oracle Advanced Security's Transparent Data Encryption (TDE) will not by themselves make Oracle E-Business Suite PCI DSS compliant. The scope of PCI DSS is the entire environment in which credit cards are being processed.

For Oracle E-Business Suite environments, meeting PCI DSS is a large and complex undertaking. Appendix B of this paper discusses additional requirements for PCI DSS for those customers using host providers or cloud vendors as well as those using virtualization technology to support the E-Business Suite.

***The difficulty with Oracle E-Business Suite and achieving PCI compliance is that even though credit card processing may be only one minor feature of the application, the entire application installation must be fully PCI DSS compliant due to the tight-integration and data model of the Oracle E-Business Suite.***

## ORACLE E-BUSINESS SUITE 11i

***In our opinion, it is not feasible nor practical to make an Oracle E-Business Suite 11i environment fully PCI DSS compliant.*** Oracle Corporation has no plans to enhance or validate Oracle E-Business Suite 11i to be a PA DSS validated payment application. See My Oracle Support Note ID 1098843.1 *"Oracle Payments - PA-DSS (Payment Applications Data Security Standards) update for Release 11i"* for more information. Oracle E-Business Suite 11i can be configured and maintained to comply with most PCI requirements like encryption and logging, however, significant deficiencies would remain due to the age of the application server technology stack, weaknesses in encryption key management, and functional limitations in the application.

The only workable solutions are to (1) upgrade to Release 12 or (2) to implement tokenization which would remove Oracle E-Business Suite 11i from the scope of PCI compliance. Oracle E-Business Suite 11i does not natively support tokenization, however, there are several third-party vendors that provide tokenization solutions compatible with Oracle E-Business Suite.

## ORACLE E-BUSINESS SUITE RELEASE 12

In order to comply with the PCI DSS, it is important to first understand how Oracle E-Business Suite handles and processes credit card information. This process should be understood, but also, new in PCI DSS 3.0, the flow must be documented in a data-flow diagram per Requirement 1.1.3. New with Release 12 of the E-Business Suite, credit card processing and data storage within Oracle Financials, for customers and vendors card data, is now done within the Secure Payment Data Repository within Oracle Payments. It is through this new standard functionality built into the Secure Payment Data Repository that PCI DSS compliance can be met.

With Release 12, the Oracle E-Business Suite has eleven modules that use Oracle Payments for the processing and storage of cardholder data. Only these eleven products can be configured to meet PCI DSS requirements through the PA DSS functionality provided by Oracle Payments. From the release notes for the Oracle Payment

Application Data Security Standard (PA DSS) Consolidated Patch Release 12.1.2 (Doc ID 981033.1), the following list of products now use the Secure Payment Repository –

**Oracle Modules using the 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

### *Secure Payment Repository*

With Release 12, the Trading Community Architecture (TCA) defines party information (e.g. suppliers and customers) and the Secure Payment Data repository stores the payment instruments (credit card and bank accounts) for the parties. It is through this consolidation of payment instruments into the Secure Payment Repository that Oracle Payments offers its new functionality for the encryption and masking of payment instruments to meet the PA DSS requirements.

The key point to note is that only those products identified above make use of the Secure Payment Repository. More importantly, the PA DSS functionality provided by the Secure Payment Repository is NOT enabled by default. The steps to enable it are outlined later in this paper.

### *External vs Internal Accounts*

Oracle Payments, with its Secure Payments Repository, only provides PA DSS functionality for what Oracle refers to as external accounts. Oracle defines “external accounts” as those accounts belonging to customers, suppliers, vendors, students, and external third parties. These are the credit cards and bank account numbers customers and vendors use to conduct business with a company. Oracle defines “internal accounts” as those accounts a company uses internally such as bank accounts defined within Accounts Payable or employee bank accounts defined within Oracle HR/Payroll for direct deposit. Because Oracle Payments only consolidates payment instrument data for external accounts and not for internal accounts, no PCI DSS protection is offered for internal accounts.

Even though Corporate Cards (corporate issued credit cards held by employees) are internal accounts, these card numbers can be protected the same as customer card numbers. Corporate Cards are defined in the Accounts Payble iExpense module, which uses the Secure Payment Data Repository.

### *Maintenance Required*

Enabling credit card number encryption in Oracle E-Business Suite for PCI DSS compliance is a one-time setup exercise. However, by design, especially if certain configuration options are elected, on-going and continuous monitoring and maintenance is required for a PCI DSS compliant environment. Examples of this maintenance include certain concurrent programs that must be run on a regular basis. Also different from 11i, R12 credit card data can be easily decrypted at any time. This requires additional steps be taken and monitoring implemented to ensure encryption is continuously maintained and not disabled.

## Cardholder Data Encryption

The default Oracle E-Business Suite installation does not meet PCI DSS requirements to protect cardholder data. Prior to PCI DSS compliance in the application, there was a patchwork of module-centric storage of cardholder data and masking of primary account numbers. Each module that requires handling of credit cards has its own tables to store the data and code to mask or protect card data. This decentralized storage of and handling of cardholder data is the default upon installation in all versions of Oracle E-Business Suite including 12.1 and 12.2.

For PA DSS compliance, Oracle developed an optional method for storing cardholder data and centralized the storage of the data in the Oracle Payments tables. This PA DSS functionality was released as a patch for 11i and as optional functionality in 12.1 and 12.2. However, encryption of cardholder data is not enabled by default in any version of Oracle E-Business Suite.

The following reviews the optional PA DSS standard functionality provided by Release 12 that must be enabled to meet PCI DSS requirements:

- Credit card number masking (Requirement 3.3)
- Credit card data storage (Requirement 3.4)
- Protect encryption keys against disclosure and misuse (Requirement 3.5)
- Encryption key management (Requirement 3.6)

### *Credit Card Number Masking (Requirement 3.3)*

Requirement 3.3 calls for the PAN to be masked (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.

By default with R12, Oracle Payments ships with a mask setting that displays only the last four digits which meets the requirements for PCI DSS. Masking is configured through the Oracle Payments System Security Options. These options supersede the prior credit card masking system profile options available in Release 11i. The options are to display first or last four digits or display none (mask all digits). The maximum number of digits allowed to be displayed is four.

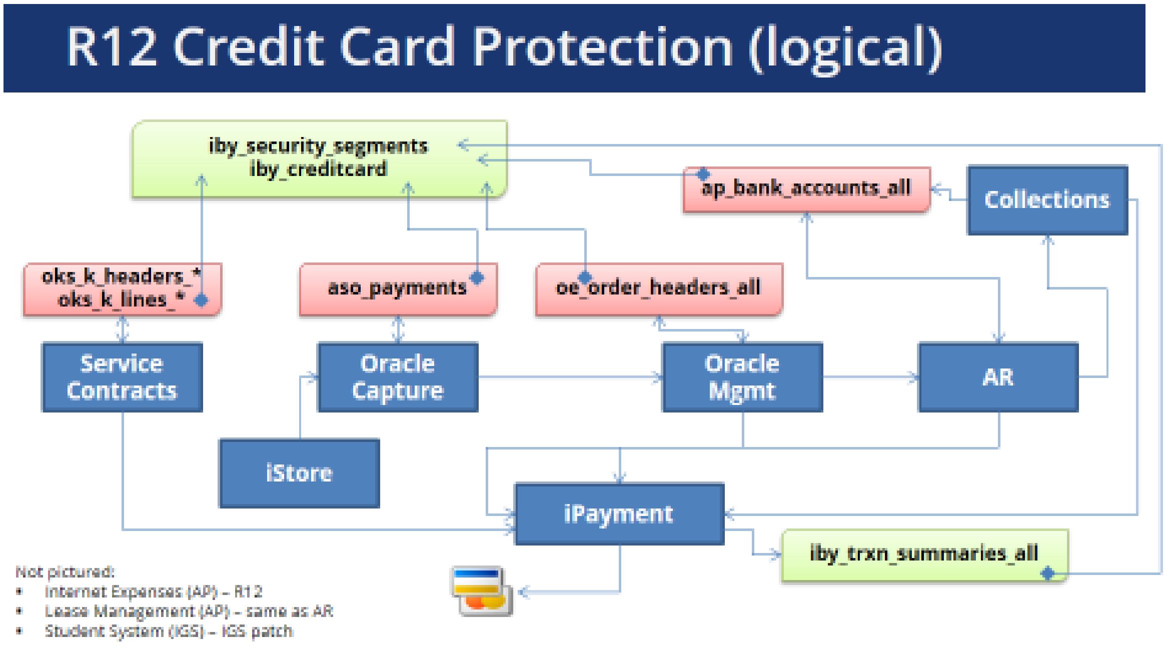
Furthermore, the encrypted PAN as well as the masked first or last four numbers of the PAN are stored in the IBY.IBY_SECURITY_SEGMENTS table. This allows for the display of the masked PAN without having to decrypt the PAN. Standard functionality also allows for highly controlled unmasked viewing of PANs for legitimate business purposes.

### *Credit Card Data Storage (Requirement 3.4)*

Requirement 3.4 mandates that the PAN is unreadable anywhere it is stored using one-way hashes or strong encryption. Oracle Payments meets this requirement first by centralizing cardholder data and then applying strong encryption.

With R12 the storage of External credit card data in Oracle Financials is centralized in Payments. Other modules within Oracle Financials in the Suite now point to Payments to obtain PAN data for External accounts. The following table highlights the major credit card processing modules and the tables that display credit card data stored in Payments –

| *Module* | *Table* |
|---:|---|
| *Accounts Payable (AP)* | ap.ap_bank_accounts_all |
| *Accounts Receivables (AR)* | ap.ap_bank_accounts_all |
| *Collections (IEX)* | ap.ap_bank_accounts_all |
| *Internet Expenses (OIE)* | ap.ap_credit_card_trxns_all |
| | ap.ap_cards_all |
| *Payments (IBY)* | iby.iby_trxn_summaries_all |
| | iby.iby_creditcard |
| *iStore (IBE)* | aso.aso_payments |
| *Lease Management (OKL)* | ap.ap_bank_accounts_all |
| *Order Capture (ASO)* | aso.aso_payments |
| *Order Management (ONT)* | ont.oe_order_headers_all |
| *Service Contracts (OKS/OKC)* | oks.oks_k_headers_b |
| | oks.oks_k_headers_bh |
| | oks.oks_k_lines_b |
| | oks.oks_k_lines_bh |
| | okc.okc_rules_b |
| | okc.okc_rules_bh |
| *Student System (IGS)* | igs.igs_ad_app_req |
| | igs.igs_fi_credits_all |
| | igs.igs_fi_inv_int_all |



## R12 Credit Card Protection (logical)

Not pictured:

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

Oracle Payments offers two modes of encryption, full or partial, as well as immediate or scheduled. Which encryption options are selected should be the result of discussions with legal counsel, compliance and risk management.

Partial encryption refers only to the encryption of the PAN. Full encryption refers to the encryption of the Primary Account Number (PAN) along with the cardholder name and card expiration date. The cardholder name and expiration date are also referred to in the documentation as supplemental data.

Immediate encryption encrypts cardholder data as it is being written to the database. Scheduled encryption leaves cardholder data unencrypted until a concurrent request is run manually or scheduled at a later point in time to encrypt cardholder data. Integrigy Corporation strongly recommends only using immediate encryption.

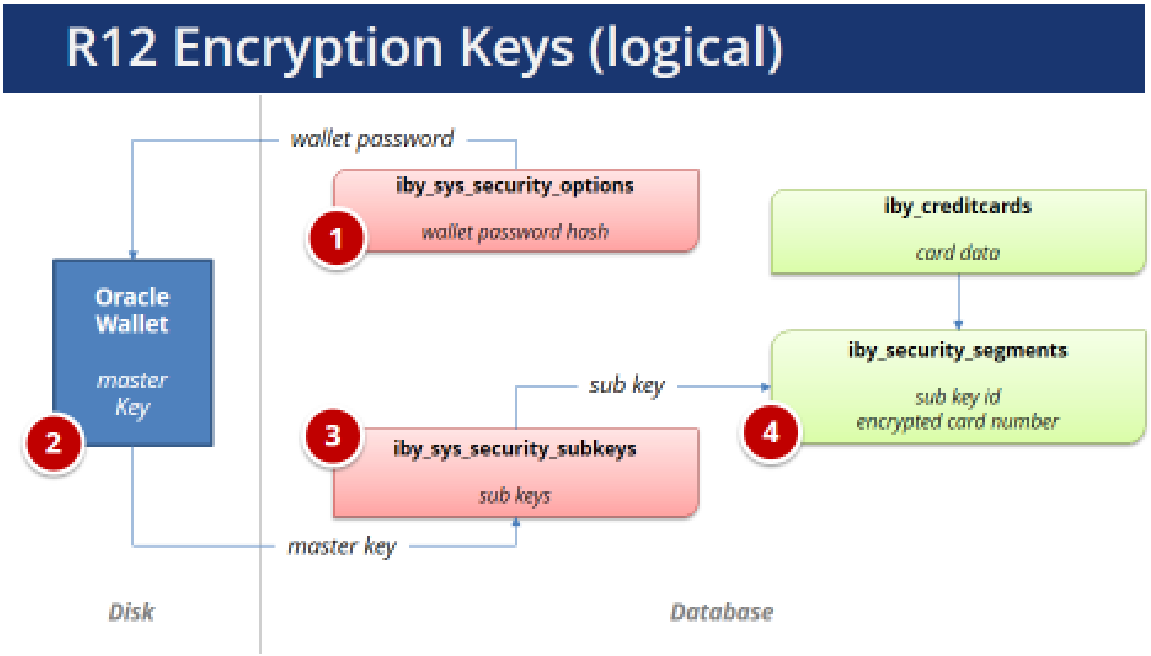
Specifically, to meet requirement 3.4, Oracle Payments uses a chained encryption key approach and a Triple Data Encryption Algorithm (TDEA, Triple DEA, TDES or 3DES) symmetric-key block cipher.  A master encryption system key is used to encrypt sub-keys. The sub-keys are 156-bit-length system generated and are encrypted using 3DES and the master key as the key. The encrypted sub-keys are then stored in the table IBY.IBY_SYS_SECURITY_SUBKEYS.

Cardholder data is encrypted using the 156 bit sub-keys using a 3DES algorithm in the table IBY.IBY_SECURITY_SEGMENTS via the standard Oracle package DBMS_OBFUSICATION_TOOLKIT. The 156 bit key exceeds the PCI DSS required minimum of double-length keys for 3DES. It is also interesting to note that the Oracle E-Business Suite is using the depreciated DBMS_OBFUSICATION_TOOLKIT package rather than the newer DBMS_CRTYPO package.

| Acceptable PCI DSS Strong Cryptography* | |
|---|---|
| **Strong Cryptographic Standard** | **PA DSS Requirement** |
| Advanced Encryption Standard  (AES) | 128 bits or higher |
| Triple Data Encryption (TDES or 3DES) | Minimum double-length keys |
| RSA | 1024 bits and higher |
| Elliptic Curve Cryptography (ECC) | 160 bits and higher |
| ElGamal | 1024 bits and higher |

*PCI Glossary of Terms, Abbreviations, and Acronyms

The PAN is also stored as an MD5 hash (using the DBMS_OBFUSCATION_TOOLKIT package) in the table IBY.IBY_SECURITY_SEGMENTS to allow for secure searching/matching of PANs.



### *Protect encryption keys against disclosure and misuse (Requirement 3.5)*

Requirement 3.5 identifies functionality and procedures that must be present to protect encryption keys against disclosure and misuse.

The chained encryption key approach largely meets this requirement. The system master key is stored outside the database in an Oracle Wallet referred to as the Payment encryption wallet. The wallet is stored in a highly secured directory within the file system and requires a password to open. As well, the wallet is encrypted using 3DES and the password as the encryption key. To further protect against disclosure and misuse, the sub-key (the key-encryption key) is 3DES encrypted using system master key in the Payment Wallet.

As requirement 3.5.1 calls for the restriction of encryption keys to the fewest number of custodians necessary, control of the wallet password is the primary concern. The wallet password can be restricted to a small number of custodians, not necessarily including the entire team of DBAs or systems administrators.

### *Encryption key management (Requirement 3.6)*

Requirement 3.6 describes specific requirements for the management of encryption keys. This includes secure key generation, dual control of the key, and periodic rotation of the encryption keys.  The use of the Oracle Wallets, specifically the Payment Wallet, largely meets this requirement. The Payment Wallet's password may be split among multiple people. This meets requirement 3.6.6 for split knowledge and dual control of keys to eliminate one person having access to the whole key.

Integrigy Corporation strongly recommends that under no circumstances should the DBA or system administrator have knowledge of or access to the entire Payment Wallet password and that the Payment password be split among multiple people. Ideally it should be split among multiple teams such as IT Security and Compliance. Integrigy Corporation further recommends that the Oracle E-Business Suite responsibility used to register the Payment Wallet be held by someone without knowledge of the Payment Wallet password.

This use of the Payment Wallet and its master system key also allows for the easy rotation of keys. Requirement 3.6.4 specifies that the encryption keys be rotated regularly – at a minimum of annually.

## Enabling Credit Card Protection

While Release 12 by default does not protect cardholder data, it can be enabled by following the Oracle Support Note 1301337.1. The steps are summarized below for a new Release 12 implementation.

There are the three basic steps to enable PCI protection for a new Release 12 implementation:

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

## Payment Encryption Wallet

The primary PCI DSS requirement for the E-Business Suite is the protection of cardholder data through the use of strong encryption. With Release 12, the most critical step in meeting PCI DSS is the creation and on-going protection and maintenance of the Payment encryption wallet.

There are several decisions to be made before creating a Payment Wallet. Wallets can either be self-signed, where the certificate is the same as the subject, or use a third party certificate from a well-known Certificate Authority. Which type of wallet is created is dependent on your trust requirements and expected usage.

Although wallets are password protected, they provide the ability for services and applications to access them without requiring a password at runtime. This is done through the autologin option which, when enabled, creates a self-signed obfuscated wallet file which allows applications to access the wallet without a login. For this reason where Payment Wallets are created and stored is very important. Integrigy Corporation recommends that the Payment Wallet be created on a middle tier application server or concurrent manager node in a highly secured directory only accessible by the E-Business Suite – ideally outside the Oracle Home.

With Release 12, wallets have multiple purposes. Besides supporting encryption within Payments, wallets can also support Transparent Data Encryption (TDE), SSL for HTTP client authentication as well as SSL for the Oracle Payments ECAPP servlet. While it is possible for a single wallet to support multiple purposes, Integrigy Corporation strongly recommends maintaining separate wallets for each function. For example, if a consolidated wallet is compromised or corrupted, it may result in the inability to access payments data.

Payment Wallets must also be backed up separately and a copy of the wallet files (ewallet.p12 and cwallet.sso) should be saved in a secure location.

## Set Protection Configuration Options

Setting the protection configuration options is done using the Funds Capture Setup Administrator or Payments Setup Administrator responsibility. The decisions regarding which options to use should be carefully reviewed with internal audit, security and counsel.

- **Wallet** - Location of the wallet file, the name of the wallet and the wallet password. Another decision is the whether the system key will be system generated or user defined. Integrigy Corporation recommends using a system generated key unless specific requirements are identified.

- **Account Number -** Yes or No whether the PAN will be encrypted. To meet PCI requirement 3.4 select 'Yes'.
- **Supplemental data** - Yes or No whether card holder name and expiration date will also be encrypted. This is also referred to as partial encryption if set to 'No'. Selecting 'Yes' is referred to as 'Full Encryption'.
- **Type –** Whether or not encryption will occur immediately prior to being written to the database or later at a scheduled time. The options are 'Immediate' or 'Scheduled'.  If you select scheduled, data will be unencrypted until the request set 'Encrypt Sensitive Data Request Set' is run.  Oracle does not automatically schedule this and it will need to be manually scheduled.  Integrigy Corporation strongly recommends using 'Immediate' and not 'Scheduled'.
- **Card Owner Verification** – Requiring the 'Security Code' and/or 'Require Statement Billing Address' by setting to 'Yes' requires the entry of the credit card security code or card statement billing address. This information is passed to the payment system, which in turn, checks with the credit card issuer to confirm the credit card owner's security code and/or statement billing address. Payments stores card-validation codes in an encrypted format and securely deletes them automatically upon completion of authorization. Whether or not collecting the card security code is appropriate, required or is permissible by PCI requirements 3.2 and 3.4 should be reviewed by corporate compliance and counsel teams.
- **Credit Card Masking** - Allows for masking of all but the first or last x digits of a PAN, for which x is identified by the field 'Number of Digits to Display. Please note the maximum number of digits is four. This means the maximum number of digits of the PAN that can be displayed unencrypted is four. To meet PCI requirement 3.3 it is recommended to display the last four digits.

## ENCRYPT EXISTING CARDHOLDER DATA

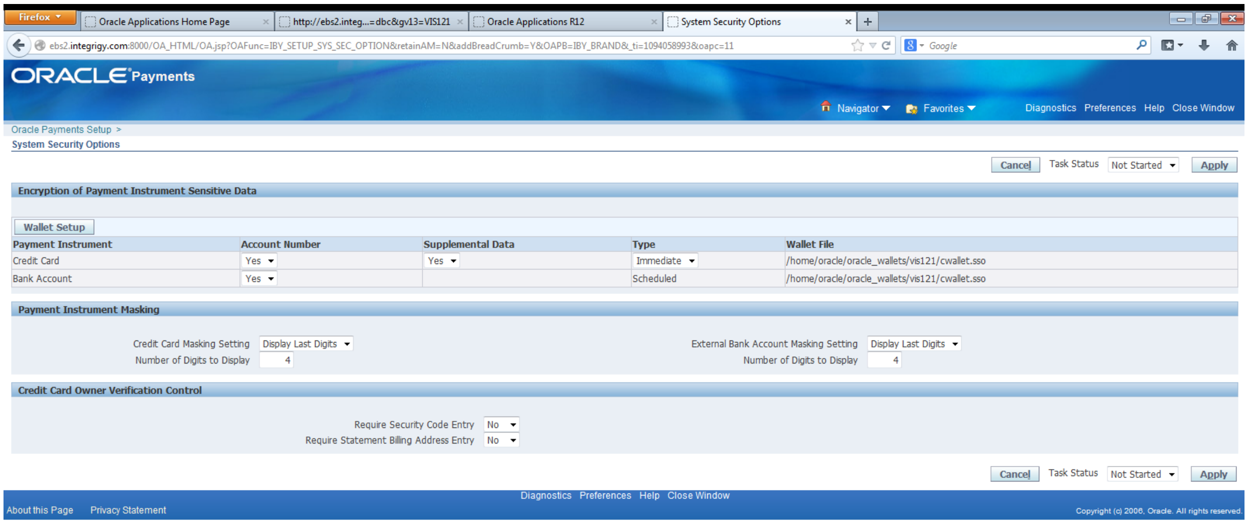
Cardholder data created prior to setting the encryption configurations will not be automatically encrypted. To encrypt cardholder data that already exists run the request set 'Encrypt Sensitive Data Request Set'. This request set will run the following concurrent programs:

- Encrypt Credit Card Data
- Encrypt External Bank Account Data
- Encrypt Transaction Extension Data
- Encrypt Credit Card Transaction Data

### *Optional - Required for Full Encryption*

If full encryption is being used (encrypting supplemental data) – the concurrent program 'Upgrade Encrypted Credit Cards' must also be run. This program is used for one-time execution, post-enabling, supplemental card holder data encryption. This ensures that the expiration date and card holder name is encrypted for the existing encrypted credit cards.

## Figure 1 Payment System Security Options



ebs2.integrigy.com:8000/OA_HTML/OA.jsp?OAFunc=IBY_SETUP_SYS_SEC_OPTION&retainAM=N&addBreadCrumb=Y&OAPB=IBY_BRAND&_ti=1094058993&oapc=11

Oracle Payments Setup >

System Security Options

Task Status: Not Started

**Encryption of Payment Instrument Sensitive Data**

| Payment Instrument | Account Number | Supplemental Data | Type | Wallet File |
|---|---|---|---|---|
| Credit Card | Yes | Yes | Immediate | /home/oracle/oracle_wallets/vis121/cwallet.sso |
| Bank Account | Yes | | Scheduled | /home/oracle/oracle_wallets/vis121/cwallet.sso |

**Payment Instrument Masking**

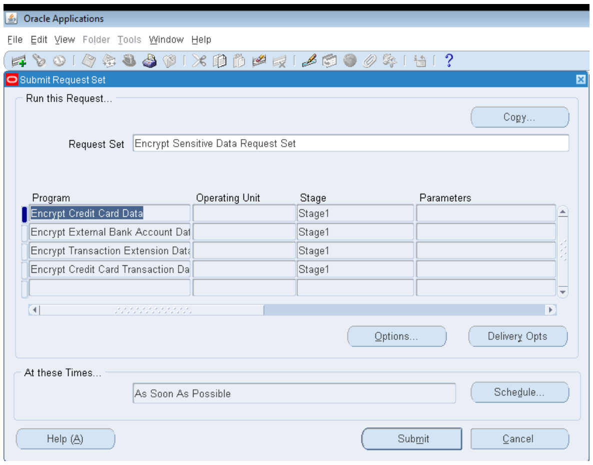
Credit Card Masking Setting: Display Last Digits
Number of Digits to Display: 4

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

**Credit Card Owner Verification Control**

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

## Figure 2 - Encrypt Sensitive Data Request Set



Submit Request Set

Run this Request...

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 | |

At these Times...

As Soon As Possible

# Maintenance of Credit Card Protection

PCI DSS compliance and enabling credit card protection with the E-Business Suite is not a one-time effort. To ensure that cardholder data is protected PCI DSS identifies a schedule of daily, monthly, quarterly and annual tasks and requirements that need to be met. As well, PCI DSS identifies on-going, continuous, requirements. As each Oracle E-Business suite implementation is unique, a definitive maintenance checklist is only possible through analysis. This section provides an overview of several of the requirements that need to be included in a PCI DSS compliance program for the Oracle E-Business Suite.

## Scheduled Tasks for PCI Compliance

### *Daily Log Review*

PCI requirement 10.6 calls for reviewing all system components daily for anomalies and suspicious activity. Log review does not need to be manual. The use of log harvesting, parsing and alerting tools may be used. Whatever automation is in place, though, judgments will need to be made by personnel, most likely on a daily basis. Attestation and evidence of daily log reviews and decisions needs to be thorough and complete.

### *Monthly Card Expiration Status Update (If Using Full Encryption)*

If full encryption is being used (not partial) to meet PCI requirement 3.4, the concurrent program “Upgrade Credit Card Expiration Status” requires execution. This program is used for updating the expiration status of credit cards. It is designed to be run on a monthly basis (preferably on the beginning of a month). The card expiration status will not change to EXPIRED, even if expiry data has passed, unless you run this program.

### *Every 90 Days Disable Inactive Users and Change User Passwords*

Per requirement 8.2.4 user accounts, including Oracle E-Business Suite user accounts, need to have their passwords changed every 90 days. As well, per requirement 8.1.4, inactive user accounts need to be disabled every 90 days. This would include Oracle E-Business Suite user accounts that have not logged on in the last 90 days.

### *Quarterly Internal and External Vulnerability Scans*

Requirement 11.2 specifies that internal and external network vulnerability scans be done at least quarterly or after any significant change to the network. While not directly involving the Oracle E-Business Suite, any applications such as iStore that exist in the DMZ will be included.

### *Purge PAN Data Every One to Two Years*

Requirement 3.1 requires that cardholder data stored be kept to a minimum. The retention time for the storage of the PAN is normally between one to two years. This is different and separate from business transactions. For example, customer orders within iStore commonly are required to be retained for five to seven years, but the PANs associated with these transactions should be purged after one to two years.

There is no single supported method provided by Oracle to purge PANs from Oracle Payments.  A few of the individual Oracle modules that use the Secure Payments Repository have limited standard functionality to purge PAN data and Oracle has several bugs and enhancement requests for the purging this data. For details on the individual purge programs, consult the implementation and user guides of the respective modules as well as Oracle Support. A few of the concurrent programs are listed below:

- Service Contracts ”Purge Credit Card Information (OKSCCPURGE)”
- Payments “Purge Redundant PA-DSS Incidental Data (IBY_PADSS_PURGE)”
- iExpense “Credit Card Historical Transactions Management (APXCCPUT)”

### *Rotate Wallet Keys Annually*

PCI requirement 3.6 requires that encryption keys be rotated on a regular basis – at a minimum of annually. This means that the Oracle Payment Wallet keys needs to be rotated. Changing the password for the wallet does not change the key. The process of rotating the wallet key for Oracle Payments requires that an entire new wallet be created, and the old wallet destroyed (both the *.p12 and the *.sso files) through a secure wipe – not just deleted from the file system.

### *Annual Application Penetration Test*

Per requirement 11.3 penetration tests are required annually. Specifically requirement 11.3.2 for application-layer penetration tests will include the Oracle E-Business Suite.  A third party firm experienced with Oracle E-Business Suite penetration testing should be utilized to conduct any such application penetration tests. Note that requirement 6.6 for the penetration of public-facing web applications is a different requirement from 11.3.2.

## On-Going Tasks for PCI Compliance

### *Backups and Payment Wallet Protection*

Requirement 3.5 governs the protection of the encryption keys. Since the Payment Wallet holds the system encryption key, it should never be backed up in the same place as Oracle E-Business Suite backups. For PCI DSS this specially means that Payment Wallets must be excluded from normal database and file system backups solutions. Payment Wallets should be backed up separately and securely.

The following guidance may be of assistance:

- RMAN only adds database files, redo-logs etc… to the backup file, hence there is no risk of the encryption wallet (ewallet.p12) or the auto-open wallet (cwallet.sso) becoming part of a database backup.
- If Oracle Secure Backup (OSB) is being used, it uses datasets defined within its configurations for which operating system files to include or exclude. By default OSB automatically only excludes auto-open wallets (cwallet.sso). It is highly recommended by Integrigy Corporation to amend the OSB datasets to also exclude encryption wallets (ewallet.p12 or *.p12).

### *Production Clones and Copies*

Creating clones and copies of production E-Business Suite databases for testing, developing and training is a regular occurrence. See Appendix A for a review of the requirements that PCI DSS places on test and development databases. These requirements include requirement 6.4.3 which forbids live production PANs to be used for development and testing as well as requirement 3.5 for the protection and management of encryption keys. Requirement 3.5 specifies that production encryption keys (including Payment wallets) cannot be copied to and/or exist in non-production instances.

### *Restrict Access To and Manage Wallet Keys*

PCI requirement 3.5 requires that encryption keys be protected and that access to encryption keys be restricted to the fewest number of custodians necessary. It is also requires split knowledge and establishment of dual control of keys. A process will need to be in place to provide evidence for who has access to the Payment wallets' password. Tools such as password safes can be used to produce such evidence.

### Keep Cardholder Data Out of Log Files

PCI Requirement 3.4 requires PAN data to be unreadable anywhere it is stored unless it is protected. Besides encrypting cardholder data stored in the database, protection for other situations needs to be considered.

To keep cardholder data out of log files, the OA Framework logging system profile option "FND: Debug Log Level" should be set to "Unexpected (6)" or a higher value to prevent the possibility of credit card numbers being included in the log file.

If using the Oracle Payments servlet, debugging should be disabled to prevent writing of cardholder data to debug files. Review all payment system servlet configurations for logging, debugging, temporary, and archiving options and directories to identify any locations where readable cardholder data might be written.

It is highly recommended by Integrigy Corporation to set up monitoring for debug settings in production (non-production instances cannot have live credit cardholder data per requirement 6.4.3). Oracle Alerts can be configured if no other monitoring tools exist. Whatever monitoring process is set up it needs to be monitored daily.

### Email Center, Exports and Attachments

PCI Requirement 3.4 requires PAN data to be unreadable anywhere it is stored unless it is protected. As the Oracle E-Business Suite allows for the attachment of documents, a policy is required forbidding cardholder data in attached documents. Users will need to be trained to abide by this policy. Likewise, the export to Excel feature of the E-Business Suite will need to be considered. A policy will also need to govern the export of cardholder data to Excel and/or from the Oracle E-Business Suite. Since temporary export files are stored until purged, Integrigy Corporation recommends a rolling purge of export files (FND_LOBS) on a regular basis.

Oracle Email Center, if it is in use, can also potentially store cardholder data if emails are sent containing such data. A policy will be required for the use of email with cardholder data.

### *Masking and Viewing Cardholder Data in Clear Text*

PCI requirement 3.3 requires the PAN to be masked when displayed unless there is a legitimate business reason.

For cases of legitimate business reasons, Oracle Payments has a menu security function called IBY_CC_SUPER_USER. When this function is added to the "Funds Capture Process Manager" responsibility, it will allow access to unmasked PANs. This feature is ONLY available from Funds Capture Process Manager responsibility, it is not available from any other module forms. iExpense has a similar function called 'Payments Credit Card Super User' which can only be added to the  'Expenses Policy Menu (OIE_POL_MENU)'.

Changes to the responsibilities that allow full un-masked access and who has access to the responsibilities needs to be carefully and regularly monitored. Integrigy Corporation highly recommends monitoring who has access to and changes to these responsibilities in production (non-production instances cannot have live credit cardholder data per requirement 6.4.3). Oracle Alerts can be configured if other monitoring tools do not exist. Whatever monitoring process is set up it needs to be monitored daily.

### *Disable and Monitor Decryption Concurrent Programs*

PCI requirement 3.4 requires PAN data to be unreadable anywhere it is stored unless it is protected. With Release 12 credit cardholder data can be decrypted at any time as easily as it is encrypted by simply running the request set "Decrypt Sensitive Data Request Set" or any of the individual programs.

Integrigy Corporation highly recommends removing the request set, as well as the concurrent programs within it, from all request groups and then disabling (end-date the request set and disable its concurrent programs.  If for any reason the programs need to be run at a later date, they can be enabled. This will help prevent accidental decryption along with nefarious attempts to access cardholder data.

It is also highly recommended by Integrigy Corporation to set up special monitoring for these Decrypt Sensitive Data concurrent programs in production (non-production instances cannot have live credit cardholder data per requirement 6.4.3). Oracle Alerts can be configured if other monitoring tools do not exist.  Whatever monitoring process is setup it needs to be monitored daily to ensure that these programs are not run.

**When not in use remove from all request groups and disable:**

Request set (end-date)

- Decrypt Sensitive Data Request Set

Concurrent Programs (disable)

- Decrypt Credit Card Data
- Decrypt External Bank Account Data
- Decrypt Transaction Extension Data
- Decrypt Credit Card Transaction Data
- Payments Scheduled Decryption

### *Monitor for PCI Configuration Changes and Decryption*

Integrigy Corporation recommends that the critical Oracle Payments security configurations for masking (requirement 3.3) and encryption (requirement 3.4) be continuously monitored in production (non-production instances cannot have live credit cardholder data per requirement 6.4.3). Oracle Alerts can be configured if other monitoring tools do not exist. Whatever monitoring process is set up it needs to be monitored daily to ensure that these programs are not run.

Specifically, the table iby.iby_sys_security_options holds the configurations for masking and encryption. This table needs to be continuously monitored and any changes should be immediately reviewed and reconciled. Integrigy also recommends additional monitoring steps be taken to notify internal audit and /or IT security if the following request set and/or concurrent programs are ever run:

Request Sets

- Encrypt Sensitive Data Request Set
- Decrypt Sensitive Data Request Set

Concurrent Programs

- Encrypt Credit Card Data
- Encrypt External Bank Account Data
- Encrypt Transaction Extension Data
- Encrypt Credit Card Transaction Data
- Decrypt Credit Card Data
- Decrypt External Bank Account Data
- Decrypt Transaction Extension Data
- Decrypt Credit Card Transaction Data
- Payments Scheduled Decryption

### *Continuously Monitor Security for Vulnerabilities*

Requirement 6.1 requires a program for continuous monitoring for new security threats and vulnerabilities. This specifically requires the monitoring for new Oracle security patches. Evidence of this monitoring is required.

### *Review Custom Code*

Requirements 6.3 and 6.4.4 address the terms and conditions for the development of custom code and the review of custom code prior to release to production. A program for the view and production migration is required and evidence of its on-going use is required for Oracle E-Business Suite Customizations, Extensions, Modifications, Localizations and Integrations (CEMLI). The review needs to test for SQL injection, cross-site scripting, and other common application security vulnerabilities.

Requirement 6.6 calls for penetration tests of public facing web applications. All CEMLI artifacts in web-facing modules (iStore, iReceivables, etc.) should be subjected to an application security code review (whitebox) as well as penetration testing (blackbox). For example, custom forms for iStore that are public facing need to be penetration tested.

# Appendix A - Test and Development Databases

Creating clones and copies of production E-Business Suite databases is a regular occurrence. There are several PCI DSS requirements that apply to non-production instances of the Oracle E-Business Suite.

### *No Production Cardholder Data*

The most important PCI DSS requirement that applies to non-production instances is requirement 6.4.3 which forbids production cardholder data to be used for development, testing, training and/or any other reason or purpose other than supporting business transactions in production.  Production cardholder data cannot exist outside production. Non-production instances need to have production cardholder data either removed or scrambled.

### *Protect Production Encryption Keys*

Requirement 3.5 governs the protection and management of encryption keys which when applied to non-production databases means that production encryption keys (specifically the Payment Wallet) cannot be copied to and/or exist in non-production instances. If, for whatever reason, the production wallet is copied to a non-production instance, the production encryption key MUST be rotated and the production wallet MUST be destroyed by a secure wipe (not just deleted from the file system). If the non-production instance is virtualized, depending on how memory is locked or shared to the guest, a secure wipe may be even more critical.

### *Building Non-Production Instances*

The points below highlight the requirements to build non-production instances:

- The production Payment Wallet will need to be rotated and securely wiped if copied from production.
- The location of the Payment Wallet will need to be reset. Do not use SQL to update to table IBY_SYS_SECURITY_OPTIONS directly. The user interface must be used to update the file location.
- Remove, purge and/or scramble production cardholder data. Depending on requirements there are several options for creating and sanitizing cardholder data. These options make use of the fact that cardholder data (the PAN and supplemental data) is separate and different from the related business transaction and that the cardholder data is centralized within the Secure Payment Repository.

# APPENDIX B –THIRD PARTY PROVIDERS/OUTSOURCING AND USE OF VIRTUALIZATION TECHNOLOGIES

Third party service providers and virtualization technologies are commonly used to support Oracle E-Business Suite environments. There is specific PCI DSS guidance for the use of third parties and virtualization technologies.

## USE OF THIRD-PARTY SERVICE PROVIDERS / OUTSOURCING

There are additional PCI DSS requirements for those using third parties to host, outsource key services and/or use remote managed services. Examples of such services include but are not limited to the management of: routers, firewalls, databases, physical security, and/or servers.

How to meet PCI DSS requirements for the Oracle E-Business Suite with regard to the use of third parties is outside the scope of this paper. However, for the E-Business Suite customers using a cloud or hosting provider there are a few points to consider. Further information on Cloud Computing and PCI DSS guidelines for Cloud Computing can be found in the Information Supplement "PCI DSS Cloud Computing Guidelines" on the PCI Security Standard's website (www.pcisecuritystandards.org).

For E-Business Suite customers using Cloud Service (Hosting) providers:

- Cloud security is a shared responsibility between the cloud service provider (hosting) and the customer.
- There are specific PCI DSS requirements for hosting providers and third parties. An example is requirement 8.5.1, which states that service providers with remote access to environments with cardholder data must use a unique authentication credential (such as a password/phrase) for each customer. Another example is requirement 2.6 which states that shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A of the PCI DSS version 3.0 - Additional PCI DSS Requirements for Shared Hosting Providers.*
- The PCI DSS compliance status of all associated third-party service providers with access to cardholder data must be monitored. Refer to Requirement 12.8 for details.
- Customers and third parties must clearly identify the services and system components which are included in the scope of the PCI DSS assessment, the specific PCI DSS requirements covered by the third party, and any requirements which are the responsibility of the third party.
- Third-party service providers may themselves outsource services. If so, there may be an impact on the security of the cardholder data environment. This is the responsibility of the E-Business Suite customer to identify and manage.

There are two basic options for third-parties to validate PCI DSS compliance:

1) Third parties can undergo a PCI DSS assessment on their own and provide evidence to demonstrate their compliance. If this is done, sufficient evidence is required to verify that the assessment covers the scope of services under contract between the Oracle E-Business Suite customer and the third party.
2) If the third party does not undergo their own PCI DSS assessment, the third party will need to have their services reviewed during the course of the E-Business Suite customer's PCI DSS assessments.

## USE OF VIRTUALIZATION TECHNOLOGIES

Virtualization technology is commonly used to support Oracle E-Business Suite environments, not only for non-production databases, but especially if third party hosting or Cloud service providers are used. The PCI Security Standards Council has additional requirements and guidelines for the use of virtualization technologies. These are documented in "PCI Security Information Supplement: PCI DSS Virtualization Guidelines version 2" which can be found on the PCI Security Standard's website (www.pcisecuritystandards.org).

The scope of this paper precludes being able to map in detail the PCI DSS requirements for the E-Business Suite to use virtualized servers. The PCI Security Information Supplement referenced above has an appendix "Virtualization Considerations for PCI DSS" which reviews in detail the PCI DSS virtualization requirements. This document should be carefully consulted but can be summarized as follows: Since the basic PCI requirement is that each and every component of a PCI DSS environment be secured, it is recommended that all guests on a particular host or hypervisor must be PCI secured.

For E-Business Suite customers who process or store cardholder data using either a private (in-house) or public cloud (hosting vendor) this recommendation by the PCI Security Council is of particular importance. Multi-tenant public clouds or large private clouds may or may not be deemed permissible if all guests components and servers cannot be PCI secured. Compliance, IT security, internal audit teams as well as the PCI QSA should be consulted on the particular details.

# APPENDIX C - PCI DSS REQUIREMENTS

This section will outline the PCI DSS requirements that are relevant to an Oracle E-Business Suite installation and will provide general guidance on complying with each requirement for Oracle E-Business Suite and the underlying technology stack (Oracle Database and Oracle Application Server). Only the requirements that directly relate to the installation and configuration of Oracle E-Business Suite are included. Other requirements, such as change management (Requirement 6), are not included in this paper, but may require operational policies and procedures directly applicable to the Oracle E-Business Suite environment.

The level of detail provided for each requirement will vary since the specific actions or changes required for your Oracle E-Business Suite environment may be dependent on your organization's unique requirements. PCI DSS addresses the entire "cardholder data environment" including networks, servers, and operating systems, however, this paper only addresses the network and operating system in context of Oracle E-Business Suite.

A degree of "Difficulty" to implement the guidance is included for each requirement as a general indicator of the amount of effort in terms of cost (hours/expense) or potential impact of implementing the guidance may have on an average Oracle E-Business Suite environment. In well-controlled and hardened environments, much of the guidance may have already been implemented and little effort will be required to be PCI compliant. However, most organizations will face challenges in implementing "High" difficulty items, especially related to applying Oracle security patches within a month of release (Requirement 6.1), to logging critical database and application events (Requirement 10.2 – 10.6), and to tracking the APPS database account (Requirement 10.1).

| Difficulty | Description |
|---|---|
| **High** | ▪ The guidance or change may involve considerable planning and effort to implement. Additional expense in terms of third-party software, hardware upgrades, or external resources may be required.<br>▪ Implementation may have a significant impact on the operation or maintenance of Oracle E-Business Suite.<br>▪ Non-credit card processing Oracle E-Business Suite modules may be affected in terms of additional security constraints, logging, or patching. |
| **Medium** | ▪ The guidance or change will require planning and effort by the DBA, system administrator, or developers. The overall effort will not require additional expense or outside resources.<br>▪ Implementation may have some impact on the operation or maintenance of Oracle E-Business Suite.<br>▪ Non-credit card processing Oracle E-Business Suite modules may be affected by any such changes, but the impact can be minimized. |
| **Low** | ▪ The guidance or change should be simple to implement by the DBA with low probability of any risk to the environment.<br>▪ Implementation should have minimal impact on the operation or maintenance of Oracle E-Business Suite.<br>▪ Non-credit card processing Oracle E-Business Suite modules will not be affected by any such changes. |

## Requirement 1: Install and maintain a firewall configuration to protect cardholder data

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **1.3** Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files). | Low | Appropriate firewalls should be in place restricting access to the Oracle E-Business Suite database server and all internal application servers.  All external Oracle E-Business Suite Web servers should only be accessible through a reverse proxy server or other such security device.<br>Educational institutions should carefully review all direct public access to Oracle E-Business Suite servers to verify the necessary restrictions are in place. |
| **1.3.1 to 1.3.8** | High | The requirement is that the internal Oracle E-Business Suite servers (web, forms, concurrent manager, database) are not able to communicate directly outside to the Internet, which is difficult to implement in most environments as there are often multiple integration points with third parties (including Payments with the payment processor).  This prevents an attacker from sending externally sensitive data from a compromised server using tools like FTP or database packages such as UTL_HTTP.<br>The solution is to implement a proxy server in the DMZ that will handle all external communications for the Oracle E-Business Suite servers and limit connections to only approved sites (Oracle, Dun & Bradstreet, payment processor, etc.).  All integration points must be verified that they will work with a proxy server. |

## Requirement 2: Do not use vendor-supplied defaults for system passwords and other

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **2.1** Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network.<br>This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, *point-of-sale* (POS*)* terminals, Simple Network Management Protocol (SNMP) community strings, etc.). | Low | In an Oracle E-Business Suite installation, there are two primary sets of default passwords: (1) database accounts and (2) seeded application users.<br>▪ All 250+ default database accounts and Oracle E-Business Suite database accounts passwords must be changed. Use the FNDCPASS utility with the ALLORACLE option to change all the Oracle Application database accounts. Refer to Oracle Metalink Note ID 189367.1 Appendix C for a detailed list of database accounts.<br>▪ All 20+ seed Oracle E-Business Suite users' passwords must be changed and these accounts must be end-dated with the exception of SYSADMIN and GUEST. Even though these accounts are disabled, the passwords must be changed due to inherent flaws in the Oracle E-Business Suite password encryption. |
| **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.<br>Sources of industry-accepted system hardening standards may include, but are not limited to:<br>▪ International Organization for Standardization (ISO)<br>▪ Center for Internet Security (CIS)<br>▪ SysAdmin Audit Network Security (SANS) Institute<br>▪ National Institute of Standards Technology (NIST) | High | The only applicable security configuration standard for Oracle E-Business Suite are listed below for Release 11i and 12 respectively. All mandatory steps must be implemented.<br>Secure Configuration Guide for Oracle E-Business Suite 11i (Doc ID 189367.1)<br>Secure Configuration Guide for Oracle E-Business Suite Release 12 (Doc ID 403537.1)<br>The Oracle Database guidelines from SANS, CIS, and NIST should not be used as these guidelines are not appropriate for an Oracle E-Business Suite database and a number of the recommendations cannot be implemented for an Oracle E-Business Suite database. |
| **2.2.1** Implement only one primary function per server (*for example, web servers, database servers, and DNS should be implemented on separate servers)* | - | The Oracle E-Business Suite architecture supports five types of logical servers: Web, Forms, Concurrent Processing, Database, and Admin. These servers can be centralized into a single server or distributed to multiple servers. See the Oracle E-Business Suite Concepts guide for more information.<br>All Oracle E-Business Suite servers residing in the DMZ must only be Web servers. Internally, the distribution of functions per server will be dependent on the selected topology as outlined in Oracle Metalink Note ID 380490.1 "Oracle E-Business Suite Release 12 Configuration in a DMZ". Whenever feasible, the Web and Forms servers should be separated from the Database, Concurrent Processing, Admin servers in order to isolate data from servers directly handling |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | end-user requests. Oracle E-Business Suite is not a true 3-tier architecture since a significant amount of business logic executes on the database server in the form of database packages. The intent of the requirement is to separate application processing from data storage, which is not feasible with Oracle E-Business Suite. |
| **2.2.2** Enable only necessary services, protocols, daemons, etc., as required for the function of the system. | Low | ▪ The Oracle Reports Server must be disabled if not used.<br>▪ Review all Oracle E-Business Suite features to determine if any unnecessary services can be disabled, such as Discoverer.<br>A separate assessment should performed for Unix/Linux servers and protocols. |
| **2.2.4** Configure system security parameters to prevent misuse | High | All mandatory steps of Oracle Metalink Note ID 189367.1 "Best Practices for Securing Oracle E-Business Suite" must be implemented. |
| **2.2.5** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers. | - | The installation of Oracle E-Business Suite installs all features and modules (250+) regardless of usage or licensing and Oracle does not support the removal of any unnecessary files. |
| **2.3** Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS (transport layer security) for web-based management and other non-console administrative access. | Medium to High | Five types of routine administrative access are required for Oracle E-Business Suite:<br>1. Operating system terminal (Unix, Linux, Windows) – SSH rather than Telnet must be used for access.<br>2. Operating system file transfer – SFTP or SSH (SCP) must be used for all file transfers.<br>3. Database access – This requirement mandates SQL*Net Encryption be implemented for all SQL*Net access to the database in order to encrypt any administrative database access. SQL*Net encryption is available as an add-on product in Advanced Security Option (ASO). Encryption can be implemented selectively by client, but not enforced based on any type of criteria. To force encryption of all administrative access, all SQL*Net traffic will have to be encrypted resulting in additional license expense and potential hardware upgrades to support such encryption (even though PCI doesn't mandate all internal network traffic that may contain cardholder data be encrypted). Another option is to configure a second database listener with encryption for administrative access and use Managed SQL*Net Access on the main listener.<br>4. Web – Access to system administrator responsibilities and Oracle E-Business Suite Manager (OAM) should be done using SSL, therefore, effectively all web access internal and external needs to be encrypted using SSL. For performance reasons and ease of configuration, SSL should be offloaded to a load balancer whenever possible.<br>Forms – System administrator responsibilities use Oracle Forms (Professional Interface) for a number of functions and this access needs to be encrypted. By default, all Forms Server traffic is encrypted using the RC4 stream cipher or can use SSL if the Forms Servlet is configured. |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | Verify that the Forms Server or Forms Servlet is using encryption. |

## Requirement 3: Protect stored cardholder data

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **3.1** Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:<br>▪ Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements<br>▪ Processes for secure deletion of data when no longer needed<br>▪ Specific retention requirements for cardholder data<br>▪ A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention | Medium to High | Review the Oracle E-Business Suite archiving and purging policy in relation to key data elements where cardholder data is stored. In many Oracle E-Business Suite environments, there is no periodic archiving and purging of data and all data is available on-line.<br>PCI DSS requires a quarterly rolling purge process. Overall retention time for the storage of the PAN is normally between one to two years. This is different and separate from business transactions. For example, customer orders within iStore commonly are required to be retained for five to seven years, but the PANs associated with these transactions should be purged after one to two years.<br>There is no single supported method provided by Oracle to purge PAN from Oracle Payments. A few of the individual Oracle modules that use the Secure Payments Repository have limited standard functionality to purge PAN data and Oracle has several bugs and enhancement requests for the purging this data. For details on the individual purge programs, consult the implementation and user guide of respective modules as well as Oracle Support. A few of them are listed below:<br>▪ Service Contracts ”Purge Credit Card Information (OKSCCPURGE)”<br>▪ Payments “Purge Redundant PA-DSS Incidental Data (IBY_PADSS_PURGE)”<br>▪ iExpense “Credit Card Historical Transactions Management (APXCCPUT)” |
| **3.2** Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3 | | |
| **3.2.1** Do not store the full contents of any track from the magnetic stripe (that is on the back of a card, in a chip or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data. | Low | Oracle E-Business Suite natively does not support swiping of credit cards, therefore, no magnetic stripe data is stored – the data model does not support such data. External eCommerce applications integrating with Payments are able to process magnetic stripe data, thus any such applications and use of Payments should be reviewed. |
| ***3.2.2*** Do not store the card-validation code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card not- | Low | The data model does not support permanently storing such data. Payments stores card-validation codes in encrypted format and securely deletes them automatically upon completion of authorization. However, the codes may be written to OA Framework and/or Payments debug |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| present transactions. | | and log files. All logging and debugging related to the OA Framework and Payments should be reviewed. Apache logs also need to be reviewed as Payments uses servlets for communication with both Oracle E-Business Suite and the payment processor. |
| **3.2.3** Do not store the personal identification number (PIN) or the encrypted PIN block. | Low | Oracle E-Business Suite only supports PINless Debit Card transactions, therefore, no PIN block data is stored – the data model does not support such data. External eCommerce applications integrating with Payments are able to process PIN blocks, thus any such applications and use of Payments should be reviewed. |
| **3.3** Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)<br>*Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN; nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale [POS] receipts).* | Low | The Release 12 Secure Payment Repository by default masks all but the last four digits of the PAN. Payment setup configurations allow this to be changed.<br>For cases of legitimate business reasons, Oracle Payments has a menu security function called IBY_CC_SUPER_USER. When this function is added to the “Funds Capture Process Manager” responsibility, it will allow access to unmasked PANs. This feature is ONLY available from Funds Capture Process Manager responsibility, it is not available from any other module forms. iExpense has a similar function called ‘Payments Credit Card Super User’ which can only be added to the ‘Expenses Policy Menu (OIE_POL_MENU). |
| **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:<br>▪ Strong one-way hash functions (hashed indexes)<br>▪ Truncation<br>▪ Index tokens and pads (pads must be securely stored)<br>▪ Strong cryptography with associated key management processes and procedures<br>*The MINIMUM account information that must be rendered unreadable is the PAN.*<br>*If for some reason, a company is unable to encrypt cardholder data, refer to Appendix B: “Compensating Controls for Encryption of Stored Data.”* | Medium to High | **Release 12 Secure Payment Repository protection not enabled:** All PANs are stored unencrypted in the database, thus can be accessed in the database as well as in the database files, database logs, database archive logs, and database backup files.<br>**Release 12 Secure Payment Repository protection enabled:** When the Release 12 Secure Payment Repository encryption is set to immediate, ALL PANs are encrypted when stored and no additional encryption or protection is required.<br>If the Secure Payment Repository is set to scheduled, PANs are unencrypted until the request set ‘Encrypt Sensitive Data Request Set’ is run. iExpense has a similar function called ‘Payments Credit Card Super User’ and must be added to the ‘Expenses Policy Menu (OIE_POL_MENU).<br>**Oracle E-Business Suite (All):** The OA Framework logging system profile option "FND: Debug Log Level" should be set to "Unexpected (6)" or a higher value to prevent the possibility of credit card numbers being included in the log file.<br>**Payments:** Payments servlet debugging should be disabled to prevent writing of cardholder data to debug files. Review all payment system servlet configurations for logging, debugging, |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | temporary, and archiving options and directories to identify any locations where readable cardholder data might be written. |
| **3.4.1** If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. | | Not Applicable. The Secure Payments Repository provides database level encryption. |
| **3.5** Protect encryption keys used for encryption of cardholder data against both disclosure and misuse. | | |
| **3.5.1** Restrict access to keys to the fewest number of custodians necessary | Low | A policy and procedure needs to be developed to manage access to the "Oracle Payment Wallet" when using the Release 12 Secure Payment Repository. The password to the wallet must be kept to a minimum. Ideally, DBAs and system administrators should not have access. |
| **3.5.2**<br>Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:<br>▪ Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key<br>▪ Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device)<br>▪ As at least two full-length key components or key shares, in accordance with anindustry-accepted method | Low | The Oracle Payment Wallet meets this requirement to securely store keys used to encrypt/decrypt cardholder data. Wallets use 3DES encryption and the password to the wallet encrypts the master key stored in the wallet. Once the wallet setup process is complete, a system security key exists in the wallet, and a passwordless version of the wallet named cwallet.sso is created in the same directory as the original wallet file. Do not share wallets, for example to also support SSL. Use a dedicated Oracle wallet for Payments and ensure that operating system and file permissions properly restrict access to the Wallet file only to the E-Business Suite. |
| **3.5.3** Store cryptographic keys in the fewest possible locations. | Low | The Oracle Wallet only requires the master key to be stored in one place. Since the loss of the wallet may result in loss of all PANs, a backup of the wallet should be stored in a second location that is well secured. |
| **3.6** Fully document and implement all key management | | |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| processes and procedures for keys used for encryption of cardholder data, including the following: | | |
| **3.6.1** Generation of strong keys | Low | Requirement met through the Oracle Wallet. It is recommended to use the Payment Wallet's 24 bit system generated key. You import your own system master key. Sub keys are automatically generated. |
| **3.6.2** Secure key distribution<br>**3.6.3** Secure key storage | Low | See requirement 3.5 above |
| **3.6.4** Periodic changing of keys<br>▪ As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically<br>▪ At least annually | Low | The Payment Wallet's system master key should be changed quarterly. To change the wallet (and system key) create a new wallet file in a new location, and provide its path and password as before using the Payments Setup Administrator Responsibility.<br>Registering the new wallet to replace the old wallet will rotate the system key and result in the immediate re-encryption of all data-encryption subkeys with the new system key.  The last step is to remove the old wallet file using a secure wipe utility. It is not sufficient to just free space in the file system with a delete command. The old wallet (both files the *.p12 and the *.sso) needs to be securely wiped. If the instance is on a virtualized server, depending on how memory is locked or shared to the guest, a secure wipe may be even more critical. |
| **3.6.6** Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key) | Low | It is possible for multiple people in the same physical location to enter portions of the Payment Wallet's password for split knowledge and establishment of dual control.  The split keys should be stored in multiple locations as loss of a portion of the key may result in loss of all encrypted PANs. |
| **3.6.7** Prevention of unauthorized substitution of keys | Low | The Payment Wallet's password should be split per requirement 3.6.6 only among the key's custodians. Furthermore, the "Payments Setup Administrator" responsibility should only be granted to the key's custodians. Physical access to the wallet file within the operating system needs to be restricted per requirement 3.5.2.<br>As the password to the wallet is required to open it and/or to register it with the E-Business Suite, therefore, any unauthorized disclosure of the current key could result in unauthorized changes. |

## Requirement 4: Encrypt transmission of cardholder data across open, public networks

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **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.<br>*Examples of open, public networks that are in scope of the PCI DSS are the Internet, WiFi (IEEE 802.11x), global system for mobile communications (GSM), and general packet radio service (GPRS)* | Medium | SSL must be implemented for all Internet accessible Web servers and for all payment processing. Based on Requirements 2.3 and 8.4, SSL should also be implemented for all internal Web servers. For performance reasons and ease of configuration, SSL should be offloaded to a load balancer whenever possible. |
| **4.2** Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.). | | If Oracle Email Center is in use this could be an issue. For example, customer support could receive emails with cardholder data. Policies would need to be developed for the use of Oracle Email Center to meet PCI DSS. |

## Requirement 5: Use and regularly update anti-virus software

No specific actions required for Oracle E-Business Suite.

## REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **6.1** 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. | Low | The Applications DBA should be responsible for monitoring for new Oracle security patches by subscribing to the Oracle security patch mailing list at http://www.oracle.com/technology/deploy/security/securityemail.html. |
| **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 within one month of release. | **Very High** | PCI DSS requirements apply to the entire technology stack for all components within the environment, from the application down through the operating system and including all storage and network components. Oracle Corporation's Critical Path Updates will cover this requirement for the following three components: Oracle E-Business Suite, database and Fusion Middleware.<br>Applying the quarterly Oracle Critical Patch Updates within 30 days of release is an extremely difficult task for most Oracle E-Business Suite implementations. The Critical Patch Updates are cumulative so if one is missed, it will be automatically applied when a later patch is applied.<br>PCI DSS seems clear on this requirement with the statement, "All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses." Organizations must prioritize these patches and devote the necessary resources to test and apply the patches in the required timeframe. |
| **6.3** Develop internal and external software applications (including web-based administrative access to applications) securely, as follows:<br>▪ In accordance with PCI DSS (for example, secure authentication and logging)<br>▪ Based on industry standards and/or best practices<br>▪ Incorporating information security throughout the software-development life cycle<br>***Note****: This applies to all software developed internally as well as bespoke or custom software developed by a third party.* | Low | All Oracle E-Business Suite customizations should require a DBA or security code review prior to migration to production, including review for SQL injection, cross-site scripting, and other common application security vulnerabilities. Coding standards should limit all use of dynamic SQL.<br>A program for the view and production migration is required and evidence of its on-going use is required for Oracle E-Business Suite Customizations, Extensions, Modifications, Localizations and Integrations (CEMLI). |
| **6.4.3** Production data (live PANs) are not used for testing or development. | Medium | Cloning is a standard operation in all Oracle E-Business Suite implementations where the production environment is copied to test, QA, training, and development environments. During the cloning process, all production cardholder data (PANs) must be scrambled or removed. |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | Even though the cardholder data may be encrypted, it still must be scrambled, as it is possible to decrypt the data. |
| **6.4.4.** Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. | Medium | See requirement 6.3. |
| **6.6** For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:<br>▪ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes<br>***Note:*** *This assessment is not the same as the vulnerability scans performed for Requirement 11.2.*<br>▪ Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic. | High | As part of any application penetration tests (see Requirement 11.3.2), all customizations to web-facing modules (iStore, iReceivables, etc.) should be subjected to an application security code review (whitebox) as well as penetration testing (blackbox).<br>All steps in Oracle Metalink Note ID "380490.1 Oracle E-Business Suite Release 12 Configuration in a DMZ" must be implemented for all web-facing Oracle E-Business Suite Web servers, including the absolutely mandatory implementation of the Oracle URL firewall and restricted responsibility access. The critical issue is that Oracle E-Business Suite always installs all web pages for 250+ modules (15,000+ web pages) – the Oracle URL firewall limits access to only the required web pages.<br>Oracle E-Business Suite includes the installation of mod_security on all Web servers, however, the Oracle provided rules are simplistic at best and should not be considered an effective application layer firewall. An external application layer firewall is recommended to provide an additional layer of security.<br>All CEMLI artifacts in web-facing modules (iStore, iReceivables, etc.) should be subjected to an application security code review (whitebox) as well as penetration testing (blackbox). For example, custom forms for iStore that are public-facing need to be penetration tested. |

## REQUIREMENT 7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED-TO-KNOW

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **7.1** Limit access to computing resources and cardholder information only to those individuals whose job requires such access. | Medium | **Application:** The standard Oracle E-Business Suite responsibilities and function security should be sufficient to meet this requirement.  Periodically review all active responsibilities and user assignments to verify that they are appropriate.  All responsibility assignments should require manager approval, especially for any responsibilities that have access to cardholder data.<br>**Database:** DBAs and system administrators with production access should be appropriately limited. Tools such as a password safe can assist with this by limiting password access only to specific teams and/or individuals.<br>All Oracle DBAs may or may not have access to the production E-Business Suite, as well pay close attention to monitoring teams and automated monitoring tools. Meeting service level agreements and responding to monitoring alerts cannot jeopardize the protection of cardholder data. |
| **7.2** Establish a mechanism for systems with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed. | Medium | **Application:** The standard Oracle E-Business Suite responsibilities and function security should be sufficient to meet this requirement.  The seeded Oracle E-Business Suite responsibilities should not be used and custom responsibilities should be created to support appropriate segregation of duties and limited access to cardholder data.<br>**Database:** Individual user accounts should be used to authenticate and authorize per job function. For example, a password safe could assist with meeting this requirement. Direct database access to production can be set up as "deny all" and only those members of specific groups with approvals would be granted access to the APPS password for production. |

## REQUIREMENT 8: ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **8.1** Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows: | | |
| **8.1.1** Identify all users with a unique user name before allowing them to access system components or cardholder data. | Medium | **Application:** All application user accounts must be individual accounts – no generic accounts should be used. On a periodic basis, all responsibilities and user assignments should be reviewed for appropriate access to cardholder data.<br>**Database:** Only database accounts linked to an individual user should be created with specific permissions limiting access to cardholder data. See requirement 10.1 for information on the APPS account. |
| **8.1.4** Remove/disable inactive user accounts at least every 90 days. | Medium | **Application:** Inactive accounts in Oracle E-Business Suite cannot be removed, only end-dated in order to preserve referential integrity. End-dating of stale application accounts is a manual process and requires the creation of scripts and/or reports.<br>**Database:** Removal of stale database accounts is a manual process and requires the creation of scripts and/or reports to identify such accounts. |
| **8.1.5** Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:<br>▪ Enabled only during the time period needed and disabled when not in use<br>▪ Monitored when in use | Medium | For those E-Business Suite customers using third party services and/or are being hosted, this requirement is particularly challenging. E-Business suite application user accounts need to be set up for third party vendors as well as standard auditing for these accounts. For direct database access by DBAs, individual user accounts and auditing will also be required. Likewise, system administrators with server access will need to be managed. Furthermore, 24x7 monitoring and event response access processes will also need to meet this requirement. |
| **8.1.6** Limit repeated access attempts by locking out the user ID after not more than six attempts. | Low | **Applications:** The system profile option "Sign-on Password Failure Limit" should be set to a maximum of "6" at the site level.<br>**Database:** All individual database accounts should have a database profile with FAILED_LOGIN_ATTEMPTS set to a maximum of 6. FAILED_LOGIN_ATTEMPTS should not be set for Oracle E-Business Suite database accounts, rather an alert should be set after 6 failed login |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | attempts. |
| **8.1.7** Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. | Low | **Applications:** Locked application accounts must be manually unlocked.<br>**Database:** All individual database accounts should have a database profile with PASSWORD_LOCK_TIME set to UNLIMITED to require manual unlocking. |
| **8.1.8** If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. | Low | **Applications:** To enable a 15 minute timeout, use AutoConfig to set the variable s_sesstimeout to 900000 (milliseconds) – this will set the timeout in the zone.properties file and the system profile option "ICX:Session Timeout". See Metalink Note ID 307149.1 for more information. This feature should be thoroughly tested, as there have been numerous issues in the past with the timeout working correctly.<br>**Database:** There is no feature in the Oracle Database that exactly satisfies this requirement. All individual database accounts should have a database profile with IDLE_TIME set to 15 minutes, but this will only terminate sessions that have been idle with no activity for 15 minutes. If a database session is open with a long running query or other process running, the session will remain open until 15 minutes after the query or process has completed. |
| **8.2** In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users:<br>▪ Password<br>▪ Token devices (e.g., SecureID, certificates, or public key)<br>▪ Biometrics | None | **Application:** The standard Oracle E-Business Suite passwords should be sufficient to meet this requirement. See section 8.5 for additional requirements related to passwords.<br>**Database:** The standard Oracle Database passwords should be sufficient to meet this requirement. See section 8.5 for additional requirements related to passwords. |
| **8.2.1** Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components. | High | **Application:** (1) With the standard Oracle E-Business Suite login process, passwords are sent in plain-text across the network if HTTP is being used. This requirement mandates SSL be used for Oracle E-Business Suite Web servers. Requirement 2.3 also mandates the use of SSL for all administrative access. For performance reasons and ease of configuration, SSL should be offloaded to a load balancer whenever possible. (2) There is a specific weakness in the Oracle Application password encryption that may allow an insider to decrypt all user passwords given sufficient privileges to the database (see Integrigy's whitepaper "Oracle E-Business Suite Password Decryption" for more information).<br>**Database:** Oracle Database passwords are sent encrypted across the network and should be sufficient to meet this requirement. SQL*Net encryption is not required as is the case for |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | Requirement 2.3. |
| **8.2.2** Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys. | Low | **Application:** The standard Oracle E-Business Suite password reset functionality (available in 11.5.10.2 or 11i.ATG_PF.H.RUP4) works by sending a new user password to the user's e-mail address. See Metalink Note ID 399766.1 for more information. This process should be sufficient to meet this requirement.<br>In older versions, the password reset is a manual process.<br>**Database:** Password resets for the database are a manual process. |
| **8.2.3** Passwords/phrases must meet the following:<br>▪ Require a minimum length of at least seven characters.<br>▪ Contain both numeric and alphabetic characters.<br>▪ Alternatively, the passwords/phrases must have complexity and strength at least equivalent to | Low | **Application**: The system profile option "Signon Password Length" should be set to a minimum of "7" at the site level. As well, the system profile option "Signon Password Hard to Guess" should also be set to "True" at the site level.<br>**Databas**e: To require a minimum password length, a custom "database password verify function" must be created. This should be set for all database profiles using the PASSWORD_VERIFY_FUNCTION parameter.<br>**Database**: To require a complex password, a custom "database password verify function" must be created. This should be set for all database profiles using the PASSWORD_VERIFY_FUNCTION parameter. |
| **8.2.4** Change user passwords/passphrases at least every 90 days. | Low | **Application:** All application accounts should be setup with password expiration set to 90 days.<br>**Database:** All individual database accounts should have a database profile with PASSWORD_LIFE_TIME set to 90 days. For all Oracle E-Business Suite database accounts, a policy rather than database profile should be in place to require all these passwords to be changed at least every 90 days. |
| **8.2.5** Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used. | Low | **Applications:** The system profile option "Signon Password No Reuse" should be set to a minimum of "450" days at the site level, which should be equivalent to the last four passwords when passwords are changed every 90 days.<br>**Database:** All database profiles should have PASSWORD_REUSE_MAX set to 4. |
| **8.2.6** Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. | Low | **Application:** All new application accounts must be created with a unique and strong password. Prior to 11.5.10 and User Management (UMX), the password assignment is a manual process. In 11.5.10, User Management should be used to generate a unique and strong password. |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | **Database:** User creation for the database is a manual process. All new database accounts must be created with a unique and strong password. |
| **8.5** Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:<br>▪ Generic user IDs are disabled or removed.<br>▪ Shared user IDs do not exist for system administration and other critical functions.<br>▪ Shared and generic user IDs are not used to administer any system components. | Medium | **Application:** Historically, shared application accounts are used to manage concurrent processing. Only individual user accounts should be created and all shared application accounts need to be end-dated.<br>**Database:** Many Oracle E-Business Suite databases have shared read-only (e.g., APPS_READ) or other ad-hoc query accounts. These accounts must be removed and replaced with individual database accounts that have a limited set of permissions. See Requirement 10.1 for information on the APPS accounts. |
| **8.7** All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:<br>▪ All user access to, user queries of, and user actions on databases are through programmatic methods.<br>▪ Only database administrators have the ability to directly access or query databases.<br>▪ Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes). | Low | **Database:** Only database accounts linked to an individual user should be created with specific permissions limiting access to cardholder data. See requirement 10.1 for information on the APPS account. |

## REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

No specific actions required for Oracle E-Business Suite. General IT policies and procedures may be required for the Oracle E-Business Suite environment.

## REQUIREMENT 10: TRACK AND MONITOR ALL ACCESS TO NETWORK RESOURCES AND CARDHOLDER DATA

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **10.1** Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. | Medium | **Application:** All application users should have individual application accounts and no generic accounts should be used under any circumstances. The SYSADMIN should not be locked as this is not supported by Oracle. As a matter of policy, all use of the SYSADMIN account should require a change request and all logins to SYSADMIN should be reviewed on a periodic basis.<br>**Database:** Procedures need to be established to control use of the APPS account and document all access. DBAs should have individual database accounts and only use the APPS account for required maintenance. All such use should be documented in a change control ticket.<br>**Operating System:** All access to the "oracle" or "applmgr" operating system accounts needs to be linked to an actual user. Use a tool like Sudo or Symark PowerBroker to provide detailed tracking of usage and for mapping usage to individual operating system accounts. |
| **10.2** Implement automated audit trails for all system components to reconstruct the following events: | | **A comprehensive database and application auditing solution needs to be implemented that satisfies the PCI requirements, protects the audit trail, and does not adversely impact application performance. Without the implementation of third-party products, the application and database audit trail can usually be manipulated by the DBA. There are a number of auditing options available including using the standard auditing functionality in the application and database, developing custom auditing solutions, using LogMiner with database archive logs, and/or implementing third-party products. The design of an auditing solution depends on the implementation size, modules implemented, if credit card encryption is used, and the availability of or ability to purchase third-party tools.** |
| **10.2.1** All individual user accesses to cardholder data | High | **Application:** The standard application controls should be sufficient to restrict access to cardholder data. The system profile option " Sign-On:Audit Level" must be set to "Forms" at the site level to provide an audit trail of all user signons and access to forms that may display cardholder data. This audit trail can be manipulated by the DBA. |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | **Database:** Since cardholder data is stored with the other transaction data in some modules, auditing of access to these tables may severely impact performance. See Requirement 10.2 |
| **10.2.2** All actions taken by any individual with root or administrative privileges | High | See Requirements 10.1 and 10.2 |
| **10.2.3** Access to all audit trails | High | See Requirement 10.2 |
| **10.2.4** Invalid logical access attempts | Low | **Application:** Logging of unsuccessful login attempts is standard functionality. This audit trail can be manipulated by the DBA.<br>**Database:** Database session auditing should be enabled. This audit trail potentially can be manipulated by the DBA. |
| **10.2.5** Use of identification and authentication mechanisms | High | See Requirement 10.2 |
| **10.2.6** Initialization of the audit logs | High | See Requirement 10.2 |
| **10.2.7** Creation and deletion of system-level objects | High | See Requirement 10.2 |
| **10.3** Record at least the following audit trail entries for all system components for each event:<br>**10.3.1** User identification<br>**10.3.2** Type of event<br>**10.3.3** Date and time<br>**10.3.4** Success or failure indication<br>**10.3.5** Origination of event<br>**10.3.6** Identity or name of affected data, system component, or resource | - | See Requirement 10.2<br>All audit trails should be reviewed for susceptibility to spoofing of Oracle Database session information to determine the impact on forensic examinations in the event of a data breach. See Integrigy's whitepaper "Spoofing Oracle Session Information" for more information. |
| **10.5** Secure audit trails so they cannot be altered. | | |
| **10.5.1** Limit viewing of audit trails to those with a job-related need | High | See Requirement 10.2 |
| **10.5.2** Protect audit trail files from unauthorized modifications | High | See Requirement 10.2 |
| **10.5.3** Promptly back-up audit trail files to a centralized log server or media that is difficult to alter | High | See Requirement 10.2 |
| **10.5.5** Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts | High | See Requirement 10.2 |

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| (although new data being added should not cause an alert). | | |
| **10.6** Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).<br>*Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with Requirement 10.6.* | High | See Requirement 10.2 |
| **10.7** Retain audit trail history for at least one year, with a minimum of three months online availability. | High | See Requirement 10.2 |

## Requirement 11: Regularly test security systems and processes

| PCI DSS Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **11.3** Perform penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:<br>**11.3.1** Network-layer penetration tests<br>**11.3.2** Application-layer penetration tests | High | This requirement mandates periodic application-layer penetration tests for applications that "store, process, or transmit cardholder data." The application penetration tests should include Oracle E-Business Suite if any significant volume of cardholder data is stored or processed by the application. All Internet-facing Oracle E-Business Suite modules (such as iStore, iReceiveables, etc.) must be included in any penetration tests and a firm experienced with Oracle E-Business Suite penetration testing should be utilized to conduct any such application penetration tests. When conducting penetration testing, be sure to provide all external Oracle E-Business Suite URLs in the scope of penetration testing. |
| **11.5** Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files; and configure the software to perform critical file comparisons at least weekly.<br>*Critical files are not necessarily only those containing cardholder data. For file integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is the merchant or service provider).* | High | Implementing file integrity monitoring software with Oracle E-Business Suite is difficult due to the complexity of the application and the sheer volume of files (750,000+). Fortunately, the requirement is only to monitor "critical system or content files." The critical system files should include the key Oracle Database, Oracle Application Server, and Oracle E-Business Suite configuration files. These files should only change when AutoConfig is run to re-instantiate these files. Review the AutoConfig template driver files ($AD_TOP/admin/driver/adtmpl.drv and $FND_TOP/admin/driver/fndtmpl.drv) to obtain a list of critical configuration files and locations.<br>Another key aspect of this requirement is that any generated alerts are reviewed by appropriate personnel. Be sure the necessary procedures and processes are in place to review such alerts.<br>In Release 12, the Oracle E-Business Suite file system has been reorganized to make all the "homes" read-only and have a separate INSTANCE_HOME with configuration files, logs, and certificates. Monitoring this configuration will be much easier with all routinely changing files in one location. |

## Requirement 12: Maintain a policy that addresses information security

No specific actions required for Oracle E-Business Suite. General IT policies and procedures may be required for the Oracle E-Business Suite environment.

# APPENDIX D - COMPENSATING CONTROLS FOR REQUIREMENT 3.4

Compensating controls are required when the Oracle E-Business Suite Credit Card Encryption functionality cannot be implemented for technical or business reasons. "Only companies that have undertaken a risk analysis and have legitimate technological or documented business constraints can consider the use of compensating controls to achieve compliance." (PCI DSS Appendix B) The risk analysis and business rationale for not implementing the Oracle E-Business Suite Credit Card Encryption should be documented.

Compensating controls must adhere to the following four criteria –

1. "meet the intent and rigor of the original stated PCI DSS requirement"
2. "repel a compromise attempt with similar force"
3. "be 'above and beyond' other PCI DSS requirements (not simply in compliance with other PCI DSS requirements)"
4. "be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement"

It is important to note that the compensating controls must be preventative and be in addition to other controls implemented for PCI compliance. See Appendix B of the PCI DSS document for more details on establishing compensating controls to protect cardholder data.

| PCI DSS Compensating Control Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| **1.** Provide additional segmentation/abstraction (for example, at the network-layer) | High | ▪ The "Managed SQL*Net Access" feature should be enabled for Release 12 or Valid Node Checking be enabled for previous releases. Only the Oracle E-Business Suite application servers, data center servers for interfaces, and DBAs should be permitted direct SQL*Net access to the database. |
| **2.** Provide ability to restrict access to cardholder data or databases based on the following criteria:<br>▪ IP address/Mac address<br>▪ Application/service<br>▪ User accounts/groups<br>▪ Data type (packet filtering) | Medium | ▪ All responsibilities should be periodically reviewed for appropriate access to cardholder data.<br>▪ All masking system profile options need to be set for configured modules. |
| **3.** Restrict logical access to the database<br>▪ Control logical access to the database independent of Active Directory or Lightweight Directory Access Protocol (LDAP) | High | ▪ The "Managed SQL*Net Access" feature should be enabled for Release 12 or Valid Node Checking be enabled for previous releases. Only the Oracle E-Business Suite application servers, data center servers for interfaces, and DBAs should be permitted direct SQL*Net access to the database.<br>▪ No ad-hoc query or reporting database accounts should allowed or these accounts are restricted access to all PAN columns. |
| **4.** Prevent/detect common application or database attacks (for example, SQL injection) | Medium | ▪ The Oracle E-Business Suite URL firewall (url_fw) or Integrigy's AppDefend application firewall should be implemented for all internal web servers as well as any external web servers. |

| PCI DSS Compensating Control Requirement | Difficulty | Oracle E-Business Suite Guidance |
|---|---|---|
| | | Oracle E-Business Suite automatically installs all 250+ modules regardless of use or licensing, therefore, there are more than 15,000 accessible web pages. Access should be blocked to all unnecessary web pages as those unused web pages may contain SQL injection or cross-site scripting flaws.<br>▪ Intrusion Detection (IDS) or intrusion prevention systems should be implemented for all external web servers and potentially for all internal Oracle E-Business Suite servers. Oracle Database specific IDS/IPS products should be evaluated if "Managed SQL*Net Access" is not enabled. When evaluating database IDS/IPS products, review Integrigy's whitepaper "Evading Network-Based Oracle Database Intrusion Detection Systems" for common methods of evading network-based IDS. |
| **5.** Other Encryption Options<br>▪ Database files<br>▪ Log files<br>▪ Backups | High | ▪ A number of options exist to encrypt the PANs in the database and backup files when the Credit Card Encryption Patch is not installed. Oracle's Transparent Data Encryption (TDE) is certified with Oracle E-Business Suite and Oracle Database 10.2, which can be used to transparently encrypt specific columns when stored in the data files. Oracle Secure Backup may be used for creating encrypted database backups. Other third-party products may be utilized for database encryption or secure backups, however, these products may not work properly with Oracle E-Business Suite or require significant configuration or customization. |

# References

## General Credit Card Information

1. " Anatomy of Credit Card Numbers", Hitesh Malviya
   http://dl.packetstormsecurity.net/papers/general/creditcard-anatomy.pdf

## Payment Card Industry Data Security Standard

1. "Payment Card Industry Data Security Standard 3.0 Release November 2013", PCI Security Standards Council, https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm
2. "Payment Card Industry Data Security Standard Self-Assessment Questionnaire D version 2.0, October 2010", PCI Security Standards Council, https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs
3. "Payment Card Industry Data Security Standard Security Audit Procedures 1.1 April 2008", PCI Security Standards Council, https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf
4. "Payment Card Industry Data Security Standard Glossary", PCI Security Standards Council, October 2010, https://www.pcisecuritystandards.org/documents/pci_glossary_v20.pdf
5. "Cardholder Information Security Information Program (CISP) Payment Application Best Practices 1.4", Visa U.S.A., 4 January 2007, http://usa.visa.com/download/merchants/cisp_payment_application_best_practices.doc
6. "CISP Bulletin Clarifications to PCI Requirements 3.4 and 10.2-10.3", Visa U.S.A., 28 July 2006, http://usa.visa.com/download/business/accepting_visa/ops_risk_management/pci_clarification_assessors.pdf
7. “Information Supplement: PCI DSS Cloud Computing Guidelines, version 2”, February 2013, PCI Security Standards Council. https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Cloud_Guidelines.pdf
8. “Information Supplement: PCI DSS Virtualization Guidelines, version 2”, June 2011, PCI Security Standards Council, https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

## Oracle E-Business Suite Security

Note: Access to Oracle Metalink notes requires an Oracle Metalink account.

1. "Oracle E-Business Suite Password Decryption", Stephen Kost and Jack Kanter, Integrigy Corporation, 9 January 2007, http://www.integrigy.com/files/Integrigy%20Oracle%20EBS%20Account%20Password%20Decryption%20Threat%20Explored%20v1.pdf
2. "Evading Network-Based Oracle Database Intrusion Detection Systems", Stephen Kost and Jack Kanter, Integrigy Corporation, 11 December 2006, http://www.integrigy.com/security-resources/evading-network-based-oracle-database-intrusion-detection-systems
3. "Spoofing Oracle Session Information", Stephen Kost and Jack Kanter, Integrigy Corporation, 12

November 2006, http://www.integrigy.com/files/Integrigy_Spoofing_Oracle_Session_Information.pdf

4. "Secure Configuration Guide for Oracle E-Business Suite Release 12", Oracle Metalink Note ID 403537.1, Oracle Corporation, 9 October 2013, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=403537.1
5. "Oracle E-Business Suite R12 Configuration in a DMZ", Oracle Metalink Note ID 380490.1, Oracle Corporation, 15 August 2013, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=380490.1

## ORACLE E-BUSINESS SUITE AND CREDIT CARDS

Note: Access to Oracle Metalink notes requires an Oracle Metalink account.

1. "How To Enable Oracle Payments Data Encryption Functionality", Oracle Metalink Note ID 1301337.1, Oracle Corporation, 1 November 2013 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=1301337.1
2. "All About Oracle Payments Release 12 Wallets And Payments Data Encryption", Oracle Metalink Note ID 1573912.1, Oracle Corporation, 16 September 2013 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=1573912.1
3. "R12: Understanding What the Oracle EBS "Payments" (IBY) module Is, and What It Does", Oracle Metalink Note ID 1391460.1, Oracle Corporation, 21 June 2013 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=1391460.1
4. "Oracle Payment Application Data Security Standard (PA DSS) Consolidated Patch Release Notes, Release 12.1.2", Oracle Metalink Note ID 981033.1, Oracle Corporation, 12 November 2012 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=981033.1
5. "Payment Applications Best Practices", Oracle Metalink Note ID 738344.1, Oracle Corporation, 28 January 2010 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=738344.1
6. "Frequently Asked Questions: Bank Account Masking Internal, External and Application Level", Oracle Metalink Note ID 1504653.1, Oracle Corporation, 20 November 2013 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=1504653.1
7. "How To Reset Oracle Payments Encryption Wallet Location After Instance", Oracle Metalink Note ID 1571608.1, Oracle Corporation, 5 August 2013 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=1571608.1)
8. "iPayment Wallet Explained", Oracle Metalink Note ID 602155.1, Oracle Corporation, 4 November 2013 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id

=602155.1

9. "How To Rotate Payments Encryption Wallet Password and Security Key Periodically For PCI Compliance", Oracle Metalink Note ID 1300956.1, Oracle Corporation, 9 October-2013 https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=1300956.1
10. "How to generate Debug Log Files for Oracle Payments Funds Capture R12**?**", Oracle Metalink Note ID 452830.1, Oracle Corporation, 9 August-2013, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=452830.1

# History

## Change History

| | | |
|---|---|---|
| 1.1.0 | January 29, 2007 | Initial Version<br>▪ Version number corresponds with PCI DSS 1.1 version |
| 1.1.1 | October 10, 2010 | ▪ Minor updates to include additional logging<br>▪ Updated to include new Oracle Metalink notes |
| 1.1.2 | March 28, 2010 | ▪ Minor updates |
| 2.0.0 | April 27, 2011 | ▪ Update to PCI DSS 2.0 version<br>▪ Change all Oracle E-Business Suite references to Oracle E-Business Suite<br>▪ Update to include Oracle E-Business Suite R12 |
| 3.0.0 | January 2014 | ▪ Updated for PCI DSS 3.0 version<br>▪ Numerous updates and enhancements |
| 3.0.1 | January 2014 | ▪ Clarifications and updates |
| 3.0.3 | April 2016 | ▪ Clarifications and updates |

## About Integrigy

**Integrigy Corporation (www.integrigy.com)**

Integrigy Corporation is a leader in application security for enterprise mission-critical applications.  AppSentry, our application and database security assessment tool, assists companies in securing their largest and most important applications through detailed security audits and actionable recommendations.  AppDefend, our enterprise web application firewall is specifically designed for the Oracle E-Business Suite.  Integrigy Consulting offers comprehensive security assessment services for leading databases and ERP applications, enabling companies to leverage our in-depth knowledge of this significant threat to business operations.

INTEGRIGY
Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60681 USA
888/542-4802
**www.integrigy.com**