INTEGRIGY

WHITE PAPER

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

APRIL 2011

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

Version 1.1.0 - January 29, 2007
Version 1.1.1 – October 10, 2009
Version 1.1.2 – March 28, 2010
Version 2.0.0 – April 27, 2011

Authors: Stephen Kost and Jack Kanter

If you have any questions, comments, or suggestions regarding this document, please send them via e-mail to alerts@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 large 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 a Report on Compliance. 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 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 2.0 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 2.0 regardless of size or transaction volume. The PCI Data Security Standard (DSS) 2.0 is a set of stringent security requirements for networks, network devices, servers, and applications. The standard details specific requirements in terms of security configuration and policies and all the requirements are mandatory. PCI DSS is focused on securely handling cardholder data, but also has a significant emphasis on general IT security.

The difficultly with Oracle E-Business Suite and achieving PCI compliance is that even though credit card processing may be only a 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 Oracle E-Business Suite. In a large global implementation that includes financials, manufacturing, and human resources, PCI compliance can be a daunting endeavor and will impact operations and management of the non-card processing modules.

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 on complying with relevant PCI DSS requirements.

PCI Compliance

The Payment Card Industry Data Security Standard 2.0 is specific about the scope of systems and applications to be included as part of the compliance effort –

> *"… 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 Payment Card Industry Data Security Standard 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.

Oracle E-Business Suite and PCI Compliance

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

The difficultly with Oracle E-Business Suite and achieving PCI compliance is that even though credit card processing may be only a 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 Oracle E-Business Suite.

The only exception to PCI DSS compliance may be the storage and use of employee cardholder data in Oracle Internet Expenses (OIE). In such an implementation where this is the only cardholder data in the database, the organization is technically not a merchant nor service provider. You should consult your legal counsel or a PCI Qualified Security Assessor for clarification on this possible exception and any potential compliance requirements and liability related to maintaining such data.

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 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 input to your PCI compliance effort specifically related to Oracle E-Business Suite, but not to be an authoritative reference in terms of Oracle E-Business Suite and PCI compliance. Integrigy Corporation and the authors of this paper are not qualified PCI assessors, 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.

Glossary

As American Express, MasterCard, and VISA have different names for the various credit card data elements, this paper will use 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 such 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.
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 – ▪ CAV2 = Card Authentication Value 2 = JCB ▪ CID = Card Identification Number = American Express ▪ CID = Card Identification Number = Discover ▪ CVC2 = Card Validation Code 2 = MasterCard ▪ CVV2 = Card Verification Value 2 = Visa

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

Credit Card Data

In order to comply with the Payment Card Industry Data Security Standard, it is important to first understand how Oracle E-Business Suite handles and processes credit card information. The core credit card processing module is iPayment, which provides the integration between the application and financial institutions and payment processors for payment and receipt processing. Within Oracle E-Business Suite, each module that handles credit cards integrates with iPayment, but has its own forms, web pages, and/or reports for entering and displaying credit card information.

With a default installation of Oracle E-Business Suite, there is no encryption of cardholder data and masking of primary account numbers is handled by each module. An optional patch is available for Oracle E-Business Suite that implements credit card encryption and centralizes the storage of primary account numbers. The next two sections of this paper describe the default credit card handling and then the features of the new credit card encryption patch.

Oracle E-Business Suite Standard Credit Card Processing

The default Oracle E-Business Suite installation provides no standard capability to encrypt credit card data and is a patchwork of module-centric storage and masking of primary account numbers. Encryption of PANs can be enabled by applying an optional patch – see Section 2.2 for more information on the Oracle Application Credit Card Encryption patch.

Credit Card Data Storage (Requirement 3.4)

The storage of credit card data in Oracle E-Business Suite is decentralized and is stored by module. PANs are not encrypted, except in the iPayment module for external ecommerce applications if the optional encryption is enabled. The following table highlights the major credit card processing modules and the tables used to store credit card data –

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
iPayment (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

iPayment Encryption

Beginning with iPayment Minipack 11i.IBY.O (patch 3042827), cardholder data that is processed for non-Oracle E-Business Suite ecommerce applications can be encrypted in iPayment using the "Payee Security Key" feature. Primary account number encryption can be setup per payee and requires a unique security key for each payee. However, the security keys must be entered using the iPayment security page whenever the web server is restarted, thus in effect requiring the DBA to know the security keys.

Credit Card Number Masking (Requirement 3.3)

The masking of PANs is module dependent and each module has a different system profile option to enable masking. These system profile options may be set at the site, responsibility, application, or user level. The following table highlights some of the system profile options used to control the display of credit card information –

Module	System Profile Option	Profile Option Description
Accounts Receivables (AR)	AR: Mask Bank Account Numbers ▪ Mask - First Four Visible ▪ Mask - Last Four Visible ▪ No Masking	Used to determine how, if at all, the bank account or credit card numbers should be masked
iPayment (IBY)	IBY: UI Visibility Class ▪ Receivables Clerk Visibility ▪ Payroll Clerk Visibility ▪ Default Payment Administrator Visibility	Determine what data will be visible for an user in iPayment operations UI
Order Management (ONT)	OM: Credit Card Privilege ▪ All, Limited, None	Privileges to control the Credit Card related information and processing
Service Contracts (OKS/OKC)	OKS: Credit Card Display Privileges ▪ All, Limited, None	Determines how much of customer's credit card number is displayed
Student System (IGS)	IGS: Mask Credit Card Number ▪ Mask - First Four Visible ▪ Mask - Last Four Visible ▪ No Masking	To mask credit card number in receipt form

Oracle E-Business Suite Credit Card Encryption Patch

Oracle introduced new credit card security features in December 2005 as a controlled release patch and the patch was generally available in May 2006. This patch provides three new features for securing cardholder data: (1) consolidation of primary account numbers from four tables to one, (2) encryption of primary account numbers, and (3) automatic masking of primary account numbers. Manual steps are required to migrate existing primary account numbers to the new encryption scheme and to enable encryption. This patch does not include encryption support for the following modules:

- Oracle Internet Expenses (OIE), encryption is expected to be in Release 12
- Oracle Student System (IGS), requires 11i.IGS.M Rollup 1 to enable encryption

Information on the new Credit Card Encryption feature is available in Metalink Note ID 338756.1 "Oracle E-Business Suite Credit Card Encryption, Release 11i" and the patch number is 4607647. At a minimum, 11.5.9 or 11.5.10.2 is required along with the most recent family packs for Financials (11i.FIN_PF.G), Marketing and Sales Suite (11i.MAS_PF.A Rollup 2), and Supply Chain (11i.SCM_PF.J). Due to the prerequisites, 11.5.9 installations may have to upgrade to 11.5.10.2 (or Release 12) in order to apply the patch and enable encryption.

Credit Card Data Storage (Requirement 3.4)

The credit card encryption is only for the Primary Account Number (PAN) and not other cardholder data such as cardholder name or card expiration date – all data, except for the PAN, remain as is in the existing tables. Only encrypting the PAN meets the PCI DSS "MINIMUM account information that must be rendered unreadable" (per Requirement 3.4). The existing PAN column is replaced with a reference to the encrypted PAN in the new IBY.IBY_SECURITY_SEGMENTS table. The PANs are encrypted using PCI DSS accepted Triple DES (3DES) with a 192-bit key (of which 168 bits are used) via the standard Oracle package DBMS_OBFUSCATION_TOOLKIT. It is interesting to note that Oracle E-Business Suite is using the deprecated DBMS_OBFUSCATION_TOOLKIT package rather than the newer DBMS_CRYPTO package.

The encrypted PAN as well as the last four numbers of the PAN are stored in the IBY.IBY_SECURITY_SEGMENTS table – allowing for the display of the masked PAN without having to decrypt the PAN. The PAN is also stored as an MD5 hash (using the DBMS_OBFUSCATION_TOOLKIT package) in the table to allow for secure searching/matching of PANs.

Credit Card Key Management (Requirement 3.6)

A single "iPayment System Key" is set using the System Security Management page under the iPayment Payment Administrator responsibility. A policy and procedure for properly managing the iPayment System key must be created to satisfy Requirement 3.6, which requires secure key generation, dual control of the key, and periodic rotation of the key. Under no circumstances should the DBA or system administrator have knowledge of or access to this key.

The iPayment System Key is then stored encrypted in the FND_VAULT using the system-generated "FND Vault Key". The iPayment System Key is used to encrypt a set of subkeys that are actually used to encrypt the PANs. When the iPayment System Key is rotated, only the subkeys are re-encrypted and not the PANs.

Credit Card Number Masking (Requirement 3.3)

By default, the PAN will be masked regardless of responsibility or even if encryption is not enabled. Unmasked PANs may only be viewed in the Customer Standard form (ARXCUDCI) if patches 5666402 and 5502540 are applied and by assigning security function IBY_UNMASK_SENSITIVE_DATA to the appropriate responsibility menu.

PCI COMPLIANCE

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 organizations 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. ▪ Implementation may have a significant impact on the operation or maintenance of Oracle E-Business Suite. ▪ 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. ▪ Implementation may have some impact on the operation or maintenance of Oracle E-Business Suite. ▪ 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. ▪ Implementation should have minimal impact on the operation or maintenance of Oracle E-Business Suite. ▪ 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
1.4 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. Educational institutions should carefully review all direct public access to Oracle E-Business Suite servers to verify the necessary restrictions are in place.
1.4.2 Restrict outbound traffic from payment card applications to IP addresses within the DMZ.	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 iPayment 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. 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 limits 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 **before** installing a system on the network (for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts).	Low	In an Oracle E-Business Suite installation, there are two primary sets of default passwords: (1) database accounts and (2) seeded application users. ▪ 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. ▪ 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 as defined, for example, by SANS, National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).	High	The only applicable security configuration standard for Oracle E-Business Suite is Oracle Metalink Note ID 189367.1 "Best Practices for Securing Oracle E-Business Suite". All mandatory steps must be implemented. 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. 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 17368.1 "Advanced Configurations and Topologies for Enterprise Deployments of E-Business Suite 11i". 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 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 Disable all unnecessary and insecure services and protocols *(services and protocols not directly needed to perform the devices' specified function)*	Low	▪ The Oracle Reports Server must be disabled if not used. ▪ Review all Oracle E-Business Suite features to determine if any unnecessary services can be disabled, such as Discoverer. ▪ A separate assessment should performed for Unix/Linux servers and protocols.
2.2.3 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.
2.2.4 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: 1. Operating system terminal (Unix, Linux, Windows) – SSH rather than Telnet must be used for access. 2. Operating system file transfer – SFTP or SSH (SCP) must be used for all file transfers. 3. Database access – This requirement mandates SQL*Net Encryption be implemented for all SQL*Net access to the database in order 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. 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. 5. 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. 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. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	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. Oracle E-Business Suite has no cardholder data specific purging routines, therefore, only when the parent data elements (like orders or receipts) are purged is the cardholder information purged.
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 iPayment are able to process magnetic stripe data, thus any such applications and use of iPayment 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-present transactions.	Low	Only the Oracle E-Business Suite modules Accounts Receivables (iReceivables) and iPayment currently support card validation codes. Order Management will support card validation codes in Release 12. The data model does not support storing such data, however, the codes may be written to OA Framework and/or iPayment debug and log files. All logging and debugging related to the OA Framework and iPayment should be reviewed. Apache logs also need to be reviewed as iPayment 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 iPayment are able to process PIN blocks, thus any such applications and use of iPayment 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) *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).*	Medium	**Oracle E-Business Suite (No Credit Card Encryption Patch):** Review the system profile options at the Site, Application, Responsibility, and User levels for each configured module to determine if the appropriate masks are configured. **Oracle E-Business Suite (With Credit Card Encryption Patch):** All PANs are automatically masked, except for the Customer Standard form when the security function IBY_UNMASK_SENSITIVE_DATA is assigned to a responsibility menu. Review all responsibilities where this security function is enabled. **iPayment:** The iPayment UI visibility masks should be reviewed and assignments for the system profile option "IBY: UI Visibility Class" need to be reviewed at the Site, Application, Responsibility, and User levels to determine if appropriate masks are configured. Only an individual authorized to view all credit card data should have access to the "System Administrator for iPayment responsibility".
3.4 Render PAN, at minimum, unreadable anywhere it is stored (including data on portable digital media, backup media, in logs, and data received from or stored by wireless networks) by using any of the following approaches: • Strong one-way hash functions (hashed indexes) • Truncation • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key management processes and procedures *The MINIMUM account information that must be rendered unreadable is the PAN.* *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	**Oracle E-Business Suite (No Credit Card Encryption Patch):** 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. Refer to section 3.13 for more information about compensating controls when PANs are not encrypted. **Oracle E-Business Suite (With Credit Card Encryption Patch):** All PANs, with the exception of Oracle Internet Expenses employee credit card numbers (fixed in Release 12), are encrypted when stored. No additional encryption or protection is required. **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. **iPayment:** iPayment 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.

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	**Oracle E-Business Suite (With Credit Card Encryption Patch):** A policy and procedure needs to be developed to manage the "iPayment System Key". The "iPayment Payment Administrator" responsibility should only be granted to key custodians.
3.5.2 Store keys securely in the fewest possible locations and forms	Low	**Oracle E-Business Suite (With Credit Card Encryption Patch):** The "iPayment System Key" is stored encrypted in the Oracle E-Business Suite database, but must also be stored off-line in a secure location. Loss of the key may result in loss of all PANs, thus the key should be stored in at least two locations.
3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data, including the following:		
3.6.1 Generation of strong keys	Low	**Oracle E-Business Suite (With Credit Card Encryption Patch):** The maximum "iPayment System Key" length of 24 characters should always be used. The key should be randomly generated whenever possible.
3.6.2 Secure key distribution **3.6.3** Secure key storage	Low	**Oracle E-Business Suite (With Credit Card Encryption Patch):** Off-line, secure storage of the "iPayment System Key" is required.
3.6.4 Periodic changing of keys • As deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically • At least annually	Low	**Oracle E-Business Suite (With Credit Card Encryption Patch):** The "iPayment System Key" should be rotated at least annually. The "FND Vault Key", which is system generated, should be rotated at least every 90 days by the DBA or application administrator.
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	**Oracle E-Business Suite (With Credit Card Encryption Patch):** It is possible for multiple people in the same physical location to enter portions of the "iPayment System Key" 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	**Oracle E-Business Suite (With Credit Card Encryption Patch):** The current "iPayment System Key" is required to change the key, therefore, any unauthorized disclosure of the current key could result in unauthorized changes. The "iPayment Payment Administrator" responsibility should only be granted to key custodians.

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. *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.

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 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install relevant security patches within one month of release.	**Very High**	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 for Oracle E-Business Suite include a database patch, one to four application server patches, two to four Oracle Developer 6i patches, and usually six or more Oracle E-Business Suite patches. 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.
6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update standards to address new vulnerability issues.	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.
6.3.4 Production data (live PANs) are not used for testing or development	Medium	Cloning is a standard operation in all Oracle E-Business Suite implementation where the production environment is copied to test, QA, training, and development environments. During the cloning process, all sensitive data including cardholder data should be scrambled or removed. Even though the cardholder data may be encrypted, it still should be scrambled, as it is possible to decrypt the data.
6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability.	Medium	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.
6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods: • Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security • Installing an application layer firewall in front of web-facing applications. *Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.*	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). All steps in Oracle Metalink Note ID "287176.1 Oracle E-Business Suite 11i 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. 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.

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	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.
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	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.

Requirement 8: Assign a unique ID to each person with computer access

PCI DSS Requirement	Difficulty	Oracle E-Business Suite Guidance
8.1 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. **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.
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: • Password • Token devices (e.g., SecureID, certificates, or public key) • 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. **Database:** The standard Oracle Database passwords should be sufficient to meet this requirement. See section 8.5 for additional requirements related to passwords.
8.4 Encrypt all passwords 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 the Integrigy's whitepaper "Oracle E-Business Suite Password Decryption" for more information). **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

		Requirement 2.3.
8.5 Ensure proper user authentication and password management for non-consumer users and administrators on all system components as follows:		
8.5.2 Verify user identity before performing password resets	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. In older versions, the password reset is a manual process. **Database:** Password resets for the database is a manual process.
8.5.3 Set first-time passwords 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. **Database:** User creation for the database is a manual process. All new database accounts must be created with a unique and strong password.
8.5.5 Remove 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. **Database:** Removal of stale database accounts is a manual process and requires the creation of scripts and/or reports to identify such accounts.
8.5.8 Do not use group, shared, or generic accounts and passwords	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. **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.
8.5.9 Change user passwords at least every 90 days	Low	**Application:** All application accounts should be setup with password expiration set to 90 days. **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.
8.5.10 Require a minimum password length of at least seven characters	Low	**Application:** The system profile option "Signon Password Length" should be set to a minimum of "7" at the site level. **Database:** 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.

8.5.11 Use passwords containing both numeric and alphabetic characters	Low	**Applications:** The system profile option "Signon Password Hard to Guess" should be set to "True" at the site level. **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.
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords 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. **Database:** All database profiles should have PASSWORD_REUSE_MAX set to 4.
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts	Low	**Applications:** The system profile option "Signon Password Failure Limit" should be set to a maximum of "6" at the site level. **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 attempts.
8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID	Low	**Applications:** Locked application accounts must be manually unlocked. **Database:** All individual database accounts should have a database profile with PASSWORD_LOCK_TIME set to UNLIMITED to require manual unlocking.
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal	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. **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.
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users	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. **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. **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. **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 is of unsuccessful login attempts is standard functionality. This audit trail can be manipulated by the DBA. **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: **10.3.1** User identification **10.3.2** Type of event **10.3.3** Date and time **10.3.4** Success or failure indication **10.3.5** Origination of event **10.3.6** Identity or name of affected data, system component, or resource	-	See Requirement 10.2 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 (although new data being added should not cause an alert).	High	See Requirement 10.2
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). *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: **11.3.1** Network-layer penetration tests **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. *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. Another key aspect of this requirement is that any generated alerts are reviewed by appropriate personnel. Be sure the necessary procedures and process are in place to review such alerts. 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.

COMPENSATING CONTROLS FOR REQUIREMENT 3.4

Compensating controls are required when the Oracle E-Business Suite Credit Card Encryption patch cannot be implemented for technical or business reasons. This patch requires significant functional and technical upgrades, therefore, all Oracle E-Business Suite implementations may not be able to immediately implement this new functionality. "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 11.5.10 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: ▪ IP address/Mac address ▪ Application/service ▪ User accounts/groups ▪ Data type (packet filtering)	Medium	▪ All responsibilities should be periodically reviewed for appropriate access to cardholder data. ▪ All masking system profile options need to be set for configured modules.
3. Restrict logical access to the database ▪ 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 11.5.10 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. ▪ 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. 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. ▪ 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 ▪ Database files ▪ Log files ▪ 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 to 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

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

1. "Payment Card Industry Data Security Standard 1.1 Release September 2006", PCI Security Standards Council, https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm
2. "Payment Card Industry Data Security Standard Self-Assessment Questionnaire 1.0 Release December 2004", PCI Security Standards Council, https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf
3. "Payment Card Industry Data Security Standard Security Audit Procedures 1.1 September 2006", 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, https://www.pcisecuritystandards.org/tech/glossary.htm
5. "Cardholder Information Security Information Program (CISP) Payment Application Best Practices 1.3", Visa U.S.A., 8 May 2006, http://usa.visa.com/download/business/accepting_visa/ops_risk_management/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

ORACLE E-BUSINESS SUITE SECURITY

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

7. "Oracle E-Business Suite Password Decryption", Stephen Kost and Jack Kanter, Integrigy Corporation, 9 January 2007, http://www.integrigy.com/security-resources/whitepapers/apps-password-weakness/view
8. "Evading Network-Based Oracle Database Intrusion Detection Systems", Stephen Kost and Jack Kanter, Integrigy Corporation, 11 December 2006, http://www.integrigy.com/security-resources/whitepapers/evade-oracle-ids/view
9. "Spoofing Oracle Session Information", Stephen Kost and Jack Kanter, Integrigy Corporation, 12 November 2006, http://www.integrigy.com/security-resources/analysis/oracle-spoofing-session-information/view
10. "Best Practices for Securing the Oracle E-Business Suite", Oracle Metalink Note ID 189367.1, Oracle Corporation, October 2006, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=189367.1
11. "Oracle E-Business Suite 11i Configuration in a DMZ", Oracle Metalink Note ID 287176.1, Oracle Corporation, 27 September 2006, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=287176.1

Oracle E-Business Suite and Credit Cards

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

12. "Oracle Oracle E-Business Suite Credit Card Encryption", Oracle Metalink Note ID 338756.1, Oracle Corporation, 12 December 2006, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=338756.1
13. "Does The Credit Card Encryption Patch 4607647 Impact Internet Expenses?", Oracle Metalink Note ID 390032.1, Oracle Corporation, 22 January 2007, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=390032.1
14. "Where The Credit Card Numbers Are Stored For iStore?", Oracle Metalink Note ID 376708.1, Oracle Corporation, 13 July 2006, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=376708.1
15. "How Is Credit Card Encryption Handled By iPayment 11i?", Oracle Metalink Note ID 312238.1, Oracle Corporation, 19 December 2005, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=312238.1
16. "How to generate Debug Log Files for Oracle iPayment?", Oracle Metalink Note ID 265330.1, Oracle Corporation, 28 November 2006, https://metalink.oracle.com/metalink/plsql/ml2_documents.showDocument?p_database_id=NOT&p_id=265330.1

General Credit Card Information

17. " Anatomy of Credit Card Numbers", Michael Gilleland, http://www.merriampark.com/anatomycc.htm

History

Change History

1.1.0	January 29, 2007	Initial Version ▪ Version number corresponds with PCI DSS 1.1 version
1.1.1	October 10, 2010	▪ Minor updates to include additional logging ▪ 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 ▪ Change all Oracle E-Business Suite references to Oracle E-Business Suite ▪ Update to include Oracle E-Business Suite R12

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. 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