WHITEPAPER | JULY 1, 2016

ORACLE EXADATA DATABASE MACHINE AND COMPLIANCE WITH PCI DSS V3.2

MUKUL GUPTA PH.D., QSA, CISA, CISSP, CAP, GREM, GWEB, GCIA, HITRUST
SENIOR MANAGER
TECHNOLOGY ADVISORY AND ASSESSMENT SERVICES

COALFIRE℠

North America | Latin America | EMEA
877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

INTRODUCTION

Oracle Exadata Database Machine (Exadata) is a platform for Oracle Database that combines storage and compute systems into a single machine. Exadata delivers a high performance database platform that can be implemented in single or multi-tenant environments. Exadata has built-in isolation features that enable it to isolate storage and compute nodes that have to adhere to varying degrees of confidentiality, integrity, and availability requirements.

Organizations that store, process, or transmit payment card data are likely to implement Exadata to meet their storage and processing needs. This may also include storing cardholder data (CHD) inside Oracle Database available with the Exadata platform. These organizations that include merchants, payment processors, issuers, and service providers are required by the payment acquiring banks to comply with Payment Card Industry Data Security Standard (PCI DSS) on an ongoing basis.

Compliance requirements necessitate certain segmentation and security measures that must be deployed in any environment that stores, processes or transmits CHD, or can potentially impact the security of the CHD.

This paper discusses the features of Exadata and Oracle Database that can be either used to address the PCI DSS requirements or can be leveraged to reduce the PCI DSS scope with Exadata.

The rest of the paper briefly describes the PCI DSS framework, presents the features of Exadata and Oracle Database that can be leveraged for PCI DSS compliance, and provides a mapping of available features in Exadata to specific requirements in PCI DSS framework.

PAYMENT CARD INDUSTRY DIGITAL SECURITY STANDARD (PCI DSS)

Payment Card Industry Digital Security Standard (PCI DSS) is a framework that defines baseline technical, physical, and operational security controls necessary for protecting payment card account data. PCI DSS defines two categories of payment account data: Cardholder Data (CHD) that includes Primary Account Number (PAN), Cardholder Name, Expiration Data, and Service Code; and Sensitive Authentication Data (SAD) that includes full track data (magnetic-stripe data or equivalent on a chip), Card Security Code (CAV2/CVC2/CVV2/CID), and PINs/PIN blocks.

PCI DSS applies to any organization that stores, processes, or transmits CHD. These organizations include (but are not limited to): merchants, payment processors, issuers, acquirers, and service providers. The PCI DSS security requirements apply to all system components included in or connected to the cardholder data environment. The cardholder data environment (CDE) is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. PCI DSS defines 12 requirements designed to address six objectives:

BUILD AND MAINTAIN SECURE NETWORK AND SYSTEMS

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

This requirement is focused on ensuring that the firewall used to segment the untrusted networks from an entity's internal networks, and sensitive areas (including the CDE) within the entity's trusted networks, are securely configured, administered, and continuously managed to ensure that sensitive areas are not directly accessible from untrusted networks. Firewall configurations must ensure that only traffic with necessary business need is allowed into and out of the sensitive areas.

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

This requirement is focused on ensuring that system configuration standards are developed based on industry best practices and proper system hardening is performed before systems and devices are deployed in a cardholder data environment. The requirement also calls for maintaining an up-to-date inventory of all systems and devices used in or connected to the CDE.

PROTECT CARDHOLDER DATA

Requirement 3: Protect stored cardholder data

This requirement is focused on ensuring that any stored PAN is protected using strong encryption techniques and proper key management techniques are being followed to ensure the integrity of the employed encryption technique. Additionally, the requirement also calls for ensuring that PAN is not retained beyond the required business need and is discarded using secure data disposal techniques.

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

This requirement is focused on ensuring that any PAN transmitted over open public networks is transmitted over secure transmission protocols using strong encryption technologies. The requirement also restricts the transmission of PAN over unsecure end-user messaging technologies.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

This requirement is focused on ensuring that all systems commonly affected by malware are protected via an anti-virus software. The requirement further specifies that anti-virus software should be kept up-to-date to protect systems against current and evolving malicious software threats.

Requirement 6: Develop and maintain secure systems and applications

This requirement is focused on ensuring that patches to all vendor-provided systems are applied in a timely manner to protect these systems against exploitation. The requirement also specifies that all in-house applications should be developed following software development life cycles that incorporate secure coding practices. Additionally, all system and application changes should be controlled via a documented change management process.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement 7: Restrict access to cardholder data by business need to know

This requirement is focused on ensuring that access to the cardholder data environment is limited to only authorized personnel with privileges necessary for business need to know.

Requirement 8: Identify and authenticate access to system components

This requirement is focused on ensuring that identification and authentication technologies and processes are in place to control access to the cardholder data environment.

Requirement 9: Restrict physical access to cardholder data

This requirement is focused on ensuring that physical access controls measures are in place to control authorized employee and visitor access to the cardholder data environment. The requirement also specifies measures to protect all electronic and paper media containing cardholder data.

REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and cardholder data

This requirement is focused on ensuring that proper logging mechanism are implemented for all systems, devices, and applications in the cardholder data environment allowing for tracking, alerting, and analysis of any unauthorized activity or compromise. The requirement further specifies that logs are retained for at least a year and integrity of the logs and the logging mechanism is maintained at all times.

Requirement 11: Regularly test security systems and processes

This requirement is focused on ensuring that the cardholder data environment is scanned and tested on a regular basis to ensure that vulnerabilities within the environments are identified, and effectiveness of the implemented security controls can be validated.

MAINTAIN AN INFORMATION SECURITY POLICY

Requirement 12: Maintain a policy that addresses information security for all personnel

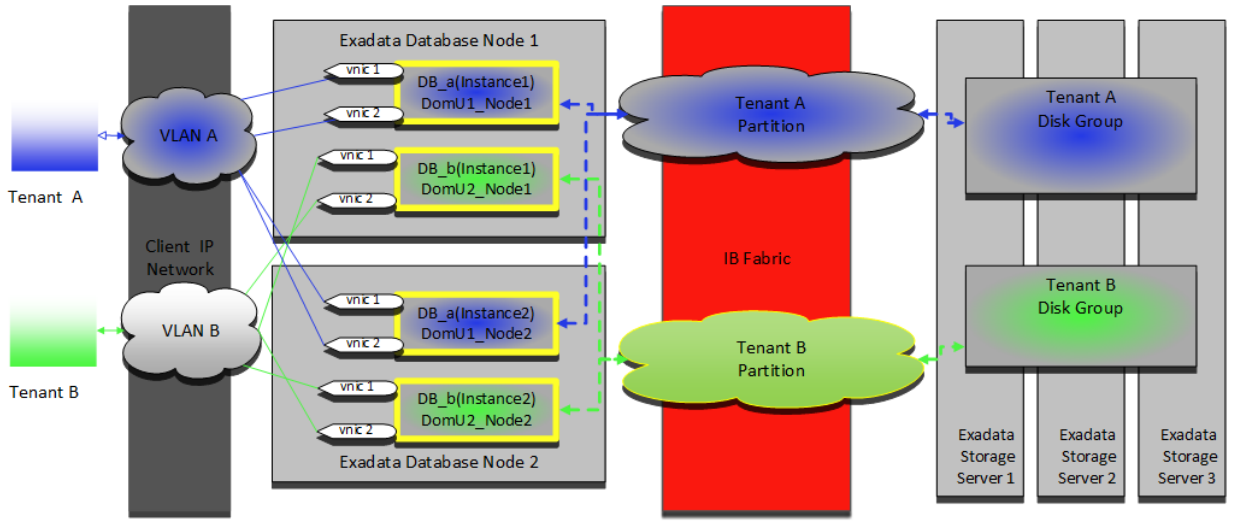
This requirement is focused on ensuring that information security and acceptable use policies are developed, reviewed, and communicated to all personnel to establish the roadmap for securing the cardholder data environment. The requirement further specifies that risk assessment methodology be developed and risk assessment for the cardholder data environment be performed at least annually. Additionally, proper vendor assessment and management processes must be in place if an organization opts to use service providers to manage any components or services within the cardholder environment.

EXADATA

Exadata is a platform architected for scalability and high availability for running an Oracle Database. Exadata includes all the hardware needed to run Oracle Database. The platform includes database servers, storage servers, and InfiniBand internal network fabric to connect database servers and storage servers. As the platform scales to support the organizational needs, additional database nodes, storage nodes, and networking modules can be added in a balanced fashion to ensure seamless scalability without any bottlenecks. In addition to the scalability within a single Exadata, multiple racks can be connected using the integrated InfiniBand networks to form larger configurations.

Exadata architecture lends itself for hosting multiple databases with different compliance requirements and the architecture supports multi-tenant environments. Oracle Database Servers and Storage Servers within Exadata can be implemented on separate physical disks or can use Oracle Virtual Machine (OVM) architecture.

Despite the support for multiple or multi-tenant environments, Exadata provides segmentation and access control mechanisms suitable for environments requiring compliance with PCI DSS. The specific database and storage nodes needing to comply with PCI DSS can be effectively segmented from the rest of the environments without potentially increasing the scope of the implementation. The segmentation features available within Exadata are described in Figure 1 below.



ASM Scoped Security - Isolate Cell / Grid Disk to Tenant
DB Scoped Security - Isolate Grid disk to DB Instances
IB Partition - Tenant DB Isolation
IPSec - Limit IPoIB traffic over IB between nodes (RDS still open)
IPFilter - Secure Network access per node
VLAN's - Used to secure network traffic per tenant

Figure 1: Exadata Tenant Isolation Overview

AUTOMATIC STORAGE MANAGEMENT (ASM) SCOPED SECURITY AND DATABASE SCOPED SECURITY

Oracle Exadata Storage Server data security defines the access mechanism for controlling access from Oracle ASM clusters and database clients to specific grid disks on storage servers. First layer of access segmentation is implemented using ASM scoped security where all database clients in a specific ASM cluster have access to only specific grid disks. All Oracle Real Application Clusters (Oracle RAC) servers

in an Oracle ASM cluster have the same content, ownership, and security for the Oracle ASM cellkey.ora file.

Second layer of access can be implemented using Database scoped security where specific database clients in a specific ASM cluster are limited to accessing only specific grid disks. Once Database scoped security is set among the database clients and the grid disks, only specific grid disks are available to the specified database clients. When using database-scoped security, there is one key file per database per host, and one access control list (ACL) entry per database on each cell.

INFINIBAND PARTITIONING ACROSS APPLICATION CLUSTERS ON EXADATA

Connections and networking within an Exadata architecture use InfiniBand. InfiniBand partitioning is used to ensure that the network traffic from one RAC cluster is not accessible to another RAC cluster. An InfiniBand partition defines a group of InfiniBand nodes that are allowed to communicate with one another. Partitions are identified by unique partition keys and are managed by the master subnet manager. Members within a partition are allowed to only communicate among themselves and are prevented from communicating to a member of a different partition. Oracle RAC nodes on a particular cluster are assigned a dedicated partition for clusterware communication and a separate dedicated partition for storage cell communication. RAC nodes from one cluster are thereby prevented from accessing storage cell nodes from a different cluster.

TAGGED VLAN INTERFACES IN ORACLE VIRTUAL MACHINES (OVM) ON EXADATA

Oracle databases running in OVM guests on Exadata platform are accessed through the entity's[1] Ethernet network. If network isolation across user domains is required, 802.1Q based VLAN tagging can be used to provide OVM isolation. Exadata architecture supports VLAN tagging of the interfaces, creation of corresponding bridge interfaces, and mapping the user domains to appropriate network interfaces.

Exadata has additional intrinsic features, configuration options, or installable solutions available to address or support additional PCI DSS requirements. These characteristics are identified in the next section that provides a mapping of available features in Exadata/Oracle to specific requirements in PCI DSS framework.

[1] The term "Entity" in the paper refers to the organization that is implementing Exadata and is attempting to achieve the PCI DSS compliance.

EXADATA SUPPORT FOR SPECIFIC PCI DSS 3.2 REQUIREMENTS

PCI DSS 3.2 requirements define baseline technical, physical, and operational security controls necessary for protecting payment card account data and Exadata is a technology platform that can be used to store, process or transmit card holder data. Some of the PCI DSS 3.2 requirements are policy/process requirements that are entirely the entity's responsibility while others apply to technology platform that is used to store, process or transmit CHD. This section provides a mapping of available features in Exadata to specific requirements in PCI DSS framework.

Below is a brief description of categories used to identify the coverage status of specific PCI DSS v3.2 requirements by Exadata.

- Supported – The requirement is supported on Exadata by configuring settings available within the application, platform, and/or the supporting operating systems
- Provided – The capability is provided by Exadata
- Entity Responsibility – The requirement is a documentation, process, or architectural design responsibility of the entity
- Not Applicable – The requirement is not supported or provided by Exadata

REQUIREMENT 1: INSTALL AND MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

Although, restriction of traffic between the untrusted networks and internal networks is best supported by network firewalls, Exadata has a few built-in features that can be configured to restrict the traffic from untrusted networks from accessing the database and storage servers within Exadata. Exadata database and storage nodes come with iptables that can be configured to restrict traffic from the Internet. Additionally, routing configurations on the database nodes can be modified to control access to the storage nodes. Exadata InfiniBand network also inherently provides the segmentation between the CDE and any other segments implemented within Exadata.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
1.1 Establish and implement firewall and router configuration standards that include the following:	Entity Responsibility	Development of configuration standards, approval and testing of configurations, and maintenance of the network diagrams and data flows are process and documentation requirements are exclusively the responsibility of the entity.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations		
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks		
1.1.3 Current diagram that shows all cardholder data flows across systems and networks		
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Supported	Exadata has segmentation capabilities built into the platform. Exadata database and storage nodes come with iptables that can be configured to restrict traffic from the Internet. Additionally, routing configurations on the database nodes can

	Entity Responsibility	be modified to control access to the storage nodes. It is recommended that Exadata should be implemented on the internal network zone. Segmentation between the Internet and DMZ, and DMZ and the internal networks should be controlled via network firewalls. Implementation and maintainance of the network firewalls are exclusively the responsibility of the entity.
1.1.5 Description of groups, roles, and responsibilities for management of network components	Entity Responsibility	Assignment of roles and responsibilities, documentation of business justification, and review of firewall rules are process and documentation requirements that are exclusively the responsibility of the entity.
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.		
1.1.7 Requirement to review firewall and router rule sets at least every six months		
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	Supported	Exadata has segmentation capabilities built into the platform. Exadata database and storage nodes come with iptables that can be configured to restrict traffic from the Internet. Additionally, routing configurations on the storage cells can be modified to control access to the storage nodes.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Entity Responsibility	It is recommended that Exadata should be implemented on the internal network zone. Segmentation between the Internet and DMZ, and DMZ and the internal networks should be controlled via network firewalls. Implementation and maintainance of the network firewalls are exclusively the responsibility of the entity.
1.2.2 Secure and synchronize router configuration files.	Entity Responsibility	Synchronization of router configurations, perimeter firewalls, implementation of DMZ and restricting inbound Internet access are controls that are exclusively the responsibility of the entity.
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.		
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.		
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.		

1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.		
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	Supported	Exadata has segmentation capabilities built into the platform. Exadata database and storage nodes come with iptables that can be configured to restrict traffic from the Internet. Additionally, routing configurations on the storage cells can be modified to control access to the storage nodes. iptables can be configured to provide stateful inspection and provide anti-spoofing protection.
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	Entity Responsibility	It is recommended that Exadata should be implemented on the internal network zone. Restriction of direct inbound and outbound connections for traffic between the Internet and the CDE, implementation of anti-spoofing measures, and permitting only "established" connections should be managed via network firewalls. Implementation and maintainance of the network firewalls are exclusively the responsibility of the entity.
1.3.5 Permit only "established" connections into the network.		
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Provided	Exadata has segmentation capabilities built into the platform. Exadata database and storage nodes come with iptables that can be configured to restrict traffic from the Internet. Exadata InfiniBand network inherently provide the segmentation between the CDE and any other segments implemented within Exadata.
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. ***Note:*** *Methods to obscure IP addressing may include, but are not limited to:* • *Network Address Translation (NAT)* • *Placing servers containing cardholder data behind proxy servers/firewalls,* • *Removal or filtering of route advertisements for private networks that employ registered addressing,* • *Internal use of RFC1918 address space instead of registered addresses.*	Entity Responsibility	Preventing disclosure of private IP addresses, implementation of personal firewalls on mobile/employee owned devices, and documenting and communicating appropriate security policies are process controls that are exclusively the responsibility of the entity.
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: • Specific configuration settings are defined. • Personal firewall (or equivalent functionality) is actively running.		

• Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.		
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.		

REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

Exadata platform has built-in utilities that enable the entity to change or disable the default accounts and/or modify the default passwords configured within the platform. Since Exadata is designed to support the database function, only services and protocols needed to support the function are enabled by default. Exadata only used secure services to reduce the attack footprint on the platform. All remote access is managed via SSH. Additionally, root access and any direct access to the storage nodes can be completely disabled and access to storage servers can be exclusively controlled by ExaCLI.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts **before** installing a system on the network. 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, payment applications, Simple Network Management Protocol (SNMP) community strings, etc.).	Supported	Oracle provides a listing of all default accounts and passwords for all components within Exadata that include database nodes, storage nodes, KVM, and switches. Oracle provides commands and utilities to change the default passwords for all Oracle configured accounts within Exadata. Oracle also provides commands and utilities to change the SNMP community strings on components that rely on SNMP. Utilities included within Exadata and configuration options available during installation can be used to ensure that all components are hardened and configured as per the entity's configuration standards.
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	Entity Responsibility	Configuration of wireless environments and developing configuration standards for implemented system components are exclusively the responsibility of the entity.
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. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO)		

• SysAdmin Audit Network Security (SANS) Institute • National Institute of Standards Technology (NIST).		
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) ***Note:*** *Where virtualization technologies are in use, implement only one primary function per virtual system component.*	Provided	Exadata is designed to serve only one primary function that is providing database servers and utilities. During the installation process, components of Exadata are configured to support the primary function and only services and protocols needed to support the function are enabled by default.
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.		
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	Supported	Exadata by default only leverages secure services and reduces the attack surface. InfiniBand partitions ensure that segmentation is maintained at all times. Root access to storage nodes can be disabled. All remote access to components is provided using SSH by default. Additionally, though the use of TLS1.0 and SSLv3 on compute and storage nodes is available, the settings can be configured to disable the use of these protocols.
2.2.4 Configure system security parameters to prevent misuse.	Provided	Exadata is designed to serve only one primary function that is providing database servers and utilities. During installation process, components of Exadata are configured to support the primary function and only services and protocols needed to support the function are enabled by default. Exadata by default only leverages secure services and reduces the attack surface. InfiniBand partitions ensure that segmentation is maintained at all times. Root access is to storage nodes can be disabled. All remote access to components is provided using SSH by default.
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.		
2.3 Encrypt all non-console administrative access using strong cryptography. ***Note:*** *Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	Provided	All passwords are stored in non-reversible format using SHA-512 cryptographic hashes. All authentication to database or storage nodes is performed over SSH sessions. Supported encryption algorithms for the SSH include 128-bit RC4, 128-bit AES, 192-bit AES, and 256-bit AES. Oracle database traffic can be encrypted using Oracle Net Manager and can be configured to support 128-bit RC4, 168-bit 3DES, 128-bit AES, 192-bit AES, and 256-bit AES.
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	Entity Responsibility	Maintaining inventory of system components, developing and communicating the security policies are process controls that are exclusively the responsibility of the entity.
2.5 Ensure that security policies and operational procedures for managing vendor defaults and		

other security parameters are documented, in use, and known to all affected parties.		
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers.*	Supported	Exadata has built-in InfiniBand segmentation and VLAN segmentation to provide isolation needed to often comply with hosting provider requirements detailed in Appendix A.

REQUIREMENT 3: PROTECT STORED CARDHOLDER DATA

Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) included as part of the Exadata platform. TDE supports both encryption of columns with sensitive data and encryption of tablespace with sensitive data. Encryption algorithms and key lengths within the TDE can be configured to one of the following combinations: 168-bit 3DES, 128-bit AES, 192-bit AES, or 256-bit AES. Exadata can also utilize the services provided by Oracle Wallet for key management, storage, and rotation.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
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: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and/or business requirements • Specific retention requirements for cardholder data • Processes for secure deletion of data when no longer needed • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Provided Entity Responsibility	Exadata has inbuilt capabilities to securely delete storage cells as per DOD recommendations. Exadata provides `DROP CELL` command with `ERASE` option. `ERASE` option supports up to 7 passes to overwrite disk with set data patterns. Determining the retention period for each data element being stored in Exadata is the exclusive responsibility of the entity.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* • *There is a business justification and* • *The data is stored securely.* Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	Entity Responsibility	Ensuring that the entity does not store sensitive authentication data is exclusively the responsibility of the entity.
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or		

elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. ***Note:*** *In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* • *The cardholder's name* • *Primary account number (PAN)* • *Expiration date* • *Service code* *To minimize risk, store only these data elements as needed for business.*		
3.2.2 Do not store the card verification 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) after authorization.	Provided	For issuers and companies that support the issuing service, who have documented business requirements for storing Sensitive Authentication Data (SAD), Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) available as part of the Exadata platform. TDE supports both encryption of columns with sensitive data and encryption of tablespace with sensitive data. By default, column encryption uses 192-bit AES encryption, and tablespace encryption uses 128-bit AES encryption. Oracle SQL ENCRYPT clause can be used to change the encryption algorithm to any of the supported key lengths and algorithms (168-bit 3DES, 128-bit AES, 192-bit AES, or 256-bit AES).
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.		
3.3 Mask PAN when displayed (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 more than the first six/last four digits of the PAN. ***Note:*** *This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	Provided	Oracle Database provides capability to create Views. Views can be configured to restrict the display of PAN to only the first six and last four digits for personnel with no legitimate business need to see the full PAN.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures. ***Note:*** *It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they*	Provided	Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) available as part of the Exadata platform. TDE supports both encryption of columns with sensitive data and encryption of tablespace with sensitive data. By default, column encryption uses 192-bit AES encryption, and tablespace encryption uses 128-bit AES encryption. Oracle SQL ENCRYPT clause can be used to change the encryption algorithm to any of the supported key lengths and algorithms (168-bit 3DES, 128-bit AES, 192-bit AES, or 256-bit AES).

have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.		
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. ***Note:*** *This requirement applies in addition to all other PCI DSS encryption and key-management requirements.*	Not Applicable	Exadata does not support full-disk encryption. However, Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) available as part of the Exadata platform. TDE supports both encryption of columns with sensitive data and encryption of tablespaces with sensitive data.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: ***Note:*** *This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*	Provided	Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) available as part of the Exadata platform. TDE uses a two tier key mechanism. When TDE column encryption is applied to an existing application table column, a new table key is created and stored in the Oracle Database data dictionary. When TDE tablespace encryption is used, the individual tablespace keys are stored in the header of the underlying OS file(s). The table and tablespace keys are encrypted using the TDE master encryption key. The master encryption key is generated when TDE is initialized and stored outside the database in the Oracle Wallet. Oracle Wallet is an encrypted container that is used to store authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by SSL. "Encryption Wallet" is recommended for storing TDE master key. Encryption Wallet needs to be opened manually after database startup and prior to TDE encrypted data being accessed. Access to the wallet is limited to appropriate user groups and can be controlled via proper directory and file permissions. Even though the 'root' user has access to the wallet file, the 'root' user does not have access to the master encryption key.
3.5.1 ***Additional requirement for service providers only:*** Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date	Entity Responsibility	Documentation of the cryptographic architecture is the exclusive responsibility of the entity.

• Description of the key usage for each key • Inventory of any HSMs and other SCDs used for key management ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*		
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	Provided	Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) available as part of the Exadata platform. TDE uses a two tier key mechanism. When TDE column encryption is applied to an existing application table column, a new table key is created and stored in the Oracle Database data dictionary. When TDE tablespace encryption is used, the individual tablespace keys are stored in the header of the underlying OS file(s). The table and tablespace keys are encrypted using the TDE master encryption key. The master encryption key is generated when TDE is initialized and stored outside the database in the Oracle Wallet. Oracle Wallet is an encrypted container that is used to store authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by SSL. "Encryption Wallet" is recommended for storing TDE master key. Encryption Wallet needs to be opened manually after database startup and prior to TDE encrypted data being accessed. Access to the wallet is limited to appropriate user groups and can be controlled via proper directory and file permissions. Even though the 'root' user has access to the wallet file, the 'root' user does not have access to the master encryption key.
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: • 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 • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As at least two full-length key components or key shares, in accordance with an industry-accepted method ***Note:*** *It is not required that public keys be stored in one of these forms.*		
3.5.4 Store cryptographic keys in the fewest possible locations.		
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: ***Note:*** *Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	Provided	Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) available as part of the Exadata platform. TDE supports both encryption of columns with sensitive data and encryption of tablespace with sensitive data. By default, column encryption uses 192-bit AES encryption, and tablespace encryption uses 128-bit AES encryption. Oracle SQL `ENCRYPT` clause can be used to change the encryption algorithm to any of the supported key lengths and algorithms (168-bit 3DES, 128-bit AES, 192-bit AES, or 256-bit AES). TDE uses a two tier key mechanism. When TDE column encryption is applied to an existing application table column, a new table key is created and stored in the Oracle data dictionary. When TDE tablespace encryption is used, the individual tablespace keys are stored in the header of the underlying OS file(s). The table and tablespace keys are encrypted using the TDE
3.6.1 Generation of strong cryptographic keys		
3.6.2 Secure cryptographic key distribution		
3.6.3 Secure cryptographic key storage		
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices		

and guidelines (for example, NIST Special Publication 800-57). **3.6.5** Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. ***Note:*** *If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*		master encryption key. The master encryption key is generated when TDE is initialized and stored outside the database in the Oracle Wallet. Both the master key and table keys can be independently changed (rotated, re-keyed) based on the entity's security policies. Tablespace keys cannot be re-keyed (rotated). A possible workaround is to move the data into a new encrypted tablespace.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. ***Note:*** *Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	Entity Responsibility	Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) available as part of the Exadata platform. If the entity choses to use manual clear-text cryptographic key-management, implementation of split knowledge and dual control are exclusively the responsibility of the entity.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	Provided	Exadata can leverage the encryption capabilities provided by Transparent Data Encryption (TDE) available as part of the Exadata platform. TDE uses a two-tier key mechanism. When TDE column encryption is applied to an existing application table column, a new table key is created and stored in the Oracle data dictionary. When TDE tablespace encryption is used, the individual tablespace keys are stored in the header of the underlying OS file(s). The table and tablespace keys are encrypted using the TDE master encryption key. The master encryption key is generated when TDE is initialized and stored outside the database in the Oracle Wallet. Oracle Wallet is an encrypted container that is used to store authentication and signing credentials, including passwords, the TDE master key, PKI private keys, certificates, and trusted certificates needed by SSL. "Encryption Wallet" is recommended for storing TDE master key. Encryption Wallet needs to be opened manually after database startup and prior to TDE encrypted data being accessed. Access to the wallet is limited to appropriate user groups and can be controlled via proper directory and file permissions. Even though the 'root' user has access to the wallet file, the 'root' user does not have access to the master encryption key.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they		Ensuring that key custodians formally acknowledge their responsibilities and

understand and accept their key-custodian responsibilities.	Entity Responsibility	documenting and communicating appropriate security policies are process controls that are exclusively the responsibility of the entity.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.		

REQUIREMENT 4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS

Exadata by design does not transmit any data over the open public networks. All communication within the operating system, storage, and database components of the Exadata product are process controls that are exclusively handled via InfiniBand networks. Management and protection of transmission over public networks, managing wireless networks, restricting communication of PAN over end-user messaging technologies, and documenting and communicating appropriate security policies are exclusively the responsibility of the entity.

REQUIREMENT 5: PROTECT ALL SYSTEMS AGAINST MALWARE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

Exadata does not intrinsically provide anti-virus software. However, since Exadata server and storage nodes run on Oracle Linux platform, any anti-virus software compatible with Oracle Linux can be installed on Exadata database nodes. Selecting and maintaining the anti-virus software, and documenting and communicating appropriate security policies are exclusively the responsibility of the entity.

REQUIREMENT 6: DEVELOP AND MAINTAIN SECURE SYSTEMS AND APPLICATIONS

Oracle tracks the vulnerabilities in the Exadata platforms, and creates, maintains, and issues appropriate patches to address the vulnerabilities. The entity can access all the vulnerabilities and patching details at https://support.oracle.com. Application development, change management, and implementation of secure coding practices that are process controls that have to be implemented by the entity.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as “high,” “medium,” or “low”) to newly discovered security vulnerabilities. ***Note:*** *Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected.*	Supported	Oracle tracks the vulnerabilities in the Exadata platforms, and creates, maintains, and issues appropriate patches to address the vulnerabilities. The entity can access all the vulnerabilities and patching details at https://support.oracle.com. Risk ranking the vulnerabilities and applying the available patches is the responsibility of the entity. Oracle provides an optional Platinum Service for patch management for Exadata platform. As part of the Platinum Service,

Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.		Oracle controls and manages the patching of subscribing entity's Exadata platform.
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. ***Note:*** *Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	Entity Responsibility	Establishing processes to identify vulnerabilities, assign risk ratings, and install vendor-supplied security patches are exclusively the responsibility of the entity.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: • In accordance with PCI DSS (for example, secure authentication and logging) • Based on industry standards and/or best practices. • Incorporating information security throughout the software-development life cycle *Note: this applies to all software developed internally as well as bespoke or custom software developed by a third party.*	Entity Responsibility	Application development, change management, implementation of secure coding practices, and web application testing are process controls that are exclusively the responsibility of the entity.

6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:
• Separate development/test environments from production environments, and enforce the separation with access controls.
• Separation of duties between development/test and production environments
• Production data (live PANs) are not used for testing or development
• Removal of test data and accounts from system components before the system becomes active / goes into production
• Change control procedures must include the following:
  • Documentation of impact.
  • Documented change approval by authorized parties.		

• Functionality testing to verify that the change does not adversely impact the security of the system. • Back-out procedures. • Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. *(**Note:** This requirement is a best practice until January 31, 2018, after which it becomes a requirement.)*		
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines. ***Note:** The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.*		
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: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ***Note:** This assessment is not the same as the vulnerability scans performed for Requirement 11.2.* • 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.		
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.		

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

Exadata has Role Based Access Control (RBAC) capabilities to manage access to the database nodes, storage nodes, and database applications. Exadata "Host Access Control" utility provides configurable options to fine-tune the access to the database nodes. "ExaCLI" utility available on the database OS provides granular access management to the storage nodes.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	Provided	Exadata has Role Based Access Control (RBAC) capabilities to manage access to the database nodes, storage nodes, and database applications. Exadata provides configurable options to fine-tune the access to the database nodes. The exacli utility available on the database server OS provides granular access management to the storage nodes. Users are required to have accounts configured on the database application to be able access the database content. "Security Domains" assigned to each user account define the specific privileges assigned to each user within the database application. Users cannot access the database nodes, storage nodes, or database applications unless they have user accounts and access explicitly configured on each of the resources.
7.1.1 Define access needs for each role, including: • System components and data resources that each role needs to access for their job function • Level of privilege required (for example, user, administrator, etc.) for accessing resources.		
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.		
7.1.3 Assign access based on individual personnel's job classification and function.		
7.1.4 Require documented approval by authorized parties specifying required privileges.	Entity Responsibility	Documented approval for access to the cardholder data environment including Exadata are process controls that are exclusively the responsibility of the entity.
7.2 Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system(s) must include the following:	Provided	Exadata has Role Based Access Control (RBAC) capabilities to manage access to the database nodes, storage nodes, and database applications. Exadata provides configurable options to fine-tune the access to the database nodes. The exacli utility available on the database server OS provides granular access management to the storage nodes. Users are required to have accounts configured on the database application to be able access the database content. "Security Domains" assigned to each user account define the specific privileges assigned to each user within the database application. Users cannot access the database nodes, storage nodes, or database applications unless they have user accounts and access explicitly configured on each of the resources.
7.2.1 Coverage of all system components		
7.2.2 Assignment of privileges to individuals based on job classification and function.		
7.2.3 Default "deny-all" setting.		
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Entity Responsibility	Documenting and communicating appropriate security policies are exclusively the responsibility of the entity.

REQUIREMENT 8: IDENTIFY AND AUTHENTICATE ACCESS TO SYSTEM COMPONENTS

Exadata has Role Based Access Control (RBAC) capabilities to manage access to the database nodes, storage nodes, and database applications. Exadata host_access_control utility provides configurable options to fine-tune the access to the database nodes. The exacli utility available on the database OS provides granular access management to the storage nodes.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
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:	Provided	Exadata has Role Based Access Control (RBAC) capabilities to manage access to the database nodes, storage nodes, and database applications. Exadata provides configurable options to fine-tune the access to the database nodes. The exacli utility available on the database server OS provides granular access management to the storage nodes. Users are required to have accounts configured on the database application to be able access the database content. "Security Domains" assigned to each user account define the specific privileges assigned to each user within the database application. Access control for each of the Exadata elements including access to the InfiniBand switches can be configured to support the required account lockout and session timeout settings. Additionally, access control mechanism can also be configured to work with centralized authentication mechanism and/or directory services like Active Directory and/or LDAP.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.		
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.		
8.1.3 Immediately revoke access for any terminated users.		
8.1.4 Remove/disable inactive user accounts within 90 days.		
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.		
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.		
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.		
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.		
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: • Something you know, such as a password or passphrase • Something you have, such as a token device or smart card • Something you are, such as a biometric.	Provided	Exadata has Role Based Access Control (RBAC) capabilities to manage access to the database nodes, storage nodes, and database applications. Access controls systems for each component support password based authentication. Additionally, access control mechanism can also be configured to work with centralized authentication mechanism that can potentially utilize other authentication mechanism that utilize "something you have" or "something you are" factors.

8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Provided	Exadata has Role Based Access Control (RBAC) capabilities to manage access to the database nodes, storage nodes, and database applications. Access controls systems for each component support password based authentication. All passwords are stored in non-reversible format using SHA-512 cryptographic hashes. All authentication to database or storage nodes is performed over SSH sessions. Supported encryption algorithms for the SSH include 128-bit RC4, 128-bit AES, 192-bit AES, and 256-bit AES. Oracle database traffic can be encrypted using Oracle Net Manager and can be configured to support 128-bit RC4, 168-bit 3DES, 128-bit AES, 192-bit AES, and 256-bit AES.
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	Entity Responsibility	Implementing password reset procedures is exclusively the responsibility of the entity.
8.2.3 Passwords/passphrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/ passphrases must have complexity and strength at least equivalent to the parameters specified above.	Provided	Exadata has Role Based Access Control (RBAC) capabilities to manage access to the database nodes, storage nodes, and database applications. Exadata host_access_control utility provides configurable options to fine-tune the access to the database nodes. The exacli utility available on the database OS provides granular access management to the storage nodes. Users are required to have accounts configured on the database application to be able access the database content. "Security Domains" assigned to each user account define the specific privileges assigned to each user within the database application. Access control for each of the Exadata elements including access to the InfiniBand switches can be configured to support the required password configurations. Additionally, access control mechanism can also be configured to work with centralized authentication mechanism and/or directory services like Active Directory and/or LDAP.
8.2.4 Change user passwords/passphrases at least once every 90 days.		
8.2.5 Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.		
8.2.6 Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.		
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication. ***Note:*** *Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.*	Supported	Exadata does not inherently support two-factor authentication. However, access control mechanism available in Exadata can be configured to work with other centralized authentication mechanism that provide two-factor authentication capabilities.

8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*		
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.		
8.4 Document and communicate authentication policies and procedures to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	Entity Responsibility	Documenting and communicating authentication policies and procedures is exclusively the responsibility of the entity.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	Supported	Oracle provides a listing of all default accounts and passwords for different components within Exadata that include database nodes, storage nodes, KVM, and switches. Oracle provides commands and utilities to change the default passwords for all Oracle configured accounts within Exadata. Additionally, use of generic user accounts can be restricted. Exadata provides exacli to manage all storage nodes that restricts all direct access and use of generic or shared accounts.
8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. ***Note:*** *This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.*	Entity Responsibility	The implementation of access control processes to the customer environment and ensuring authentication mechanism is associated with individuals are exclusively the entity's responsibility.
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts		

• Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.		
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	Provided	Exadata provides fine grained controls for managing the user access to the databases. User access can be restricted to programmatic methods by revoking `CONNECT THROUGH` to prevent direct connects to the database. Additionally, audit policies can be created to log all user actions performed on the databases.
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	Entity Responsibility	Documentation and communication of security policies are process controls that are exclusively the responsibility of the entity.

REQUIREMENT 9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA

Exadata does not have any inbuilt physical security controls. Implementation of all physical security and media controls are exclusively the responsibility of the entity. However, by design Exadata makes implementing physical security more convenient as all components of the architecture are encased within a single physical machine.

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

Exadata has auditing capabilities available for all components. Auditd is installed on all components and audit rules can be configured to record audit trails for all system components and control the collected features. Additionally, syslog.conf can be configured to direct the logs to a centralized syslog servers.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
10.1 Implement audit trails to link all access to system components to each individual user.	Provided	Exadata has auditing capabilities available for all components. Auditd is installed on all components and audit rules can be configured to record audit trails for all system components and control the collected features. Additionally, syslog.conf can be configured to direct the logs to a centralized syslog server. Oracle Database also provides an equivalent fine-grained and conditional auditing capability to ensure critical users and activities are audited.
10.2 Implement automated audit trails for all system components to reconstruct the following events:		
10.2.1 All individual user accesses to cardholder data		
10.2.2 All actions taken by any individual with root or administrative privileges		

10.2.3 Access to all audit trails		
10.2.4 Invalid logical access attempts		
10.2.5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges		
10.2.6 Initialization, stopping, or pausing of the audit logs		
10.2.7 Creation and deletion of system-level objects		
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.		
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. ***Note:*** *One example of time synchronization technology is Network Time Protocol (NTP).*	Supported	Exadata has a custom utility called `ipconf` to configure NTP settings to receive time data from industry accepted sources. NTP configurations are by default only available to administrators and cannot be modified by an unauthorized user.
10.4.1 Critical systems have the correct and consistent time.		
10.4.2 Time data is protected.		
10.4.3 Time settings are received from industry-accepted time sources.		
10.5 Secure audit trails so they cannot be altered.	Supported	Exadata has Role Based Access Control (RBAC) capabilities that can be configured to restrict access to and prevent unauthorized modifications of the audit trails. Additionally, `syslog.conf` can be configured to direct the logs to a centralized syslog server.
10.5.1 Limit viewing of audit trails to those with a job-related need.		
10.5.2 Protect audit trail files from unauthorized modifications.		
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.		
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.		

10.5.5 Use file-integrity monitoring or 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).	Entity Responsibility	Exadata has Oracle Linux installed on them. Entity has an option to install any change detection mechanism that is available for Oracle Linux. The change detection mechanism can be configured to protect the audit trails.
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. ***Note:*** *Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*	Entity Responsibility	Review of logs and security events are process controls that are exclusively the responsibility of the entity.
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).		
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.		
10.6.3 Follow up exceptions and anomalies identified during the review process.		
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Supported	Log rotate parameters for Auditd can be configured to retain logs for requisite periods. Additionally, `syslog.conf` can be configured to direct the logs to a centralized syslog servers.
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	Entity Responsibility	Implementation of processes for detecting, reporting and responding to failure of security controls, and development and communication of security policies are exclusively the responsibility of the entity.

10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls **Note:** This requirement is a best practice until January 31, 2018, after which it becomes a requirement.		
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.		

REQUIREMENT 11: REGULARLY TEST SECURITY SYSTEMS AND PROCESSES

Oracle provides details on vulnerabilities to the Exadata platform and provides patching support for vulnerabilities. Oracle also maintains documentation on common vulnerabilities identified on Exadata by vulnerability scanning tools. Execution of actual vulnerability scans and penetrations tests are the entity's responsibilities. Additionally, although Exadata does not intrinsically provide intrusion detection systems and change detection mechanism, any host based intrusion detection system and change detection mechanism that support Oracle Linux can be installed on the database nodes.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. ***Note:*** *Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.*	Entity Responsibiilty	Ensuring unauthorized wireless access points are not present in the cardholder data environment is exclusively the responsibility of the entity.

Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.		
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.		
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.		
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). ***Note:*** *Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*	Entity Responsibility	Execution of periodic vulnerability scans addressing "high-risk" vulnerabilities is the responsibility of the entity. However, Oracle provides details on vulnerabilities to the Exadata platform and provides patching support for vulnerabilities. Oracle also maintains documentation on common vulnerabilities identified on Exadata by vulnerability scanning tools.
11.2.1 Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.		
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. ***Note:*** *Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.*		
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change.		

Scans must be performed by qualified personnel.		
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	Entity Responsibility	Ensuring that penetration tests are conducted and findings are remediated are exclusively the responsibility of the entity.
11.3.1 Perform external penetration testing at least annually 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).		
11.3.2 Perform internal penetration testing at least annually 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).		
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.		
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.		
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing		

penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. ***Note:*** *This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*		
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Entity Responsibility	Exadata have an option to use Oracle Virtual Machines (OVMs) that have Oracle Linux installed on them. Entity has an option to install any host based intrusion detection or prevention system available for Oracle Linux. Network intrusion-detection and prevention should also be implemented at the perimeter of the cardholder data environment by the entity.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. ***Note:*** *For change-detection 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. Change-detection mechanisms such as 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).*	Entity Responsibility	Exadata have an option to use Oracle Virtual Machines (OVMs) that have Oracle Linux installed on them. The entity has an option to install any change detection mechanism that is available for Oracle Linux.
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	Entity Responsibility	Responding to alerts, and development and communication of security policies are process controls that are exclusively the responsibility of the entity.
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.		

REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR ALL PERSONNEL

Policy maintenance and communication, risk assessment, security awareness program, vendor management, and incident response are process controls that are exclusively the responsibility of the entity.

APPENDIX A1: ADDITIONAL PCI DSS REQUIREMENTS FOR SHARED HOSTING PROVIDERS

Exadata architecture lends itself for hosting multiple databases with different compliance requirements and the architecture supports multi-tenant environments. Oracle Database Servers and Storage Servers within Exadata can be implemented on separate physical disks or can use Oracle Virtual Machines (OVM) architecture. InfiniBand partitions and VLAN segmentation implemented within OVM architecture automatically provide the necessary segmentation between the database and storage nodes belonging to different entities. Additionally, ASM and database scoped security implements the access control mechanism to prevent nodes from RAC cluster from accessing the storage disks associated with another cluster.

PCI DSS Requirement	Coverage Status	Exadata Supporting Features
A.1 Protect each entity's (that is, merchant, service provider, or other entity) hosted environment and data, per A.1.1 through A.1.4: A hosting provider must fulfill these requirements as well as all other relevant sections of the PCI DSS. ***Note:*** *Even though a hosting provider may meet these requirements, the compliance of the entity that uses the hosting provider is not guaranteed. Each entity must comply with the PCI DSS and validate compliance as applicable.*	Provided	Exadata is designed to support multi-tenant environments. InfiniBand partitions and VLAN segmentation implemented within OVM architecture automatically provide the necessary segmentation between the database and storage nodes belonging to different entities. Hosting provider could control and configure the granularity of the segmentation and role based access control mechanism to restrict each entity's traffic and access to its own environment.
A.1.1 Ensure that each entity only runs processes that have access to that entity's cardholder data environment.		
A.1.2 Restrict each entity's access and privileges to its own cardholder data environment only.		
A.1.3 Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.	Supported	Exadata has auditing capabilities available for all components. Auditd is installed on all components and audit rules can be configured to record audit trails for all system components and control the collected features. Additionally, syslog.conf can be configured to direct the logs to a centralized syslog servers. Auditd and syslog configurations can be set to segment the logs for each entity in a multi-tenant environment. Built-in role base access controls within Exadata can be used to restrict access to the logs to appropriate entities.
A.1.4 Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.	Entity Responsibility	Forensic investigation is a process control that is the exclusive responsibility of the entity and the hosting provider.

APPENDIX A2: ADDITIONAL PCI DSS REQUIREMENTS FOR ENTITIES USING SSL/EARLY TLS

Exadata supports the use of TLS1.0 and SSLv3 on compute and storage nodes, however, the settings can be configured to disable the use of these protocols. Ensuring that TLS1.0 and SSLv3 are not configured for use is exclusively the responsibility of the entity, validating logical access controls, and responding to suspicious events are process controls that are exclusively the responsibility of the entity.

APPENDIX A3: DESIGNATED ENTITIES SUPPLEMENTAL VALIDATION (DESV)

Implemention of a PCI DSS compliance program, documentation and validation of PCI DSS scope, incorporation of PCI DSS into business-as-usual (BAU) activities, validating logical access controls, and responding to suspicious events are process controls that are exclusively the responsibility of the entity.

Note: This applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements.

CONCLUSION

Exadata is an integrated technology platform that is designed to consolidate database servers, storage servers, and InfiniBand networks into a single scalable platform. Exadata is primarily designed and implemented by organizations to support database functions. Exadata has segmentation technologies available that makes it suitable for deploying multiple or mult-tenant environments, some of which may require compliance with PCI DSS v3.2. Exadata, Oracle Database, and other support utilities provide features that enable organizations to achieve compliance for their databases even in multi-tenant environments.

REFERENCES

1. PCI Security Standards Council, LLC. (2016). Payment Card Industry Data Security Standard version 3.2.
2. PCI Security Standards Council Virtualization Special Interest Group. (2011). Information Supplement: PCI DSS Virtualization Guidelines.
3. Oracle. (2014). Exadata Overview From PCI Perspective.
4. Oracle. (2015). Exadata OVM Overview.
5. Oracle. (2015). Configuring Security for Oracle Exadata Storage Server Software.
6. Oracle. (2016). Implementing InfiniBand Partitioning across OVM RAC clusters on Exadata.
7. Oracle. (2016). Implementing Tagged VLAN Interfaces in Oracle VM Environments on Exadata.
8. Oracle. (2016). Exadata Maintenance Guide.
9. Oracle. (2016). Using the ExaCLI Utility.
10. Oracle. (2016). Database Enterprise User Security Administrator's Guide.
11. Oracle. (2016). Oracle Exadata Database Machine Security Guide.

ACKNOWLEDGEMENTS

The author would like to acknowledge the following individuals from Oracle for their contributions to this paper: Manish Shah, Dan Norris, Tina Rose, Tim Shetler and Kristian Toms. In addition, the author recognizes Deepa Saldana of Coalfire for her contributions to making this paper a possibility.

ABOUT THE AUTHOR

Mukul Gupta | Senior Manager | Technology Advisory & Assessment Services

Mukul Gupta has over 15 years IT Security experience and currently advises, evaluates, and assesses organizations on their information security practices to assist organizations in minimizing IT risks and achieving compliance goals.

THE NATION'S CYBER RISK MANAGEMENT AND COMPLIANCE LEADER

With more than 15 years in IT security and compliance and ASV-certified since inception, Coalfire is a leading provider of IT advisory services, helping organizations comply with global financial, government, industry, and healthcare mandates while helping build the IT infrastructure and security systems that will protect their businesses from security breaches and data theft.