

Oracle Managed Compliance Services

ORACLE® Advanced Customer Services

KEY FEATURES

- Systems monitoring, alerts, and access control
- Frequent vulnerability assessments
- Proactive risk detection and improvement recommendations
- External and internal scans
- Installation and management of applicable Oracle security software
- Complete and accurate reporting and documentation according to compliance requirements
- PCI Level 1 compliant service provider for customers hosted in the Oracle data centers

KEY BENEFITS

- Compliance of platforms, processes, security, and identity management procedures in Oracle Cloud environments with required standards of PCI, HIPAA, and GxP/FDA
- Protection of Electronic Protected Health Information (ePHI) against unauthorized access and attacks
- Security and identity management in Oracle Cloud or on premises
- Enable smooth transition to Oracle Fusion SaaS
- Seamless service delivery management
- Reduced time and cost

Oracle Managed Compliance Services help customers define and manage their cloud platforms and processes according to industry standards or legislative regulations. This includes Payment Card Industry-Data Security Standards (PCI-DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and GxP validation. Oracle Managed Compliance Services packages include design, implementation, monitoring, ongoing management, and reporting.

Enabling Compliance with Industry and Regulatory Standards

Compliance with industry and regulatory standards is mandatory for many enterprises, especially financial services and healthcare industries. Required standards in data security, integrity, and privacy can be challenging to achieve and maintain in cloud deployments. Mandatory audits and reporting call for a high level of expertise and can bind significant resources of enterprise security teams throughout the year.

Applicable Regulations	
Payment Card Industry (PCI)	Compliance with the PCI-DSS is an international requirement by the payment card industry for enterprises and government agencies that store, process, or transmit credit card information. Advanced Customer Services for customers hosted in the Oracle data centers recognized by Visa and Mastercard are PCI Level 1 compliant service providers since 2006.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	HIPAA is a legislative requirement in the United States, which aims at health insurance portability, reduced healthcare fraud, security and privacy of health information, and enforced standards of health information. Applicable companies must also comply with the required standards of "electronic protected health information" (ePHI). Advanced Customer Services maintains a HIPAA Certification with an annual third-party audit.
FDA 21 CFR Part 11 and International Equivalents	The Food and Drug Administration (FDA) regulations for the United States and European Union Annex 11 require complete and accurate production documentation, quality testing data management, and records to support audit needs as well as accurate process instructions, revision control, and change control processes.

Oracle Managed Compliance Services are designed to help customers efficiently achieve and maintain compliance with the required security and regulation standards in Oracle Cloud deployments including Oracle SaaS, Oracle PaaS, Oracle Cloud Infrastructure (OCI), and Oracle Cloud at Customer. Oracle Advanced Customer Services has many years of experience with ensuring regulatory compliance of Oracle environments.

RELATED SERVICES

- Managed Security Services
- Managed Identity Services
- Managed Database Cloud Service
- Managed Applications Unlimited on Oracle Technology Cloud
- Managed Cloud Help Desk for Applications Unlimited
- Managed Cloud Help Desk for SaaS

Customers benefit from Oracle Managed Compliance Services through:

- **Enablement of efficient and sustainable compliance with required standards of PCI, HIPAA, and FDA 21 CFR Part 11 in Oracle Cloud environments**
- **Security and identity management** according to required standards for managed Oracle environments in Oracle Cloud
- **Seamless service management** with periodic status reviews, comprehensive reporting, and proactive guidance
- **Reduced time and cost associated** with achieving and maintaining compliance regulations in Oracle Cloud environments

Managed Compliance Services

Service Offering	Description
Base PCI Compliance Services *	<p>Safeguards credit card information and maintains compliance with the PCI-DSS.</p> <p>Service features include:</p> <ul style="list-style-type: none"> • Management of Oracle-owned PCI-DSS controls to required standards • PCI-DSS Controls Ownership Matrix identifying responsibility for each control • File integrity and operating system monitoring, alerts, and protection • Annual network and application penetration tests and security assessment by a third party Qualified Security Assessor (QSA) • Quarterly external, PCI Approved Scanning Vendors (ASV), and internal scans using industry-leading QualysGuard platform • Reviews of firewall policies • Network diagrams
Advanced PCI Compliance Services *	<p>Additional services enhancing the Base PCI Compliance Services:</p> <ul style="list-style-type: none"> • Web Application Security (WAS) assessments • Transparent database encryption • Installation, configuration, and management of a Web Application Firewall for internet facing application environments • Network scans for internet facing web service hosted outside of Oracle's data center • Application file review utilizing a credit card discovery tool to conduct reviews of the application files (logs, reports, and transaction output) for the purpose of detecting insecurely stored credit card information
Base HIPAA Security Services *	<p>Centralized management and reporting of ePHI environments to protect against unauthorized access, potential threats or attacks.</p> <p>Service features include:</p> <ul style="list-style-type: none"> • Risk, compliance, and network topology assessments of the ePHI environments against HIPAA controls • Operating System management to protect against dictionary and brute force attacks • Deploying, monitoring, and managing third party host-based Data Loss Prevention (HDLP) software on Windows workstations to monitor activity of Database Administrators and System Administrators. Alerts and blocks of potential unauthorized access to customer's ePHI • QualysGuard scans of externally accessible web service on the production ePHI environment • Periodic status reviews to identify changes in customer's business or environment that may require modification of the services to address new threats
Advanced HIPAA Security Services *	<p>Additional services enhancing the Base HIPAA Security Services:</p> <ul style="list-style-type: none"> • Identification of system and security vulnerabilities in ePHI environments, including remediation recommendations

	<ul style="list-style-type: none"> • Network and application penetration test for production ePHI environments • File integrity and database monitoring of ePHI environments to detect database security events and potential compromises • Periodic reviews of the firewall policies, network devices, and router configurations for the ePHI environments • Design and deployment of data masking service to mask ePHI stored in the non-production Oracle databases within the ePHI environments • Deployment and management of database encryption in the Oracle database for securing the ePHI environments against attacks at system or operating system level and unauthorized access • Flat File Encryption to protect flat files (excluding database files) that contain ePHI data • Installation, configuration, and management of a Web Application Firewall for internet facing application ePHI environments • Enhanced protection against unauthorized access to web application environments using strong authentication • Network and application penetration test for customer's production ePHI environments
<p>GxP Compliance Services</p>	<p>Enabling compliance with United States FDA 21 CFR Part 11 and European Union Annex 11 regulations by fulfilling platform processes consistently and reproducibly. Computer System Validation (CSV) is the documented process of assuring that a computer system does exactly what it is designed to do in a consistent and reproducible manner.</p> <p>These services enable customers to move smoothly to Oracle Fusion SaaS. Service features include:</p> <ul style="list-style-type: none"> • Support and maintenance of the qualification of customer's platform (IQ/OQ) • Implementation of a standard set of processes to support regulatory needs such as change and access management, physical data center controls, and clear definition of roles and responsibilities • Documentation and reporting including: System Design Document, network diagrams, installation qualifications (IQ) for hardware, operating system, database, and applications • Disaster recovery testing and platform audits

* Availability of Managed Compliance Services for cloud PaaS and IaaS is dependent on Oracle Cloud certification for the base service compliance.

Whether you have to comply with regulatory requirements, or aim to meet or exceed industry standards in Oracle Cloud, Advanced Customer Services has the expertise, tools, and offerings to help you achieve the demanded security levels and gain a competitive advantage.



CONTACT US

For more information about Oracle Managed Compliance Services, visit oracle.com, email us at acs_ww@oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0218