

Oracle Security Review and Recommendations for Oracle Database

ORACLE® Advanced Customer Services

KEY FEATURES

- Comprehensive and detailed security assessment of Oracle Database
- Identify and map existing database security practices and standards
- Detailed technical and executive summary reports provide identification, categorization, and mitigation strategies
- Wide coverage of focus areas include Oracle Database configuration, password security, network configuration, and auditing practices among other areas
- Local and remote delivery options

KEY BENEFITS

- Effective recommendations to mitigate risk based on deep knowledge and expertise of Oracle Database security products
- Reduces security risks due to database configuration issues
- Visualized, intuitive dashboard to categorize risks
- Predictable scope, cost, and timeframe of delivery

Oracle Security Review and Recommendations for Oracle Database is a comprehensive database security risk assessment (DBSRA) designed to detect areas of potential vulnerabilities and identify strategies to mitigate them. This assessment focuses on the database; however, it also examines surrounding system components including storage, network, and applications. It provides a view into data processes and policies with recommended approaches to mitigate potential security risks.

Secure Information from the “Inside Out”

The Oracle Security Review and Recommendations for Oracle Database service is designed to help customers identify and assess security risks, and look at mitigation strategies. This unique and in-depth holistic assessment can be conducted on any number of production or non-production Oracle databases and will:

- **Identify Vulnerabilities:** Identify deviations from standard recommended practices in existing deployments to point out areas where current practices, configuration, and technology implementation leave data at risk of a potential breach.
- **Categorize Risks:** The report will classify and categorize identified risks into severity categories. It will highlight common recommended practices used as a reference. Findings are presented through an intuitive dashboard.
- **Provide Mitigation Strategies:** The report will include recommended strategies to remediate and mitigate as appropriate for associated business practices. Classify mitigation approaches into areas such as configuration, process, and technology that will help identify low-cost and/or low-effort activities easily.

Key Activities

This database security risk assessment follows a multi-stage process with a dedicated Oracle Database security expert. The assessment usually takes about two weeks and is performed onsite or offsite.

Key activities during this engagement include:

- Collection and analysis of information on database configurations.
- Interviews with application owners and administrators to assess database access mechanisms, applications using the target database, information flows, security policies, standard procedures, compliance requirements, use of database security products, and security and compliance strategy.
- Collaborative analysis to develop mitigation strategies and practices covering configuration changes, process modifications, and technology adoption.

RELATED SERVICES

- Managed Security Services
- Managed Identity Services
- Managed Compliance Services
- Managed Database Cloud Service
- Managed Cloud Help Desk for SaaS

Key Activities (continued)

- Assessment scripts including checks for initialization parameters, operating system security, password security, role and privilege assignments, encryption and access control, network configuration, auditing and database links, storage security, database listener security, patch compliance, and adherence to recommended practices. Additional checks may be included to reflect a specific application's use of the database.

In-Depth Database Defense for Maximum Security

Reducing risk at the database level with Oracle Security Review and Recommendations for Oracle Database is key to securing business-critical data. Oracle Advanced Customer Services can strengthen these preventive measures by adding follow-on installation and configuration services for operating system hardening and any needed database security products.

Oracle Advanced Customer Services has many years of experience with implementing Oracle security products and services, and managing security for customer environments in Oracle Cloud or on premises.

The broad portfolio of Oracle Managed Security Services can help customers minimize security risks, and meet compliance requirements. Oracle Managed Security Services can set the stage to use cloud services safely or to integrate with external service providers minimizing risk exposure.

**CONTACT US**

For more information about Oracle Security Review and Recommendations for Oracle Database, visit oracle.com/acs, 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. 0418

