Information Technology

Oracle Database Auditing

Course Introduction

Analysis by security professionals has proven that most vulnerabilities in Oracle database are due to poor configuration of the Oracle database as well as lack of change of vendor default parameters. Attackers as well as dubious operators and administrators try to find these security flaws in the Oracle applications or servers and then try to take advantage of them to steal confidential customer information, modify or delete customer or transaction data to their benefit and gain control of the Oracle database to cause harm or denial of service to the targeted organization. Hence, it has become a must for organizations to educate their System Auditors about security auditing of Oracle database.

This training course is designed to provide participants with the concepts of Oracle Application Auditing. This will focus topics such as how Oracle is built and the concept of what the various categories of user do on the database and the risks they carry. This course will discuss Oracle database and implement security countermeasures that will address the flaws and ensure the overall security of the Oracle database.

Target Audience

- Cloud Computing Engineer
- Computer Network Specialist
- Computer Support Specialist
- Database Administrator
- Information Technology Analyst
- Information Technology Leadership
- Information Security Specialist
- Software/Application Developer
- Web Developer
- Technology sales consultant

Learning Objectives

- Gain a comprehensive understanding of the principle of relational database management system as well as the Oracle database as an object-relational database management system software.
- Understand Oracle Application Security, Application Architecture and common security threats and vulnerabilities associated with Oracle database.
- Know the step-by-step technique of auditing Oracle database.
- Perform access control review of Oracle Database.
- Know and apply best practice security configuration of Oracle database and how to proactively detect poorly configured Oracle application database and ways of remediating same.
- Identify and use best practice organizational policies and procedures required to ensure security of Oracle database.
- Utilize Audit Command Language (ACL) software to perform security audit of Oracle database.
- Provide an audit program or audit checklist for Oracle database.

Course Outline

- **Day 01**

  Module 01: Understanding principles of relational database management system software

- **Day 02**
  - **Module 02**: Oracle application architecture and understanding various threats and vulnerabilities associated with Oracle database.
  - **Module 03**: Best practice configuration of Oracle database and ways to detect security flaws in Oracle database.
- **Day 03**

  Module 04: Step by step process of auditing Oracle database

- **Day 04**
  - ◦ **Module 05**: Understanding Oracle database file and directory permission: Best practice configuration that will ensure security of Oracle system files as well as application audit trail.
  - ◦ **Module 06**: Using Audit Command Language (ACL) software to perform audit of Oracle database
- **Day 05**

  Module 07: Using SQL to perform audit of Oracle database

  - ◦ **Module 08**: Reporting audit exception to management

Confirmed Sessions

FROM	TO	DURATION	FEES	LOCATION
June 30, 2025	July 4, 2025	5 days	4250.00 $	UAE - Dubai
Sept. 22, 2025	Sept. 26, 2025	5 days	4950.00 $	Azerbaijan - Baku
Nov. 24, 2025	Nov. 28, 2025	5 days	4250.00 $	UAE - Abu Dhabi