

Control and Security of Oracle

Course Duration: 2 Days
CPE Hours: 16 Hours
Level: Intermediate/Group-Live
Prerequisites: None
Advanced Preparation: None

This two-day seminar provides participants with a thorough understanding of the key control and security issues of the Oracle Database management product. The session begins with an overview of the Oracle product, its features, and capabilities. Once the basic concepts are understood, the instructor focuses on each of the critical components and provides participants with in-depth coverage of the major control issues. It is essential that strong controls are in place when the product is first loaded to prevent the installation of Trojans and backdoors that can grant unauthorized access to programs and data files. For this reason, the section on product installation and configuration identifies the key control points necessary to establish a security baseline. This ensures security is implemented early in the Oracle development life cycle. The instructor moves on to the controls required for application design and construction, testing, and then implementation. Special emphasis is placed on developing and implementing strong security practices that ensure the programs, databases, and Oracle operating environment are protected. As with all Canaudit control and security seminars, participants receive a series of risk/control tables and checklists to assist in their first audit.

Who Should Attend:

This seminar is intended for auditors and security personnel needing a basic understanding of the control features of Oracle security practices and a solid approach to ensure Oracle security is fully implemented.

Seminar Outline:

I) Introduction

- Why Oracle?
 - ⇒ Most popular database
 - ⇒ Powerful and widely accepted
 - ⇒ Cross-platform capability
 - ⇒ Choice of mainframe
 - ⇒ Capability to span multiple platforms
 - ⇒ World-wide service support
 - ⇒ Multi-language capability
 - ⇒ Large customer base
- Audit risks
- What we need to know

II) Understanding Oracle

- Overview of Oracle
- Database internals
- Memory terminology
- User terminology
- Additional query-related terminology
- Risk/Control tables
- Audit checklists

III) Security and Audit Functions

- Oracle security
- User issues
- User administration
- Oracle auditing function
- Risk/Control tables
- Audit checklists
- Audit software

IV) Operating System Security

- Identifying server security requirements by platform
 - ⇒ UNIX/AIX
 - ⇒ Windows
 - ⇒ Novell NetWare
- Security requirements
 - ⇒ Client and user security
 - ⇒ File data and share security
- Risk/Control tables
- Audit checklists

V) Backup and Recovery

- Oracle backup and recovery
- Exports and imports

- Mirroring, raid and other backup methodologies
- Risk/Control tables
- Audit checklists

VI) Database Administration Issues

- Database layout
- Monitoring the database
- Space: The next frontier
- Other methods to improve performance
- Risk/Control tables
- Audit checklists

VII) Appendix A and B

- Glossary
- Object audit options