Assessors must understand the relationship of the operating system, database server and network environment and how they interact with each other to determine whether data are sufficiently protected. This book explains that DBAs need to work with application developers and security architects to develop a database encryption strategy that meets the security needs of the enterprise. The assessor should review applications, database design documentation and interview management to understand what sensitive data are used by the applications and stored in the applications’ database. In addition, the book covers how encryption can protect highly confidential information from being misused by DBAs and unauthorized persons. The transparent data encryption (TDE) feature, for example, which forms part of Oracle advanced security for the 10g database version, provides column-based encryption for sensitive fields.

Effectively managing security privileges and access controls in the Oracle database is paramount in securing the database. Strong user access control is, therefore, a fundamental component of a good security model. Access security must be flexible enough to control different types of user access, including DBAs. This book explains DBA secure-access control practices from the assessor point of view as the assessor has the “keys to the kingdom,” so it is very important to have controls in place.

Reviewed by Ravi Ayappa, Ph.D., CISA, CRISC, CISM
Who is currently a principal security consultant with Cognizant Technology Solutions based in the United States. Over the last 25 years of his career, he has worked in the domains of governance, risk and compliance consulting; Internet of Things security; infrastructure security; application security; business continuity planning; disaster recovery; and information and communications technology security in Asia, Europe and the United States across various industries, including the military. He is also a volunteer instructor for certification courses at the ISACA® Detroit (Michigan, USA) Chapter.
Vendors managing databases should be bound by service-level agreements (SLAs) that address security requirements, which should be reviewed by the assessors for acceptable use. Security, Audit and Control Features: Oracle Database 3rd Edition explains the procedure for emergency access, how to handle generic accounts, password controls and resource limits.

Auditing helps monitor the database to detect unauthorized activity that may occur. An Oracle database provides the capability to perform granular auditing over any database object or action performed by a user on the system. The various audit options are explained in detail in the book.

This book covers the issue of identifying weak public, private and global database links. It outlines the risk associated with insecure links and actions that can be taken to mitigate this risk. Network security is an important component of an overall Oracle security strategy. This book has a chapter on network security, and that chapter is designed to help the assessor understand network risk associated with the Oracle database. The Transparent Network Substrate (TNS) listener authenticates remote clients to the server and is the first interface for an attacker wishing to compromise the Oracle database, so its configuration needs to be secured. Oracle database servers should reside in a protected database tier in the internal network and should never be accessible from the public Internet.

The book explains how Oracle advanced security can be used for encrypting network traffic among clients, database servers and application servers. Oracle Net Manager can be used to manage Oracle advanced security settings for Oracle clients and servers, including configuration options for authentication, integrity, encryption and SSL security. Centralized user management can be implemented using OID, which can be configured to authorize user connections using LDAP-, Kerberos- or secure sockets layer (SSL)-based authentication.

Key general control environment areas that should be reviewed to help ensure a protected Oracle system, including change management, information classifications, segregation of duties, system development life cycle, incident response, vulnerability and patch management, and monitoring backup and recovery processes are covered in this book.

This book discusses in detail the importance of using secure web-facing applications since vulnerable and insecure applications could be a backdoor entry to data theft despite having a secure Oracle configuration. Tools available in the market that can assess the logical security of the databases are also discussed. An audit plan and internal control questionnaire developed and reviewed with regard to COBIT®, key issues and components are enumerated in detail in this book.

The authors of Security, Audit and Control Features: Oracle Database 3rd Edition are successful in providing high-level guidance to assess security controls in Oracle databases.

Editor's Note

Security, Audit and Control Features: Oracle Database 3rd Edition is available from the ISACA® Bookstore. For information, visit www.isaca.org/bookstore, email bookstore@isaca.org or call +1.847.660.5650.