- *Implementing Database Security and Auditing*, by Ron Ben Natan
- *SQL Server Security*, by Chip Andrews, David Litchfield, Chris Anley, and Bill Grindlay
- *SQL Server Security Distilled*, by Morris Lewis
- *SQL Server Security: What DBAs Need to Know*, by K. Brian Kelley
- *Oracle Privacy Security Auditing*, by Arup Nanda and Donald Burleson
- *Effective Oracle Database 10g Security by Design*, by David Knox
- *Special Ops: Host and Network Security for Microsoft, UNIX, and Oracle*, by Erik Birkholz
- *MySQL Security Handbook*, by John Stephens and Chad Russell
- *Cryptography in the Database: The Last Line of Defense*, by Kevin Keenan
- *Database Security*, by Maria Grazia Fugini, Silvana Castano, and Giancarlo Martella
- *Database Security and Auditing: Protecting Data Integrity and Accessibility*, by Sam Afyouni

Many online technical guides are also available. These guides are often free, up-to-date, and can be accessed from anywhere. Of course, they are also typically incomplete and not nearly as comprehensive as the books just listed.

Resource	Website
Oracle Database Security Checklist, by Oracle Corporation	www.oracle.com/technology/deploy/security/database-security/pdf/twp_security_checklist_database.pdf
SANS Oracle Security Checklist	www.sans.org/score/oraclechecklist.php
Ten Steps to Securing SQL Server 2000	www.microsoft.com/sql/techinfo/administration/2000/security/securingsqlserver.asp
SQLSecurity.com Checklist	www.sqlsecurity.com
NIST Security Checklists	web.nvd.nist.gov/view/ncp/repository
DISA Checklists	iase.disa.mil/stigs/checklist/
ISACA Auditing Guidelines	www.isaca.org
Links to papers and presentations covering Oracle security	www.petefinnigan.com/orasec.htm
Oracle security website	www.oracle.com/technology/deploy/security/index.html

Most database vulnerabilities discovered and fixed can be credited to a relatively small subset of security researchers. Although some groups, including many of the database vendors, view this work as "malicious," security researchers have done the database security market a huge service, and to top it all off, they have done it free of charge. The database vendors themselves have gone as far as to threaten lawsuits and revoke partnership agreements, and they have been particularly vocal about telling customers about how security researchers are "evil." The silver lining is that these security researchers are watchdogs in the community, and many simple security vulnerabilities have been eliminated or at least reduced because of their work. Of course, the vendors have been dragged into securing and fixing their databases kicking and screaming the whole way.

The most prominent database security research teams include the following:

Research Team	Website
Argeniss Information Security	www.argeniss.com
Red-Database-Security	www.red-database-security.com
Application Security, Inc., Team SHATTER	www.appsecinc.com/aboutus/teamshatter/index.html
NGS Research	www.ngssoftware.com
Pentest Limited	www.pentest.co.uk
Pete Finnigan	www.petefinnigan.com
Integrigy	www.integrigy.com
Chip Andrews	www.sqlsecurity.com

These websites serve as the most definitive source of vulnerability information on databases. If you have a question about a particular vulnerability, search these locations, and you're likely to find an answer.

As always, never forget the most up-to-date source of database security—Google. Simply search on any term of interest such as "Oracle Exploits" or "Auditing MySQL." Google provides a great list of resources to explore to help you do your job.

Master Checklist

The following table summarizes the steps listed herein for auditing databases.

Auditing Databases

Checklist for Auditing Databases	
□	1. Obtain the database version and compare it against policy requirements. Verify that the database is running a version the vendor continues to support.
□	2. Verify that policies and procedures are in place to identify when a patch is available and to apply the patch. Ensure that all approved patches are installed per your database management policy.
□	3. Determine whether a standard build is available for new database systems and whether that baseline has adequate security settings.
□	4. Ensure that access to the operating system is properly restricted.
□	5. Ensure that permissions on the directory in which the database is installed, and the database files themselves, are properly restricted.
□	6. Ensure that permissions on the registry keys used by the database are properly restricted.

Checklist for Auditing Databases

□ 7. Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there's a legitimate business need. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.

□ 8. Check for default usernames and passwords.

□ 9. Check for easily guessed passwords.

□ 10. Check that password management capabilities are enabled.

□ 11. Verify that database permissions are granted or revoked appropriately for the required level of authorization.

□ 12. Review database permissions granted to individuals instead of groups or roles.

□ 13. Ensure that database permissions are not implicitly granted incorrectly.

□ 14. Review dynamic SQL executed in stored procedures.

□ 15. Ensure that row-level access to table data is implemented properly.

□ 16. Revoke PUBLIC permissions where not needed.

□ 17. Verify that network encryption is implemented.

□ 18. Verify that encryption of data at rest is implemented where appropriate.

□ 19. Verify the appropriate use of database auditing and activity monitoring.

□ 20. Evaluate how capacity is managed for the database environment to support existing and anticipated business requirements.

□ 21. Evaluate how performance is managed and monitored for the database environment to support existing and anticipated business requirements.

2011

IT Auditing: Using Controls to Protect Information Assets

Second Edition

Chris Davis
Mike Schiller
with Kevin Wheeler

McGraw Hill

New York • Chicago • San Francisco • Lisbon
London • Madrid • Mexico City • Milan • New Delhi
San Juan • Seoul • Singapore • Sydney • Toronto