Database Security
Chapter 9
Security Auditing

Objectives

- Provide an overview of security auditing fundamentals
- Describe the different phases of auditing and identify activities within each phase
- List the goals and objectives of a security audit
- Provide an overview of database auditing fundamentals
- Identify the auditing activities that are specific to database security auditing
- Identify the auditing tasks that are specific to supporting database tools

+

Security Auditing

- Security audit
  - Review of an environment's security controls and systems to identify weaknesses
  - Meant to provide an accurate view of organization's security controls
    - To initiate positive changes for weak areas
  - Can be an important security measure in itself
- This section addresses:
  - Purpose of a general security audit
  - Common characteristics of the auditing process

Audit Classification

- Frequency of security audits
  - Depend on nature of the business
- Audits can be conducted:
  - Informally as part of an organization’s yearly self-assessment
  - After a security intrusion
  - In reaction to an identified risk
  - Formally to satisfy industry-specific standards or laws

Audit Classification (cont'd.)

- Reason for audit
  - Determines individuals who conduct it
- Audits to satisfy legal obligations generally conducted by third-party group
- Self-assessment audits generally conducted by internal committee
- Auditing classifications
  - Informal audits
    - Provide evidence that security policies and practices are effective and working properly

Audit Classification (cont'd.)

- Auditing classifications (cont'd.)
  - Formal audits
    - Conducted to satisfy specific industry standards that are required by law
  - Internal audits
    - Initiated from within the organization to serve as a self-assessment
  - External audits
    - Conducted by third-party group
  - Automated audits
    - Uses tools to record typical system behavior

The Goal of an Audit

- Internal security controls
  - Systematic measures and checks to ensure networks remain secure
- Audits meant to provide accurate view of these controls
- Security audit does not remove vulnerabilities
  - Only tests to ensure proper policies and procedures are in place to handle a potential vulnerability

The Goal of an Audit (cont'd.)

- Auditor's goals
  - Identify security measure's purpose
  - Locate any risk on the network that might prevent security measure from achieving its purpose
  - Search for process or practice already in place to mitigate the identified risks
  - Report any areas in which risks are identified and no mitigation process is in place

The Auditing Process

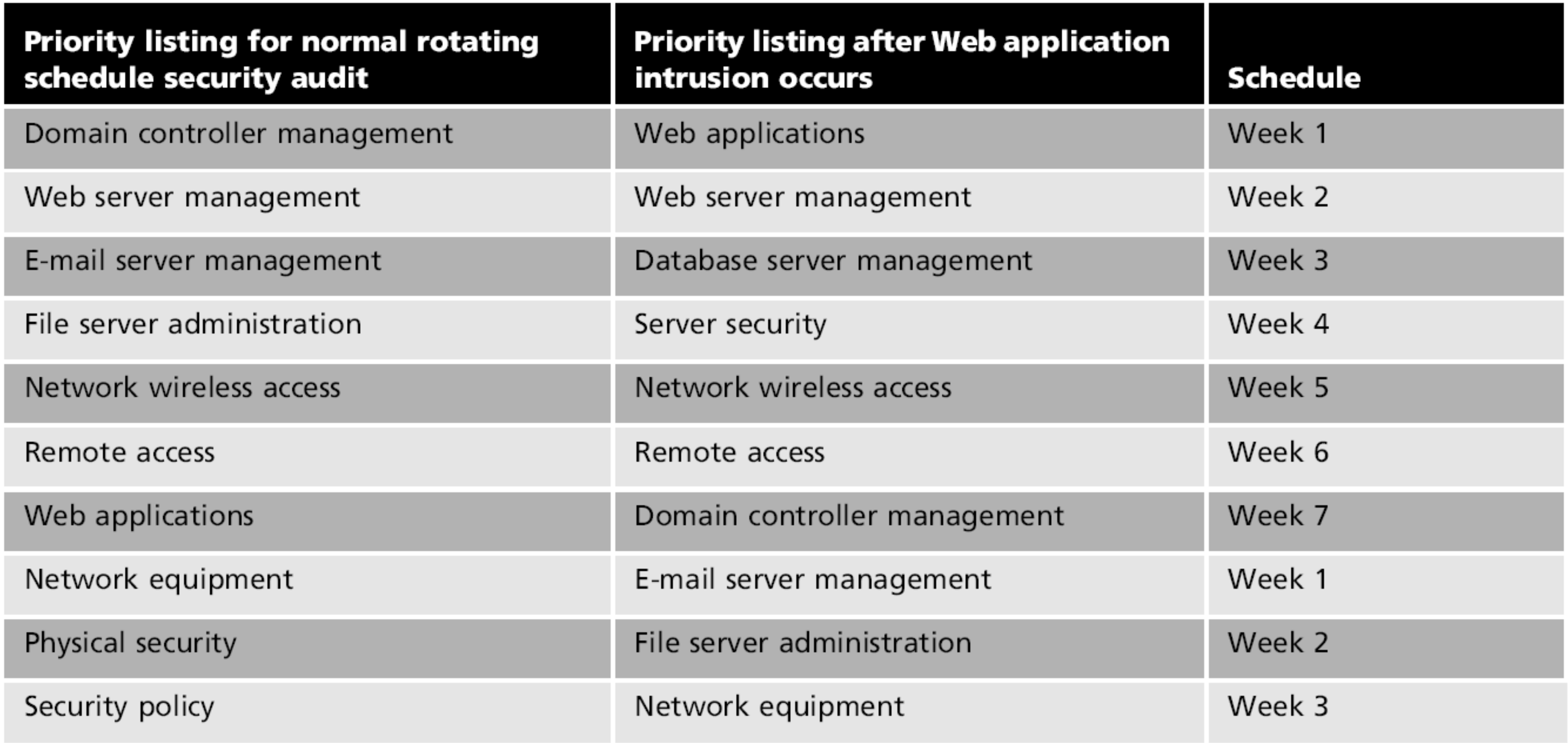
- Audit process characteristics
  - Prepare
  - Audit
  - Report
- Planning and preparation phase
  - Determine what systems, department, or component of the organization will be included
  - Conduct preliminary interviews to learn about network and business structure
  - List and prioritize assets
  - Identify potential threats

The Auditing Process (cont'd.)

- Audit scope
  - Area or systems on which security audit will focus
- Defining scope is one of the most important steps
  - Identify priority assets
  - Make conceptual perimeter of the security audit
- Understand network and organizational structure
  - People, policies, systems, and controls
  - List tangible and intangible assets
  - Prioritize assets

+ The Auditing Process (cont'd.)

- Audit plans
  - Include logistical details and information already gathered
  - Include backup strategy and impact to daily operations
- Nearly impossible to conduct security audit on all areas of the network at the same time
  - Several small security audits should be scheduled
  - Schedule may be modified if an elevated risk is identified



Priority listing for normal rotating schedule security audit	Priority listing after Web application intrusion occurs	Schedule
Domain controller management	Web applications	Week 1
Web server management	Web server management	Week 2
E-mail server management	Database server management	Week 3
File server administration	Server security	Week 4
Network wireless access	Network wireless access	Week 5
Remote access	Remote access	Week 6
Web applications	Domain controller management	Week 7
Network equipment	E-mail server management	Week 1
Physical security	File server administration	Week 2
Security policy	Network equipment	Week 3

Table 9-1 Sample security auditing schedule

+ The Auditing Process (cont'd.)

- Priority shifts could cause certain areas to be left unchecked for a time
  - Defeats the purpose of a proactive security strategy
- Organization should do little preparation for a security audit
  - Conduct daily activities in typical form
- Some organizations prepare extensively for audits
  - Do not want negative repercussions from audit results
  - Provides inaccurate view of the typical environment

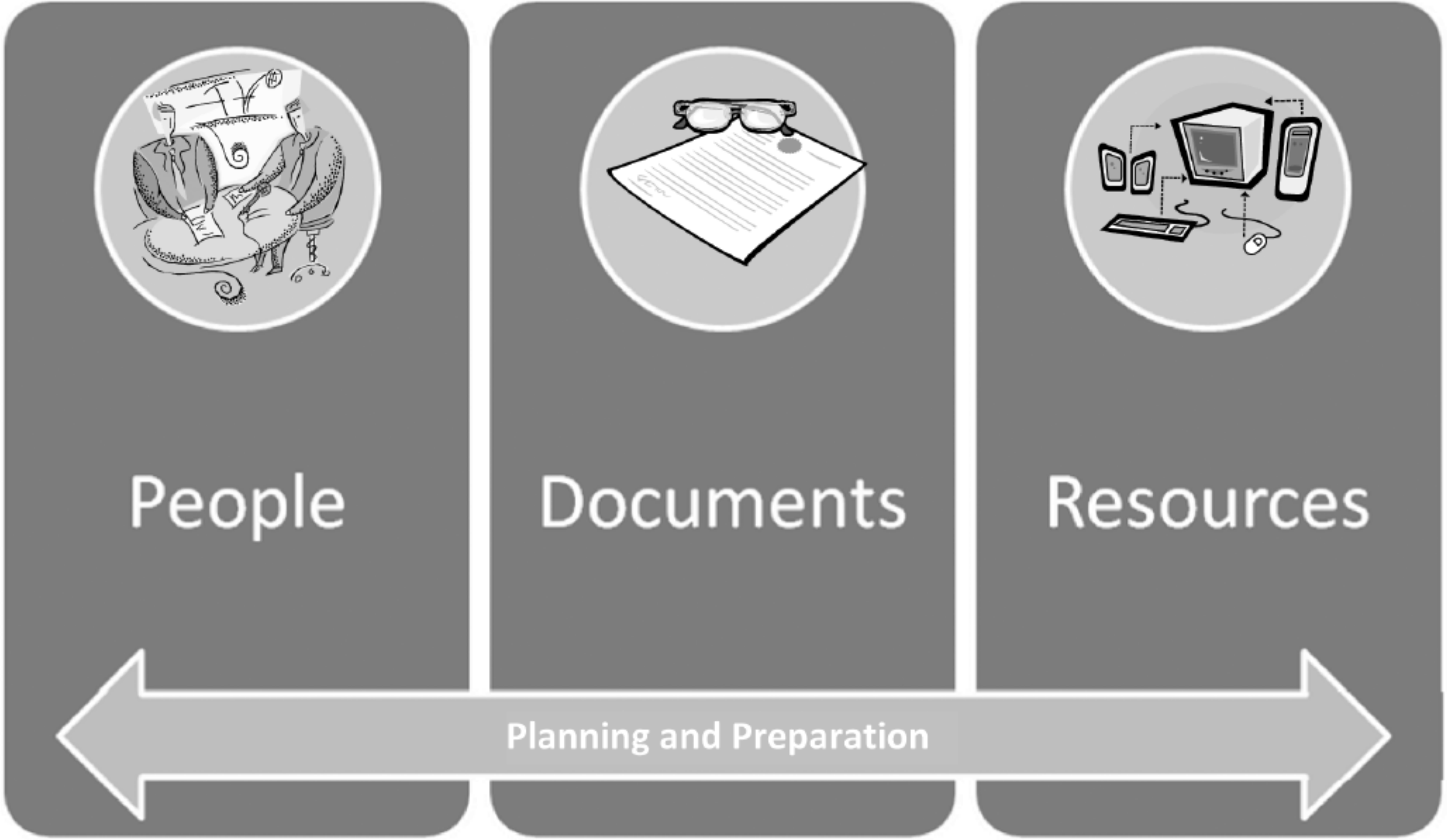
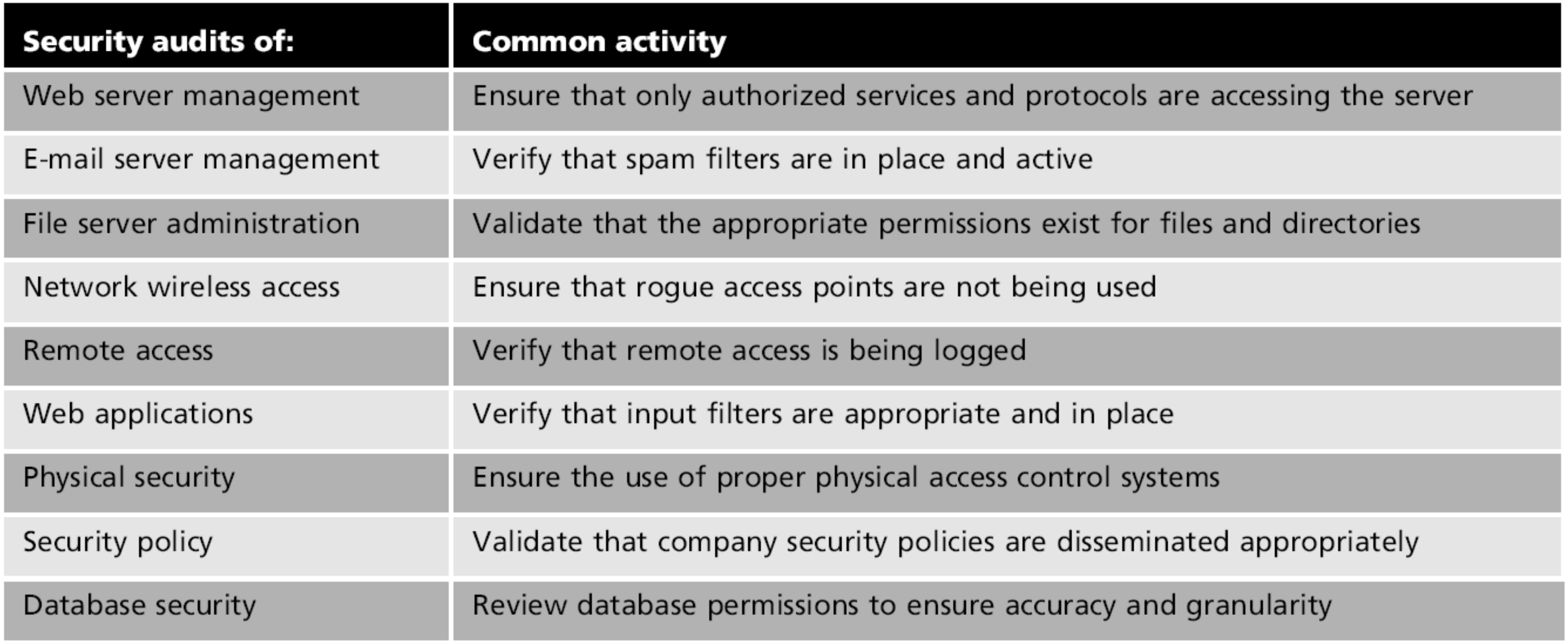


Figure 9-1 Planning and preparation
© Cengage Learning 2012

The Auditing Process (cont’d.)

- The audit
  - Plan is put into action
  - Activities vary depending on scope, type of audit, and the organization
  - Validate risks or concerns using business policies identified during planning stage
  - Ask customers to explain issues as they are found



Security audits of:	Common activity
Web server management	Ensure that only authorized services and protocols are accessing the server
E-mail server management	Verify that spam filters are in place and active
File server administration	Validate that the appropriate permissions exist for files and directories
Network wireless access	Ensure that rogue access points are not being used
Remote access	Verify that remote access is being logged
Web applications	Verify that input filters are appropriate and in place
Physical security	Ensure the use of proper physical access control systems
Security policy	Validate that company security policies are disseminated appropriately
Database security	Review database permissions to ensure accuracy and granularity

Table 9-2 Common security auditing activities

The Auditing Process (cont’d.)

- Reporting a security audit
  - Final step in the process
  - Debriefing meeting where results are communicated
    - Usually involves company’s owners, senior managers, and other stakeholders
  - Vulnerabilities and risks are identified
    - Sometimes strengths as well
- Common components of an audit report
  - Background information
  - Defined perimeter and scope

The Auditing Process (cont’d.)

- Common components of an audit report (cont’d.)
  - Audit objectives
  - Key findings
  - Methodology used to identify risks
  - Remediation recommendations
  - Specific remediation actions to implement recommendations
- Formal or external audit includes deliverables and time frames for implementing expected actions

Database Auditing

- Database audits
  - Should be conducted frequently and thoroughly to contribute to the security measures
- This section explores security auditing process for a database
  - Focus is on the auditing phase itself

Preparation and Planning for a Database Security Audit

- Database-specific planning topics
  - Auditor should gather as much information about the database environment as possible
  - Perimeter should address all layers of a database environment
    - Should include detailed information about people, data, technology, and documents that play a role in the audit
  - Gathering information involves:
    - Interviews with the DBA and database system team
    - Examining schemas, diagrams, policies, procedures

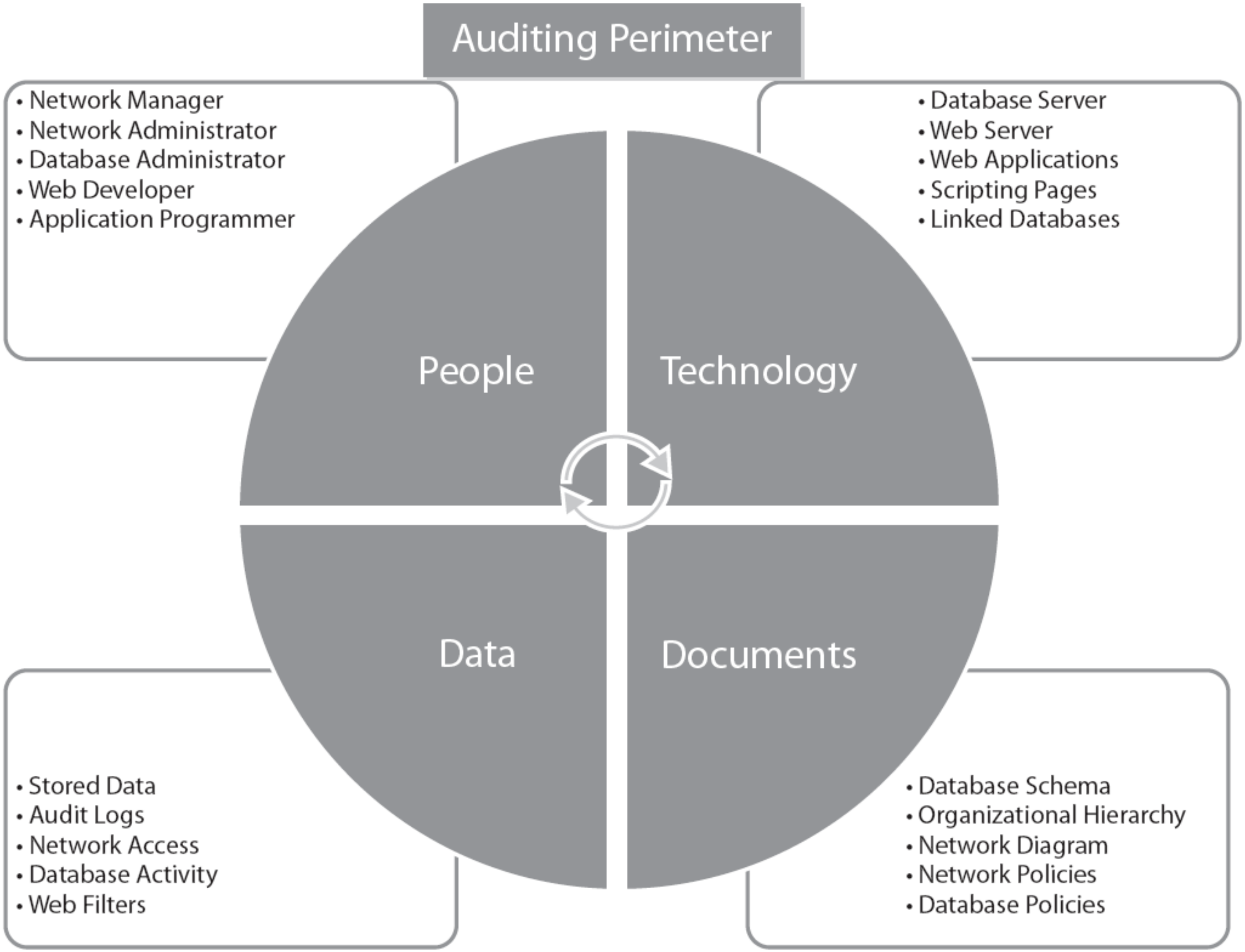


Figure 9-2 Database audit perimeter
© Cengage Learning 2012

Preparation and Planning for a Database Security Audit (cont'd.)

- Analyze how data is stored within the database
  - Builds understanding of relationship between workers and their data needs
- Conduct risk and threat analysis
  - Especially important if database is accessed remotely or from the Web
  - Consider entire database infrastructure
- Two methods of database auditing
  - Focus on database supporting components and then move to database itself, or vice versa

The Database Audit

- Database audits often conducted in small pieces
  - Focus on a specific area of functionality
    - Examples: server maintenance, access control, passwords, account administration
- Topics included in auditing server maintenance
  - Software updates
  - Backup strategies
  - Application version control
  - Resource management
  - Hardware updates

+ The Database Audit (cont'd.)

- Examples of server maintenance audit checks
  - Latest security patches are applied
  - Latest DBMS critical updates have been applied
  - Current version of the DBMS is supported
  - Procedure exists for maintaining patches and software versions
  - Appropriate backup policy exists that includes disaster recovery
  - Feasible and appropriate backup schedule exists
  - Procedure exists to test the integrity of backups

The Database Audit (cont’d.)

- Topics included in auditing account administration
  - Defining and creating user accounts
  - Removing user accounts
  - Applying security policies
  - Assigning groups, roles, and privileges
- Examples of account administration audit checks
  - Administrators’ roles are clearly defined
  - Administrative accounts are distributed appropriately
  - Inactive or unneeded user accounts are removed

+ The Database Audit (cont’d.)

- Examples of account administration audit checks (cont’d.)
  - Generic accounts are not used
  - Default accounts are disabled or removed
  - Application object owner accounts are disabled
  - Backups integrity is tested
- Auditing access control
  - Can be very time consuming
  - Can require logging database access over a period of time

+

The Database Audit (cont’d.)

- Examples of access control audit checks
  - Only trusted IP addresses can access the database
  - Sensitive data is accessed only by those who require it
  - Database links are appropriate
  - Linked databases have applied appropriate access controls
  - Administrators are not able to make changes to the database remotely without special authentication
  - Access to backups and disaster recovery are restricted to administrators only

+ The Database Audit (cont'd.)

- Examples of data privilege audit checks
  - PUBLIC is revoked from the system
  - Implicit granting of privileges is carefully considered
  - The principle of least privilege is utilized
  - Account privileges within the operating system are restricted
  - Privileges are granted using groups rather than individuals
  - Privileges to stored procedures are restricted

The Database Audit (cont’d.)

- Examples of password audit checks
  - Password management capabilities are enabled within the DBMS
  - Password policy includes specifications for failed logins, aging, complexity, history, expiration, and content
  - Default passwords have been changed
  - Passwords are not stored within the database if possible
  - Strong encryption used for passwords stored in the database

The Database Audit (cont'd.)

- Examples of encryption audit checks
  - Stored and moving data is encrypted using strong encryption techniques
  - Encryption is configured accurately
  - Symmetric keys are used for data encryption
  - Sensitive data is documented and labeled as such
  - Passwords are encrypted while remotely logging in to the database

The Database Audit (cont'd.)

- Examples of activity audit checks
  - Auditing has been configured on the server in a way that coincides with the security policy
  - Failed logins are being monitored
  - Failed queries are being monitored
  - Changes to the metadata are being monitored
  - The dynamic SQL that is being executed within a stored procedure is being validated
  - Resource consumption baselines have been set and alerts are being monitored

Reporting a Database Security Audit

- Same considerations as reporting a general security audit
  - Debriefing meeting with stakeholders
  - Written and verbal report
  - Remediation actions
  - Time frame specified for organization to become compliant

Vendor-Specific Auditing Information

- Automatic functions or tools to aid database auditing
  - Included in most types of databases
  - Save time and effort during the auditing process
  - Many tools create logs
    - Can become quite large and resource intensive
    - Purge logs as often as needed
- Microsoft SQL Server
  - Enables tracking and logging of activities throughout all levels of the database

Vendor-Specific Auditing Information (cont'd.)

- Microsoft SQL Server (cont'd.)
  - Auditing can be created at the server or database level
  - Recorded activity send to a target file or Windows event logs
  - Audits can be enabled, reviewed, and created using Object explorer in SQL Server Management Studio
- Steps to create audits in SQL Server
  - Create a server audit object to record desired actions
    - Created at the instance level

Vendor-Specific Auditing Information (cont'd.)

- Steps to create audits in SQL Server (cont'd.)
  - Create a specification object that belongs to either the server audit object or database audit object
  - Custom database audits may be defined for any given action on a database or object
    - Examples: (SELECT, UPDATE, DELETE)
  - Server auditing can be defined to record actions on the server itself
    - Examples: (login information, backups, role changes)

Vendor-Specific Auditing Information (cont'd.)

- Levels of auditing in Oracle
  - Database
    - Monitors changes to a specific database object
  - Application
    - Monitors user sessions
  - External
- Configuring Oracle's embedded tools can be complex
  - First step: enabling default security settings in the Security Settings window in the DBCA

Vendor-Specific Auditing Information (cont'd.)

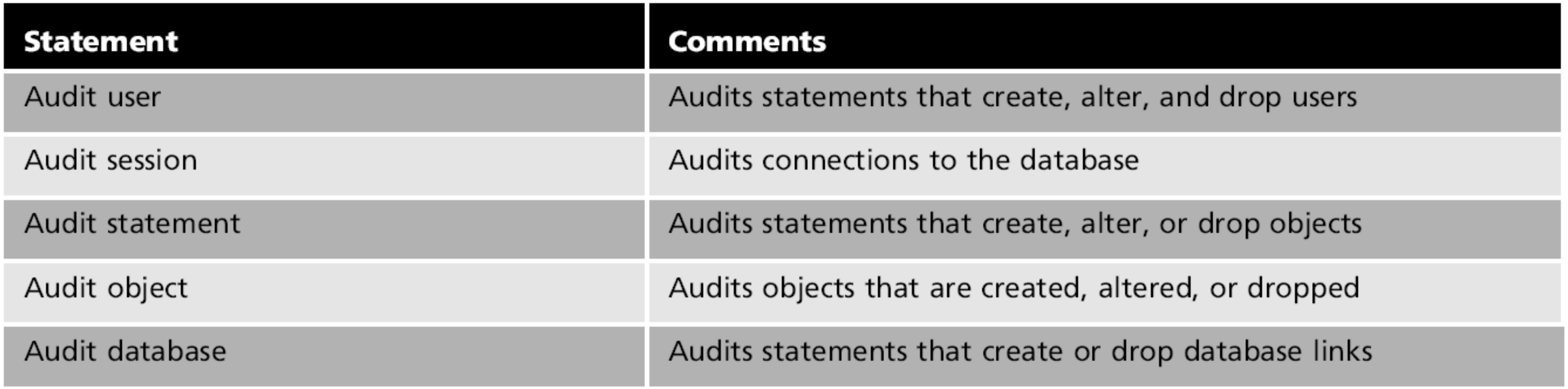
- Oracle's default auditing procedures include:
  - Statements using the ALTER function on procedures, tables, databases, profiles, systems, and users
  - Statements using the CREATE function on libraries, procedures, tables, jobs, database links, public database links, sessions, and users
  - Statements using the DROP function on procedures, tables, profiles, and users

+ Vendor-Specific Auditing Information (cont'd.)

- Oracle's default auditing procedures include (cont'd.):
  - Statements using the GRANT function on privileges, roles, and object privileges
  - AUDIT SYSTEM statements
  - EXEMPT ACCESS POLICY statements
- Default security settings will enable the audit_trail function
  - Allows granular administration of system wide auditing

Vendor-Specific Auditing Information (cont'd.)

- Audit_trail function options
  - None: Disables auditing altogether
  - DB: Enables auditing and sends log to the database SYS.AUD$ table
    - This is the default setting
  - OS: Enables auditing and sends log to the operating system
  - XML: Enables auditing and sends log to an XML operating system file



Statement	Comments
Audit user	Audits statements that create, alter, and drop users
Audit session	Audits connections to the database
Audit statement	Audits statements that create, alter, or drop objects
Audit object	Audits objects that are created, altered, or dropped
Audit database	Audits statements that create or drop database links

Table 9-3 Sample Oracle auditing

Vendor-Specific Auditing Information (cont'd.)

- MySQL
  - No built in auditing tools are available
  - Auditing process involves manual exploration of logs and objects
  - General database security auditing guidelines can be applied
  - Third-party automated auditing tools are available online

+

Summary

- Security audits allow companies to identify vulnerabilities of their security efforts and controls
- Formal or informal audits may be conducted
  - Formal audits ensure compliance with laws
  - Informal audits done as self-assessment or in reaction to an intrusion
- Gaining familiarity with typical database errors is important in identifying system anomalies
- Auditor should gather as much information as possible to prepare for an audit

+
Summary (cont'd.)

- Audit scope identifies what is included and excluded from a security audit
- The security audit report includes background information, scope, defined perimeter, methodology, and key findings
- Remediation actions are defined by a set of deliverables and should include a schedule for completion
- Database auditing can be divided into several different areas of concentration