




After reading this chapter and completing the exercises, you will be able to:

- 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 In Your World

Rae Ann has been running the IT department for a small financial accounting firm in Arizona for a little over a year now. She was hired into the position after the previous administrator, Gary, retired. Gary had worked for the company for over 15 years and built the network from the ground up. Luckily for Rae Ann, Gary was meticulous in his documentation and left several instructional papers that Rae was able to follow throughout the year. One of these documents was a set of strict instructions for how to maintain the company's database storage backup. According to the instructions, full backups are to be run once a day, at the end of the day, while inferential backups are to be completed every hour. An external hard disk is used to store the data at the end of the day. Rae Ann is to walk the hard disk to the local bank and place it in a safety deposit box from which she retrieves it the next morning. This was a solid routine to maintain the integrity of the organization's data, or so it seemed.

Friday was the start of a typical day at the office; the backups were in place and everything was running smoothly. Rae Ann was working on her daily administration tasks when she received a call from the owner of the company explaining that he was unable to access his files from his computer. When she arrived at his desk, she realized that the files were no longer accessible from the file server. After a bit of troubleshooting, she discovered that the file server was out of service. Unable to get the server back up and running, Rae Ann had to find a way to retrieve the owner's files and return them to him, so she decided to use the previous day's backup. As Murphy's Law would have it, the backup server was not reading the files from the backup and she was unable to restore them. She checked Gary's documentation for some type of resolution, but there was nothing in terms of troubleshooting instructions. It seems that Gary never tested the backups or attempted to restore the files once they were saved—so no controls were built into the system to handle a situation like this. As a result, Rae Ann found herself in quite a difficult situation—one that could ultimately have a big impact on her job security.

All of the security measures in the world are insignificant without internal controls and plans to support them. If managers create policies that forbid users to open suspicious e-mails, but do not have a control in place to deal with those who defy the policies, then, in reality, how effective is the policy? It is not easy to identify missing internal controls or poorly written backup plans within an organization's architecture, so often no one is aware that a step is missing until disaster has struck. This is where auditing comes into play. Auditing helps to prevent disasters and improve an

(continued)

environment by locating risks within that environment that exist due to a lack of secondary internal controls.

This chapter explores the security and database auditing processes. It defines the different types of security audits, explores the phases of an audit, and provides tips for locating vulnerabilities within a database environment. Auditing in itself is a strong security practice, and is vital to maintaining the confidentiality, integrity, and reliability of database environments.

Security Auditing

To thoroughly explore the process of database auditing, we must first identify the purpose of a security audit in its most general form. This can be achieved by formulating a basic appreciation of the auditing process and identifying an audit's goal within an environment. This section defines the term *audit*, identifies the purpose of a security audit, and explores common characteristics of the auditing process.

The term **security audit** refers to the procedures by which all of an environment's security controls and systems are thoroughly reviewed to identify and report weaknesses within an organization. Security audits are meant to provide an accurate view of the organization's internal security controls and to initiate positive changes for identified weak areas. Security audits focus specifically on the security of an environment, testing and exploring each layer of security to identify potential existing risks or weaknesses within security controls. They offer great insight into the effectiveness of an organization's security practices.

Security audits are often the means by which companies begin to realize the sheer vulnerability of their security efforts and are important security measures in themselves.

Audit Classification

Security audits can be conducted for many reasons, and the frequency with which they take place is dependent on the nature of the business. Audits should be conducted informally as part of an organization's yearly self-assessment, as a result of a recent security intrusion, or in reaction to an identified elevated risk. They can also be conducted formally, as a way to satisfy a group of industry standards or a set of industry-specific laws (e.g., the Health Insurance Portability and Accountability Act, the Sarbanes-Oxley Act, the Gramm-Leach-Bliley Act).

The reasoning for which an audit is conducted will dictate the individuals chosen to conduct it. For example, audits intended to satisfy legal obligations will be conducted externally or by a third-party group, whereas those that are conducted for the purpose of self-assessment will likely be conducted by an internal committee developed within the organization. The following list identifies different auditing classifications and their typical usage:

- **Informal audits**—Conducted as a way to provide organizations evidence that their security policies and practices are effective and working properly. Although informal audits are most often conducted internally using a committee of the organization's own employees, some organizations hire third-party security consultants to audit the network to obtain the most objective review.

- **Formal audits**—Most often conducted to satisfy specific industry standards that are required by law for certain types of organizations. Formal audits utilize an external group of individuals who are hired or employed by the government or other standard-setting groups for the purpose of conducting an audit. A hospital is an example of an organization that would commonly conduct a formal audit. In a hospital, security is bound by HIPAA, a privacy act that dictates which network security standards must be in place and effectively practiced in network environments that maintain and share sensitive medical records, so informal audits are conducted regularly to ensure compliance with these standards.
- **Internal audits**—Conducted using a committee of individuals who are employees of the company itself. The committees are often composed of individuals from an organization's senior management team and advisory board. Often informal, internal audits that are initiated from within the organization are most likely done as a way to self-assess an organization, to ensure that the company is meeting its auditing standards and complying with its own policies. They can also be conducted in reaction to a certain incident or intrusion, and are used as a way to determine the cause of the negative event.
- **External audits**—Conducted using a third-party group or a number of individuals from a source outside the organization itself. Often formal, these audits are usually conducted to satisfy a requirement or certify that a company is complying with a certain group of standards or laws established by governing bodies or financial institutions. These audits can also be requested by governing bodies or financial institutions out of concern for noncompliance or corrupt undertakings.
- **Automated audits**—Conducted using tools that are either installed onto a machine or embedded within an application for the purpose of recording the typical behavior of a system. The recorded behavior is stored within some type of system or application log. These logs are used to create administrative reports that are analyzed to troubleshoot or validate the system's behavior.

The Goal of an Audit

As mentioned previously, security audits are meant to provide an accurate view of the organization's internal security controls. What are internal security controls and why are they important? Internal security controls are the systematic measures and checks put into place to ensure that networks remain sound and secure. This section provides a real-world example of a security control and identifies its important role in the security auditing process.

A common misconception about security audits is that they are used to remove and eliminate a company's security vulnerabilities. As was explained in Chapter 1, there is no such thing as a foolproof security implementation; no security can be guaranteed with 100 percent certainty. This is true even after a security audit. In fact, a security audit does not remove vulnerabilities at all; it only tests to ensure that the proper policies and procedures are in place to handle a potential vulnerability and that these policies and procedures are followed as needed. The goals of an auditor are as follows:

1. Identify the purpose of a security measure implemented within systems or areas of an organization.
2. Locate any risk on the network that might prevent security measures from achieving this purpose.

3. Search for some type of process or practice already in place to lessen the harm that these identified risks can cause.
4. Report any areas in which risks are identified *and* no process or policy is in place to lessen the harm that these risks can have on the main purpose of a given security measure.

For example, let's say that an auditor learns of a policy that forbids users from leaving their desktops unattended and unlocked. The policy is put into place to lower the potential for unauthorized access to the network. (1. Identify the purpose of a security measure implemented within systems or areas of an organization.) The auditor finds that some employees leave their desk without locking their PCs, disregarding the policy altogether. (2. Locate any risk on the network that might prevent security measures from achieving this purpose.) The auditor waits to see if the desktop automatically locks after a certain period of inactivity. (3. Search for some type of process or practice already in place to lessen the harm that these identified risks can cause.) The PC does not lock automatically after 10 minutes of inactivity, so the auditor writes the incident down for reporting. (4. Report any areas in which risks are identified *and* no process or policy is in place to lessen the harm that these risks can have on the main purpose of a given security measure.)

As this example shows, the goal of auditing is not to fix issues on the network or to identify security holes, but to ensure that processes are in place to deal with potential risks that may exist and that the controls comply with these processes and policies.

The Auditing Process

Although many different types of security audits can be conducted within an organization, the characteristics of the overall process remain consistent for all. The auditing process generally includes three steps: prepare, audit, and report. This section explores these three steps and provides a clear picture of what each entails.

Planning and Preparation Phase The first step in preparation for an audit is the planning and preparation stage. At this time, the auditor is to determine exactly what systems, department, or component of the organization will be included within the security audit. In planning for an audit, the organization will conduct a number of preliminary interviews to ensure that an auditor is thoroughly informed about the network and business structure itself. The tasks included in this phase are defining the audit scope, becoming familiar with the organization or department for which the audit will take place, listing and prioritizing assets, and identifying potential threats. Preparation for an audit will vary greatly from one organization to another, but, for the most part, preparation is highly dependent on the reason for which the audit is taking place (e.g., formal or informal).

The audit scope is the area or system on which the security audit will focus. Defining the scope of the audit is one of the most important steps of the auditing process. During this phase, the priority assets are identified and a conceptual perimeter of the security audit is determined. Related and central assets are studied and classified as being either in or out of the perimeter of the security audit.

This phase requires the auditor to develop a strong understanding of the network and organizational structure. Knowledge of the people, policies, systems, and controls is a necessity that should include an understanding of the relationships and correlations that exist among

them. A list of assets must be made by reviewing inventories, table schemas, network design plans, and organizational hierarchies. Both tangible (e.g., computers, servers, printers, individuals) and intangible (e.g., data, e-mails, Web applications, passwords) items should be included. Threats to these assets must be identified and considered, while prioritization is handled using the results of a risk analysis combined with the objectives of the management personnel. It is good practice to check previous security audit results for clues as to where priorities have been placed in the past.

Once the perimeter has been created and the assets prioritized within it, the objectives of the audit can be clearly defined and a solid plan can be created. The plans will likely include the logistical details as well as the information already gathered. Information such as the date and time of the audit, the backup strategy, and the effect the audit will have on daily operations should all be included.

Because of the many layers (e.g., files, servers, applications, data) and techniques (e.g., policies, firewalls, biometrics, encryption) involved in security, it is nearly impossible to conduct a security audit on all areas of the network at the same time. Therefore, to ensure that enough resources are available for the entire network, several small security audits are scheduled for an organization at different times of the year, each focusing on only one area of the environment. A common breakdown of areas of a security audit includes physical security, operating systems, Web applications, Web server security, database server, policies and procedures, central help desk, and network equipment security.

Often, rotating schedules are used in an attempt to ensure that all areas of the organization are audited over a certain period of time. Rotating schedules appear to work well at first glance, but should be used with caution. As was mentioned in the earlier sections, an audit can be initiated (or take priority) as a result of an elevated risk or recent network intrusion. In these cases, it is almost certain that the existing condition will take precedence over the current rotating schedule, and adjustments will need to be made to the existing table to accommodate the new priority. Whether the items that are listed toward the end of the rotating schedule are reached in a reasonable amount of time is dependent on the number of incidents that may occur in a given period of time.

For example, Table 9-1 displays a potential security auditing rotating schedule for an organization. The first column of the table displays the original rotating security audit schedule for a given organization and the second column displays the same schedule after adjustments were made due to a detected SQL injection intrusion on day one. As shown, the schedule was affected greatly as the priorities shifted and urgent security audits potentially related to the intrusion were pushed to the top of the list, while less urgent tasks, like the physical security audit, were bumped quite a few weeks.

Although this might not seem urgent now, continued future priority shifts can cause certain areas to be left unchecked for an extended period of time. In the example provided in the table, there is a potential that the environment would become a reactive one where only those items that were compromised would obtain highest priority, defeating the security audit's purpose of creating an effective proactive security strategy.

Until now, there has been no mention of the ways an organization prepares for an audit. This section has solely focused on ways an auditor becomes prepared. This is because besides gathering requested information for the auditor, very little preparation should be done on the organizational end. The goal of a security audit is to report an accurate view

| 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

of the organizational control weaknesses, so the desire is to audit the organization while conducting daily activities in its most typical and raw form. Unfortunately, audits are often not welcomed with great anticipation, particularly in situations of formal external audits.

Many insecure organizations fear that the outcome of an audit—if too many weaknesses are found—will result in negative consequences or severe penalties (which may certainly be true in cases where privacy laws are broken) for the organization. These are often organizations that are insecure about the way they create, maintain, and enforce effective internal controls. They tend to overprepare by spending weeks prior to the audit conducting quick but vast cleanup efforts across the company in an attempt to hide or minimize weaknesses that may be found. Some companies even go as far as forging documents and bribing employees to get rid of any evidence of inconsistency. It is an unfortunate reality, but one that is important to be aware of. This type of behavior will skew the audit results by providing an inaccurate view of the typical environment, leaving no room for real growth.

Audits are meant to provide an accurate view of the organization's internal controls and to initiate positive changes of identified weaknesses. To achieve the highest accuracy through an audit, the auditing process itself must be standardized and little to no preemptive preparation should be made within the environment. Figure 9-1 represents all that is involved in the planning and preparation stage of an audit.

The Audit At this point, perimeters have been identified and objectives are well understood, so the detailed security audit plan is put into action. This phase involves activities that help the auditor analyze the environment for potential vulnerabilities. As risks or concerns are identified, they are validated using the business policies and specifications gathered in the planning stage, and are also verified by asking customers to explain issues as they are found. This phase takes the most time in an auditing process. The activities involved in the actual audit depend on a great number of factors, including the type of audit, the audit scope, and the organization. Obviously, an audit that is meant to review the internal



Figure 9-1 Planning and preparation

© Cengage Learning 2012

controls of physical security will involve much different activities than one that is intended to audit internal administration of a database management system (DBMS). Table 9-2 displays a list of common activities that are conducted during the security auditing process for different system type audits.

| 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

Reporting a Security Audit The final step of the security auditing process is a debriefing meeting in which the auditor or committee of auditors communicate verbally and in writing the results of the audit. This communication usually involves the company's owners, senior managers, and other major stakeholders. It provides a detailed view of the organization's internal security controls, including vulnerabilities and risks and, in some

Copyright 2011 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

cases, the strengths are defined as well. The format of the written report is dependent on the classification of the audit (e.g., informal, formal, internal, external, automated) as well as the individual auditors or auditing committee.

Although the format and content will vary, some important commonalities are found within all audit reports. These common components include the background information, the defined perimeter and scope, the objective of the audit, the key findings, the methodology used to identify the risks, and the remediation recommendations. The auditor or auditing committee's recommendations are typically followed by a specific set of remediation actions. If the review was that of a formal audit or external audit, all remediation actions are defined by a set of expected deliverables. The time frame for the submission of these deliverables is set forth and is required for the organization to become compliant. If the review was that of an informal audit or internal audit, all remediation actions need to be tracked internally and the deadlines for deliverables must be met for the audit process to be completed and senior management to be informed of compliance. In some cases, reports provide recommendations with no remediation actions or requirements.

Database Auditing

9

With a general understanding of the security auditing process, we can now explore the security auditing process for a database. This section focuses primarily on the audit phase itself. It revisits the planning and preparation phase to discuss those planning needs that are specific to database management systems, but the primary focus here is the auditing phase itself. Different areas of the database environment are identified and explored and the tasks that correspond with these areas are discussed. This section provides the reader with the tools to perform a security audit on a database management system. Again, it must be reiterated that this process is a cumbersome and laborious one that does not ensure the security of a network. In reality, database auditing takes a great deal of time, effort, and resources, and is not conducted as often as is necessary. Database audits must be conducted frequently and thoroughly to contribute to an environment's security measures. Intruders are sophisticated and their knowledge grows each day; so even under the best of circumstances with best practices put into place, there is no guarantee that an audit will keep a database environment secure.

Preparation and Planning for a Database Security Audit

As mentioned in the previous sections, the preparing and planning stage is the time the auditor takes to get to know the system and the environment. It is at this stage that the audit scope and work perimeter are identified for the area in which the audit will take place. Along with the suggestions provided in the previous section, a few considerations specific to database environments must be addressed during this stage. This section discusses these database-specific planning topics to help an auditor complete a DBMS security audit.

Preparing for a database security audit requires the auditor to gather as much information about the database environment as possible to define the specific perimeter. A perimeter should address all layers of a database environment. It should include detailed information about the people, data, technology, and documents that will play a role within a particular audit. Figure 9-2 provides examples of each of these layers of the environment.

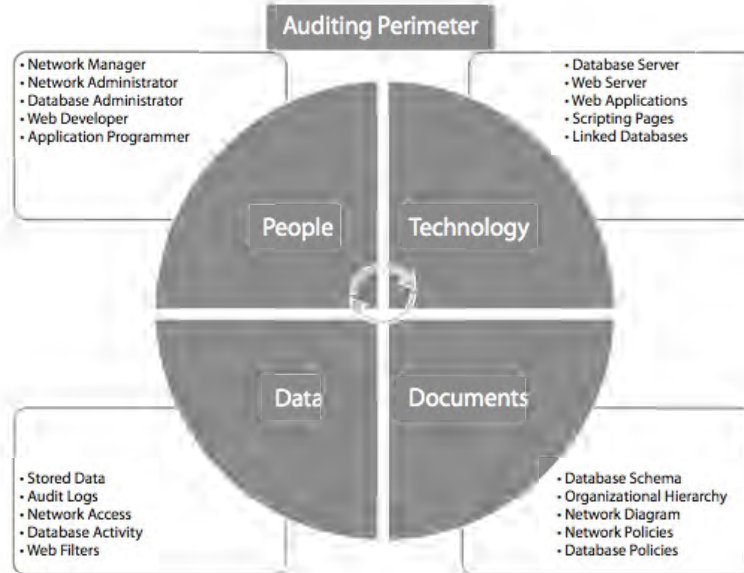


Figure 9-2 Database audit perimeter

© Cengage Learning 2012

Gathering information involves interviews with the database administrator (DBA) and the database system team as well as an examination of the database schemas, network diagrams, and database-related policies and procedures. Organizations often contain several database management systems, so a decision as to how many systems will be audited must be made with purposeful intent.

An understanding of the functionality, purpose, and structure of all database management systems must also be obtained in this stage to conduct an effective and comprehensive audit. Information such as the vendor of the database or the operating system on which the database resides is important, as well as knowledge of the backup strategy that is being implemented. An analysis of the data and how it is stored within the database must be examined and coupled with the organizational hierarchy so as to build an understanding of the relationship between the individuals within the organization and their data storage and manipulation needs.

Risk and threat analysis is another important aspect of planning for a database audit, as it helps to define a prioritized checklist of activities that can be developed as a starting point for the DBMS audit. As was shown in previous chapters, many components of a network interact and communicate with a database. This is especially the case within an environment where the database is accessed remotely or from the Web because many more components are involved in the data-retrieval process. Therefore, to ensure that all measures have been taken to secure the database and that all risks are considered, the entire database infrastructure should be considered any time a security audit is conducted within a database environment.

A thorough audit can be conducted on a database, ensuring that proper security controls are in place for that management system, yet if a Web application that communicates with this database has not been audited, a potential SQL injection risk remains. Database audits can be done in one of two ways. An auditor can choose to focus initially on the database-supporting components (e.g., Web applications, Web servers, middleware, scripting pages) before moving on to the database itself, or the audit can begin at the database and work through the other components thereafter.

Although the rest of this chapter focuses more on the database and less on the database infrastructure's supporting components, a comprehensive and complete audit should include activities that involve the exploration of both.

The Database Audit

Due to the sheer size of a database environment and resources that are required to complete a database audit, they are often conducted in small pieces, focusing on specific functionality or areas of concentration. These different areas of concentration can include server maintenance, account administration, access control, data privileges, passwords, encryption, and activity. This section reviews each of these areas and discusses the activities involved in the auditing process of each.

Server Maintenance Measures should be taken to ensure that servers are being maintained appropriately and policies exist that standardize the maintenance of the database server. Auditing server maintenance includes the review of software updates, backup strategies, application version control, resource management, and hardware updates. Following is a list of audit check examples:

- The latest security patches are applied.
- The latest DBMS critical updates have been applied.
- The current version of the DBMS is supported.
- A procedure exists for maintaining patches and software versions.
- An appropriate backup policy exists that includes disaster recovery.
- A feasible and appropriate backup schedule exists.
- A procedure exists to test the integrity of backups.

Account Administration Account administration is a vital component to database security. The way user accounts are handled is important to access and privilege controls. Auditing account administration includes a review of how the administrator is defining and creating user accounts; removing user accounts; applying security policies; and assigning groups, roles, and privileges. Some sample audit checks include the following:

- Roles for administrators are clearly defined.
- Administrative accounts are distributed appropriately.
- Inactive or unneeded user accounts are removed.
- Generic accounts are not utilized.

- Default accounts are disabled or removed.
- Application object owner accounts are disabled.
- The backup's integrity is tested.

Access Control Access control is the act of minimizing, handling, and detecting user access to the database and its resources. Appropriate access control is essential to ensure the confidentiality, integrity, and availability of the DBMS. Auditing access control is very time consuming and can require the logging of access to the database over a period of time. Some sample audit checks include the following:

- 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 the 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.

Data Privileges Monitoring privileges very closely to ensure security and granularity is a must. Ensuring the appropriateness of privileges during an audit is the most time-consuming task that often requires quite a bit of collaboration with the network administrator. Some sample audit checks include the following:

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

Passwords Strong passwords are critical in a secure environment, as they are the first line of defense that intruders will encounter. Most database management systems can be configured to ensure that passwords meet a specific policy automatically to ensure the strength of the password. Auditing password management involves the review of a written policy, the server configuration, and default user accounts. Some sample audit checks include the following:

- Password management capabilities are enabled within the DBMS.
- The 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.
- Passwords are encrypted using strong encryption if stored in the database.

Encryption Without effective and strong encryptions, data might as well be stored as text. Encryption utilization and sensitive data storage are two considerations that must be included in any database security audit. Encryption should be checked for both stored and moving data throughout the database. Some audit checks include the following:

- Stored data is encrypted using strong encryption techniques.
- 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.

Activity Auditing activity automatically and between larger security audits is a best-practice technique to keeping the database secure. Much information can be discovered using embedded monitoring tools and even logs. In fact, auditing the activity of the database is the means by which much of the information in this section can be identified by an auditor during the database security audit itself. Sample audit checks include the following:

- 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

The final step of the security auditing process is a debriefing meeting in which the auditor or committee of auditors communicates verbally and in writing the results of the audit. This communication usually involves the company's owners, senior managers, and other major stakeholders. It provides a detailed view of the organization's internal security controls, including vulnerabilities and risks and, in some cases, the strengths are defined as well. The format of the written report is dependent on the classification of the audit (e.g., informal, formal, internal, external, automated) as well as the individual auditors or auditing committee. Although the format and content will vary, some important commonalities are found within all audit reports. The common components include the background information, the defined perimeter and scope, the objective of the audit, the key findings, the methodology used to identify the risks, and the remediation recommendations. The auditor or auditing committee's recommendations are typically followed by a specific set of remediation actions.

If the review was that of a formal audit or external audit, all remediation actions are defined by a set of expected deliverables. The time frame for the submission of these deliverables is set forth and is required for the organization to become compliant. If the review was that of an informal audit or internal audit, all remediation actions need to be tracked internally and the deadlines for deliverables must be met for the audit process to be completed and senior

management to be informed of compliancy. In some cases, reports provide recommendations with no remediation actions or requirements.

Vendor-Specific Auditing Information

Most types of databases contain their own unique automatic functions or tools for aiding in the process of auditing database and user activity. These tools often require some type of configuration, but once set up, they can offer great value to the auditing process, saving both time and effort. While reading through this section, keep in mind that many of these tools create logs that contain the information gathered and that the logs are often saved within the database itself. Depending on which actions are selected, these logs can become quite large and resource intensive. It is important to choose your audited activities carefully and to purge your logs as often as needed. This section describes the unique auditing tools found within Microsoft SQL Server, Oracle, and MySQL.

Microsoft SQL Server Microsoft SQL Server enables the tracking and logging of activities throughout all levels of the database. Several features are available that allow administrators to create an auditing trail that best fits their needs. Auditing can be created at the server level or the database level. The recorded activity can be sent to a target file, or to event logs within Windows that the creator of the audit can specify. Audits can be enabled, reviewed, and created using the Object explorer in the SQL Server Management Studio. On this page, the administrator can choose one of two paths, depending on which audit records are desired. These are Security/Audit/Server Audit Specification and Database/Database Name/ Security/Database Audit Specification.

To create audits in Microsoft SQL Server, an administrator must first create a server audit object to record the server or database level actions (or groups of actions) that are desired. These are created at the instance level and more than one audit can be created for each instance. The next step is to create a specification object that will belong to either the server audit object or the database audit object previously created. Database-level auditing provides an administrator with the ability to create custom audits to be defined for any given action (e.g., SELECT, UPDATE, INSERT, DELETE, EXECUTE) on the database or a database object (e.g., tables, views, functions, procedures). Server-level auditing can be defined to record actions performed on the server itself and includes login information, password changes, backups, server role changes, maintenance procedures, schema changes, and permission adjustments.

Oracle Oracle provides several ways to audit the database both manually and automatically, yet the configuration for these embedded tools can be quite complex in their setup. Three basic levels of auditing are available: database, application, and external. Ideally, auditing would be configured at each level to ensure the most comprehensive audit trail, yet resources are not always available. To achieve the best auditing results, both application- and database-level auditing should be configured. Application-level auditing provides information about changes made by a specific user session; therefore, application-level auditing monitors sessions. Database-level auditing provides information about changes made to a specific database object; therefore, database-level auditing monitors databases. Together, they essentially inform auditors what is changed and by whom it has been changed. Therefore, both must be applied for a comprehensive picture of the activities on a database.

The most basic step in beginning the auditing process within an Oracle Database is enabling the default security settings. This can be done within the Security Settings window found in the Database Configuration Assistant (DBCA). Enabling this setting will begin the default auditing procedures that include the following:

- Statements that use the ALTER function on procedures, tables, databases, profiles, systems, and users
- Statements that use the CREATE function on libraries, procedures, tables, jobs, database links, public database links, sessions, and users
- Statements that use the DROP function on procedures, tables, profiles, and users
- Statements that use the GRANT function on privileges, roles, and object privileges
- AUDIT SYSTEM statements
- EXEMPT ACCESS POLICY statements

The default security settings will also enable the audit_trail function, which allows granular administration of systemwide auditing at both application and database layers. There are essentially four options for setting the parameter for the audit_trail function. These options determine whether database auditing is enabled and identify where the audit records will reside. Here is a list of the options for the audit_trail function:

- None—Disables auditing altogether.
- DB—Enables auditing and sends the log to the database SYS.AUD\$ table. This is the default setting chosen when Security Settings is enabled.
- OS—Enables auditing and sends the log to the operating system.
- XML—Enables auditing and sends the log to an XML operating system file.

Table 9-3 provides a list of these options as well as a description of what these options determine. When the security settings are enabled, audit_trail is set to DB, but can be changed by locating the parameter found in int.ora.

Once audit_trail has been enabled, the administrator can begin to audit activities and system characteristics at the application and database levels. As part of the auditing process, an auditor can take note, or log, user login information, unsuccessful password attempts, processes that are executed, processes that are concurrently running, row and table changes, and tables that are accessed frequently. Table 9-3 displays a few common SQL statements used to audit information in Oracle.

| 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

Copyright 2011 Cengage Learning. All Rights Reserved. May not be copied, scanned, or duplicated, in whole or in part. Due to electronic rights, some third party content may be suppressed from the eBook and/or eChapter(s). Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. Cengage Learning reserves the right to remove additional content at any time if subsequent rights restrictions require it.

MySQL At the time of this writing, MySQL has no built-in tools available to aid in the auditing process. The auditing process within MySQL involves the manual exploration of logs and objects, following the general database security auditing guidelines provided earlier in the chapter. Third-party automated tools can be found online to aid in the process of auditing a MySQL database.

Chapter Summary

- Security audits are implemented as a way for companies to identify the vulnerabilities of their security efforts and internal controls.
- Security audits can be formally conducted to ensure compliance with industry standards and privacy laws.
- Informal security audits can be conducted as a way to provide organizations with a clear picture of their internal security controls, or in reaction to an intrusion as a way to identify the vulnerability related to the intrusion.
- External security audits are usually conducted by third-party companies and are most often formally done; the results are reported to government or financially supportive organizations.
- Internal audits are most often conducted informally by an internal auditing team; the results are reported to senior management and CEOs.
- In general, an auditor first identifies a security measure and determines its purposes. Next, the auditor locates any risks associated with the identified measure, and then searches for a company policy or process that exists for handling that risk. So, the primary goal of an audit is to ensure that controls are in place for handling security vulnerabilities and risks.
- Gaining familiarity with typical database errors is important in identifying the anomalies in the system.
- In preparing for an audit, the auditor must first gather as much information as possible from an organization, including network diagrams and employee hierarchical structures.
- An audit scope is created as a way to specify the area of the infrastructure and identify those tasks that will be included and excluded from the security audit.
- An audit perimeter is a specific area of the infrastructure's network diagram that is identified to define those components and areas of the network that will be included and excluded from the security audit.
- Informal security audits are often too resource intensive to be conducted in all areas of an organization at the same time. Therefore, informal security audits are often conducted by breaking the organization into smaller parts for which a rotating schedule is developed to ensure regular maintenance.
- The security audit report will include the background information, the scope, the defined perimeter, the goal, the methodology, and the key findings.
- Remediation actions are defined by a set of deliverables and should include a schedule for completion.

- Database audit planning and preparation include a review of the database schema, the network diagrams specific to the database management systems, and data usage policies.
- Database auditing can be divided into different areas of concentration, such as server maintenance, account administration, access control, database privileges, passwords, sensitive data storage and encryption, and auditing activity.
- Oracle provides several ways to audit the database, including both manual and automatic methodologies. To achieve the best audit results in Oracle, both application- and database-level auditing should be configured.
- The `audit_trail` function allows granular administration of systemwide auditing and is a requirement before any type of automatic auditing can take place within an Oracle database.
- Microsoft SQL Server allows auditing at both the application and database level and the reports can be sent to the operating systems to lessen the database resources used by the report logs.
- Microsoft SQL Server enables administrators to create custom audits for all `SELECT`, `UPDATE`, `DELETE`, and `EXECUTE` actions on a database or database object.
- MySQL requires manual auditing, which involves the review of logs and database objects in hopes of identifying anomalies.

Key Terms

automated audit An audit conducted using tools that are either installed onto a machine or embedded within an application for the purpose of recording the typical behavior of a system.

audit scope The area or system on which the security audit will focus. Defining the scope of the audit is one of the most important steps of the auditing process.

external audit An audit conducted using a third-party group or a number of individuals from a source outside the organization itself.

formal audit An audit most often conducted to satisfy specific industry standards that are required by law for certain types of organizations.

informal audit An audit conducted as a way to provide organizations evidence that their security policies and practices are effective and working properly.

internal audit An audit conducted using a committee of individuals who are employees of the company itself.

internal security controls The systematic measures and checks put into place to ensure that networks remain sound and secure.

security audit The procedures by which all of an environment's security controls and systems are thoroughly reviewed to identify and report weaknesses within an organization.

Review Questions

1. Identify the purpose of an internal audit and an external audit.
2. Identify those persons who might be included within an auditing team for both formal and informal audits.
3. Explain the goal of an auditor. Provide an example to support your response.
4. List the documents that would likely be reviewed in the planning and preparation phase of a formal external audit.
5. What is the difference between a scope and a perimeter?
6. List the typical sections of information included within an audit report.
7. Identify documents that would likely be reviewed in the planning and preparation phase of a database-specific informal audit.
8. List database-supporting components that would require an audit to ensure reliability of the database.
9. Identify and explain the different areas of concentration for database security audits.
10. Explain the purpose of `audit_trail` found within Oracle.
11. Describe the difference between a database-level audit and an application-level audit.

Case Projects



Case Project 9-1: Auditing Organizations

Use the Internet. Find and describe at least one company for which security audits would be required to be compliant with a standardization organization.

Case Project 9-2: Internal Controls

Provide a list of internal security controls that your current school or company has implemented.

Case Project 9-3: Database Auditing

Use the Internet. Find and describe one automated tool that aids in database security auditing. (It is not recommended to install the tool.)

Case Project 9-4: Auditing Oracle

Use the Internet. Identify the steps for creating a custom audit within Oracle.

Case Project 9-5: Auditing MySQL

Use the Internet. Identify a third-party application that can aid in the auditing of MySQL databases.

Case Project 9-6: Auditing Microsoft SQL Server

Use the SQL Server Web site www.microsoft.com/sqlserver/2008/en/us/. Identify the steps for creating a custom audit for Microsoft SQL Server.

Hands-On Projects



Hands-On Project 9-1: Creating and Implementing an Audit

You have been hired as the lead auditor within your own company. You are to create and implement an internal, informal database auditing schedule for the organization. Create a paper that responds to the following:

1. Create a table that includes a rotating schedule for the 12 months of auditing. Include columns that identify time estimates for each audit listed.
2. Create a planning and preparation checklist common to all audits as a whole.
3. Identify any special planning and preparation needed for each individual audit.
4. Identify the scope for each audit and identify any special considerations that need to be addressed.
5. Create a list of at least five audit activities for each audit.
6. Describe any special considerations unique to Oracle that must be addressed.
7. Describe any special considerations unique to MySQL that must be addressed.
8. Describe any special considerations unique to SQL Server that must be addressed.