Database Security and Auditing: Protecting Data Integrity and Accessibility

Chapter 7
Database Auditing Models

Auditing Overview

- Audit examines: documentation that reflects (from business or individuals); actions, practices, conduct
- Audit measures:
  - compliance to policies,
  - procedures,
  - processes and laws

Definitions

- Audit/auditing: process of examining and validating documents, data, processes, procedures, systems
- Audit log: document that contains all activities that are being audited ordered in a chronological manner
- Audit objectives: set of business rules, system controls, government regulations, or security policies

Definitions (continued)

- Auditor: a person authorized to audit
- Audit procedure: set of instructions for the auditing process
- Audit report: a document that contains the audit findings
- Audit trail: chronological record of document changes, data changes, system activities, or operational events

Definitions (continued)

- Data audit: chronological record of data changes stored in log file or database table object
- Database auditing: chronological record of database activities
- Internal auditing: examination of activities conducted by staff members of the audited organization
- External auditing

Auditing Activities

- Identify security issues that must be addressed
- Establish plans, policies, and procedures for conducting audits
- Organize and conduct internal audits
- Ensure all contractual items are met by the organization being audited
- Act as liaison between the company and the external audit team
- Provide consultation to the Legal Department

Auditing Process

- Auditing process: ensures that the system is working and complies with the policies, regulations and laws
- Auditing process is done after the product is commissioned into production.

Auditing Process (continued)

- Auditing process flow:
  - System development life cycle
  - Auditing process:
    - Understand the objectives
    - Review, verify, and validate the system
    - Document the results

Auditing Process (continued)

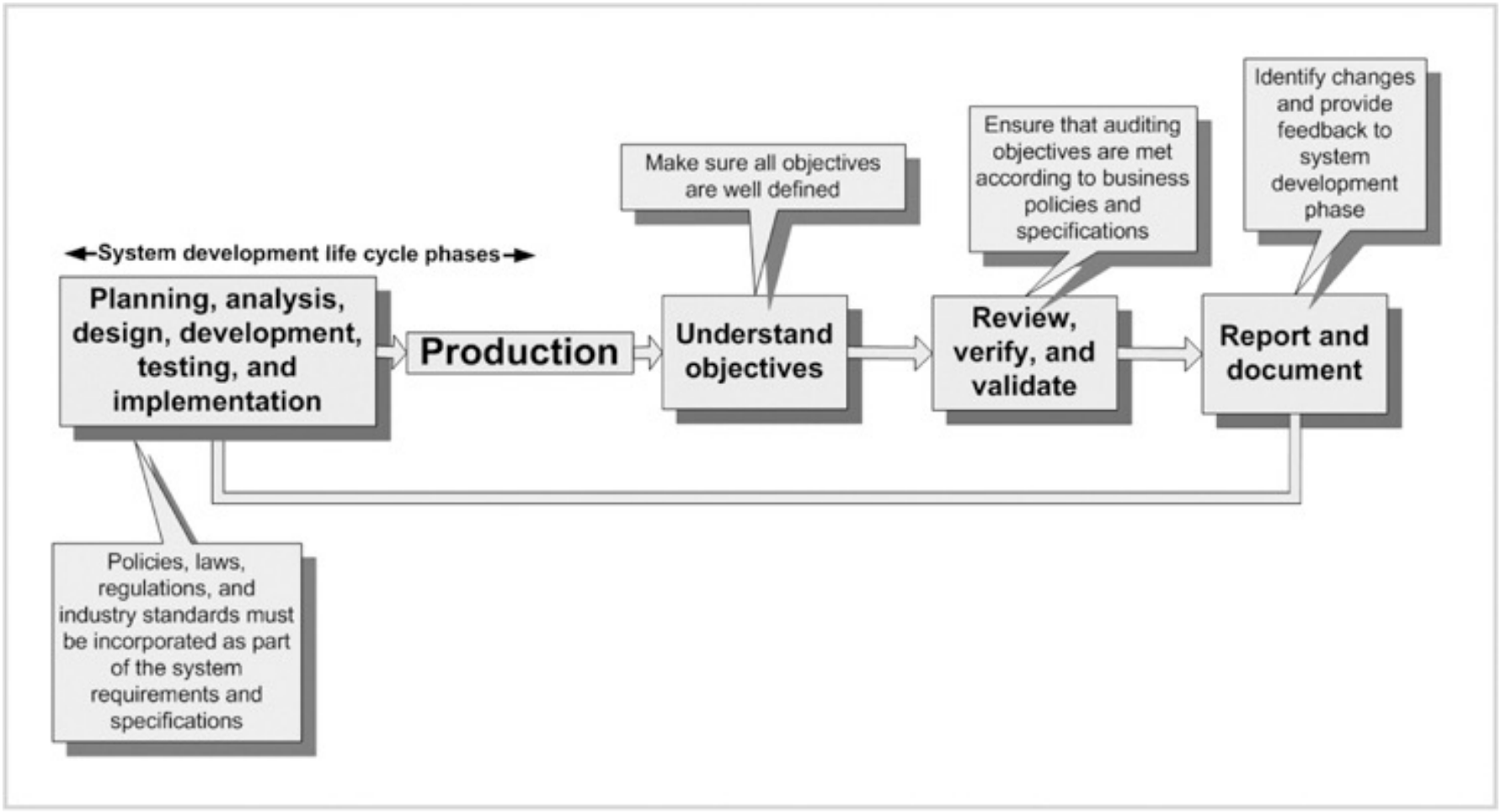

FIGURE 7-4 Auditing process phases

Auditing Objectives

- Part of the development process of the entity to be audited
- Reasons:
  - Complying
  - Informing
  - Planning
  - Executing

Auditing Objectives

- Database auditing objectives:
  - Data integrity
  - Application users and roles
  - Data confidentiality
  - Access control
  - Data changes
  - Data structure changes
  - Database or application availability
  - Change control
  - Auditing reports

Audit Classifications

- Internal audit:
  - Conducted by a staff member of the company being audited
  - Purpose:
    - Verify that all auditing objectives are met
    - Investigate a situation prompted by an internal event or incident
    - Investigate a situation prompted by an external request

Audit Classifications (continued)

- External audit:
  - Conducted by a party outside the company that is being audited
  - Purpose:
    - Investigate the financial or operational state of the company
    - Verify that all auditing objectives are met

Audit Classifications (continued)

- Automatic audit:
  - Prompted and performed automatically (without human intervention)
  - Used mainly for systems and database systems
  - Administrators read and interpret reports; inference engine or artificial intelligence
- Manual audit: performed completely by humans
- Hybrid audit

Audit Types

- Financial audit: ensures that all financial transactions are accounted for and comply with the law
- Security audit: evaluates if the system is secure
- Compliance audit: system complies with industry standards, government regulations, or partner and client policies

Benefits and Side Effects of Auditing

- Benefits:
  - Enforces company policies and government regulations and laws
  - Lowers the incidence of security violations
  - Identifies security gaps and vulnerabilities
  - Provides an audit trail of activities
  - Provides means to observe and evaluate operations of the audited entity
  - Makes the organization more accountable

Benefits and Side Effects of Auditing (continued)

- Side effects:
  - Performance problems
  - Too many reports and documents
  - Disruption to the operations of the audited entity
  - Consumption of resources, and added costs from downtime
  - Friction between operators and auditor
  - Same from a database perspective

Auditing Models

- Can be implemented with built-in features or your own mechanism
- Information recorded:
  - State of the object before the action was taken
  - Description of the action that was performed
  - Name of the user who performed the action

Auditing Models (continued)

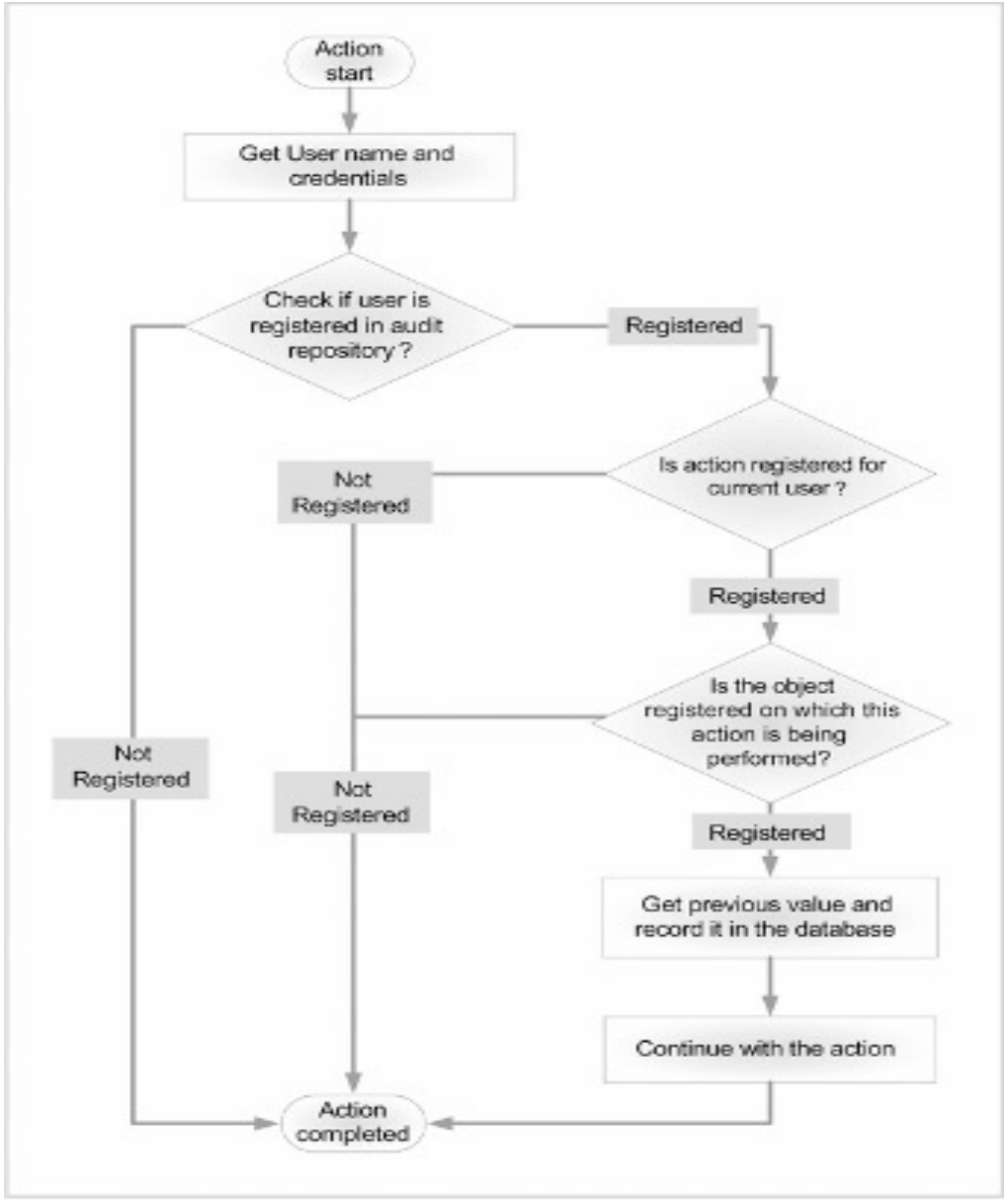

FIGURE 7-5 Data auditing flowchart

User-name

Action

Object

Previous values and record

Simple Auditing Model 1

- Easy to understand and develop
- Registers audited entities in the audit model repository
- Chronologically tracks activities performed
- Entities: user, table, or column
- Activities: DML transaction (update, insert, delete) or logon and off times
- Status: active, deleted, inactive

Simple Auditing Model 1 (continued)

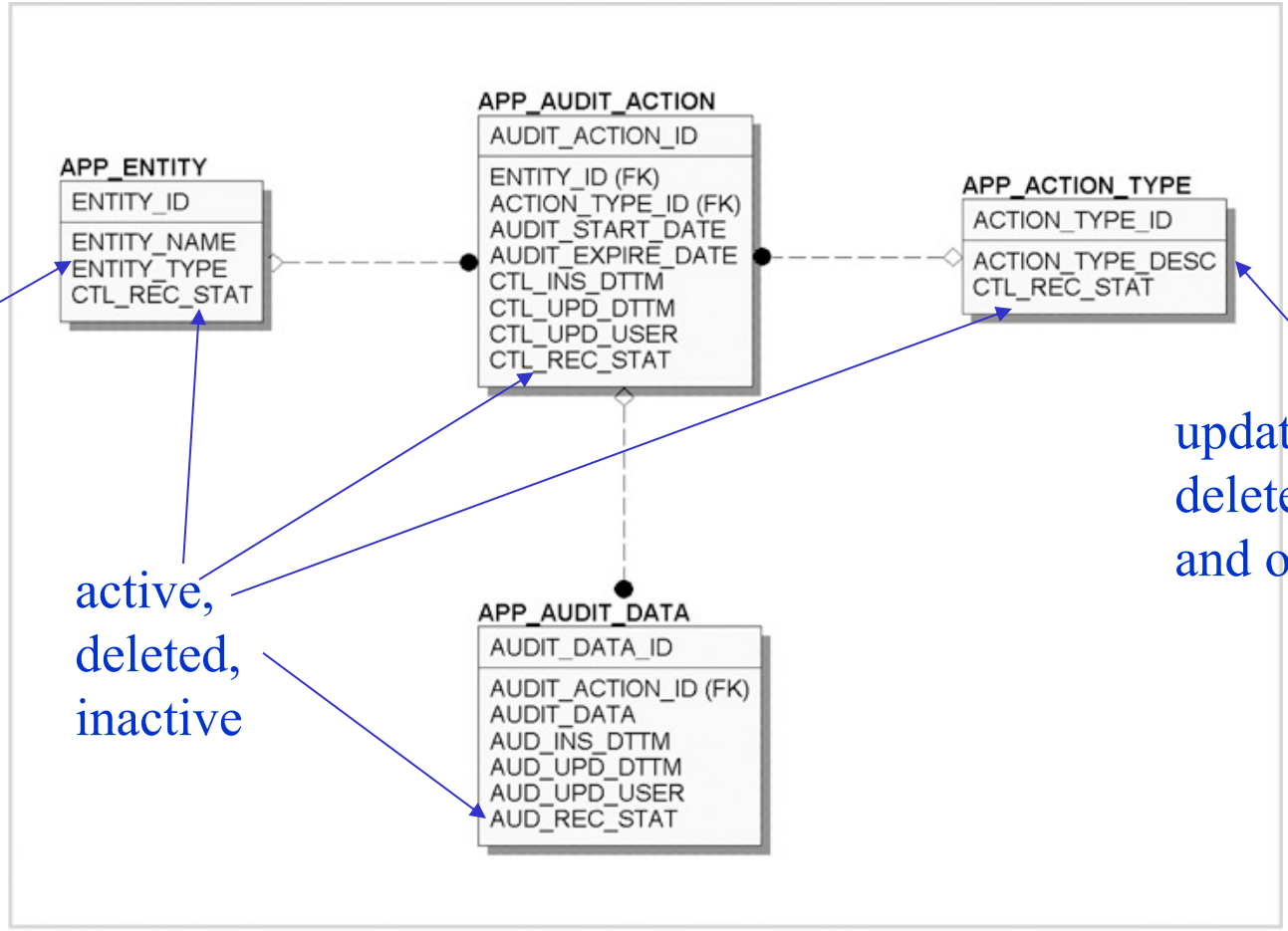

FIGURE 7-6 Data model of a repository for simple auditing model 1

Simple Auditing Model 1 (continued)

- **Control columns**:
  - Placeholder for data inserted automatically when a record is created or updated (date and time record was created and updated)
  - Can be distinguished with a CTL prefix

Simple Auditing Model 1 (continued)

Table 7-4 Description of control columns

Column	Stands for	Description of the Control Column
CTL_ARC_FLAG	CONTROL ARCHIVE FLAG	Indicates whether current record can be archived or not; possible values are Yes and No
CTL_AUD_END	CONTROL AUDIT END	Stores audit end date and time for current record
CTL_AUD_FLAG	CONTROL AUDIT FLAG	Indicates whether current record is audited or not; possible values are Yes and No

Simple Auditing Model 2

- Only stores the column value changes
- There is a purging and archiving mechanism; reduces the amount of data stored
- Does not register an action that was performed on the data
- Ideal for auditing a column or two of a table

Simple Auditing Model 2 (continued)

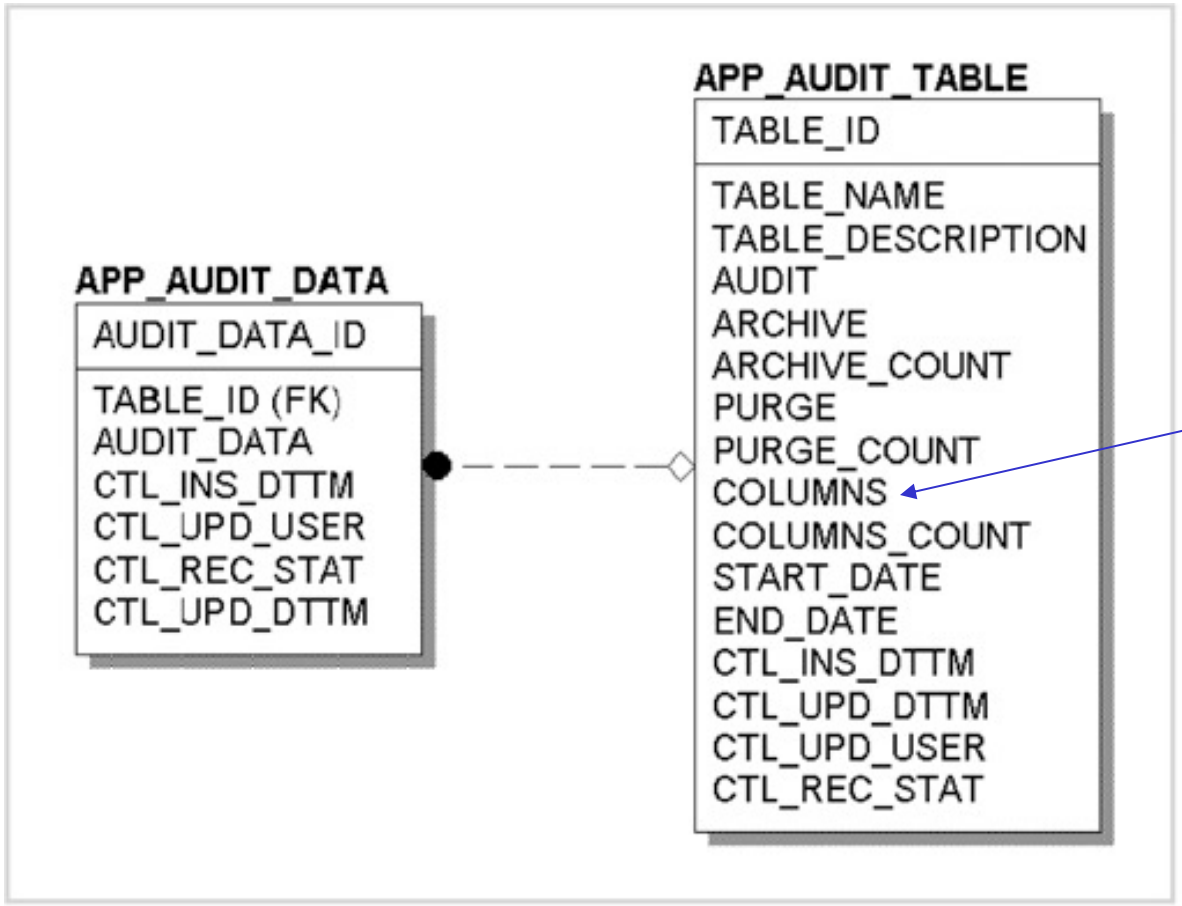

FIGURE 7-7 Data model of a repository for simple auditing model 2

Historical Data Model

- Used when a record of the whole row is required
- Typically used in most financial applications

Historical Data Model (continued)

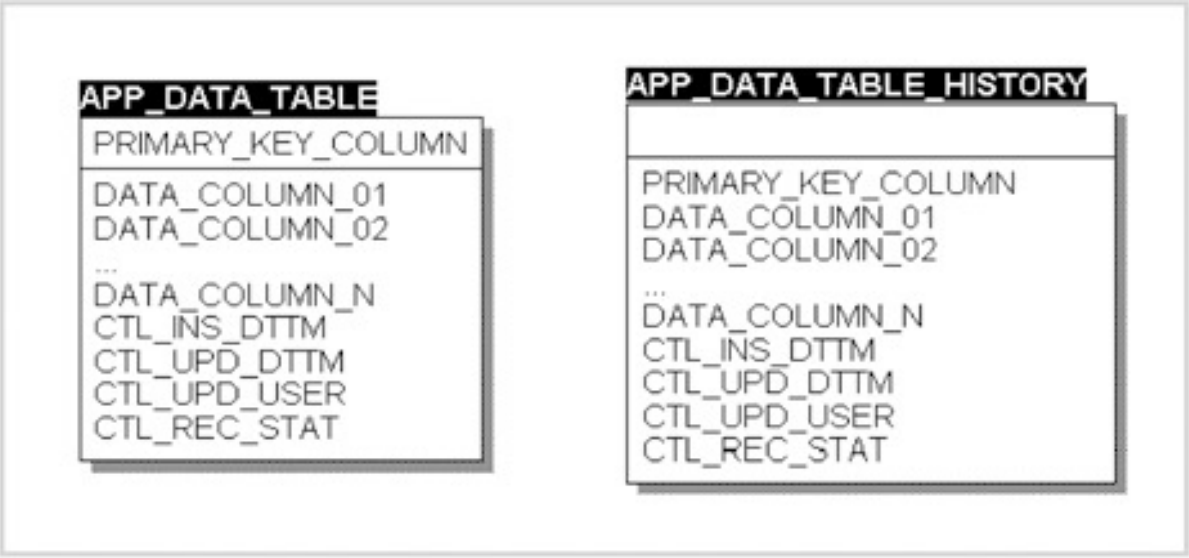

FIGURE 7-10 Data model of a repository for a historical auditing model

Auditing Applications Actions Model

- Used to audit specific operations or actions.
- You may want to audit a credit to an invoice, the reason for it being credited, the person who credited it, and the time it was credited.

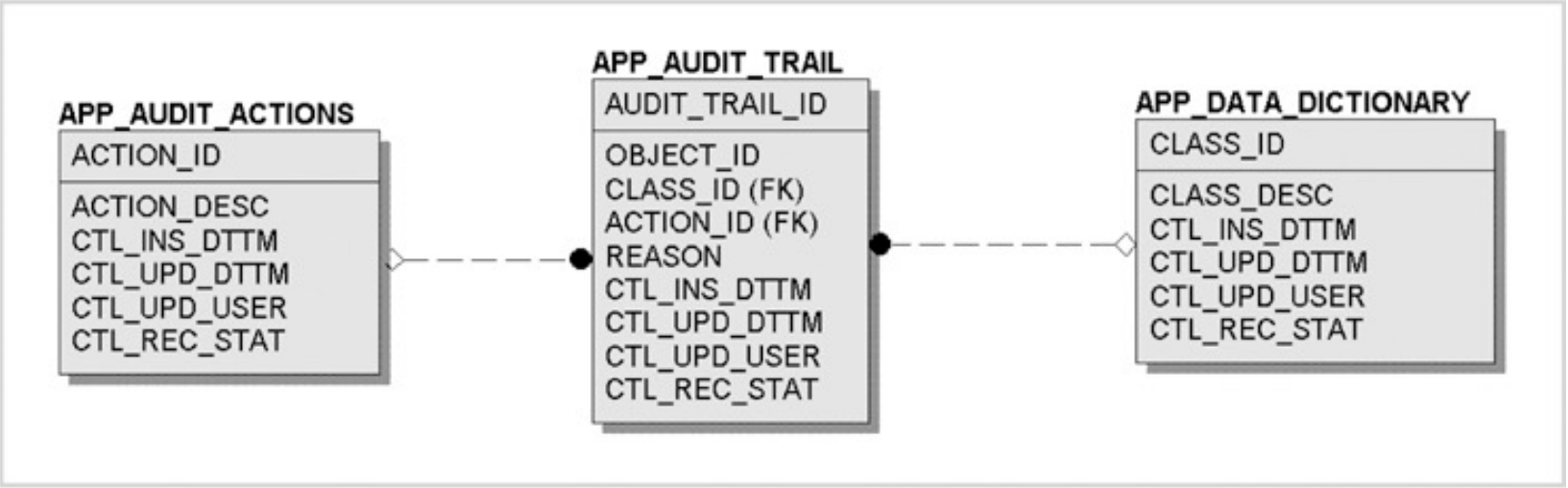

FIGURE 7-11 Data model of a repository for auditing application actions

C2 Security

- C2 security is a government rating for security in which the system has been certified for discretionary resources protection and auditing capabilities.
- SQL server has a C2 certification, but this certification is only valid for a certain evaluated configuration.
- You must install SQL server in accordance with the evaluated configuration.

C2 Security Requirements

- A system must be able to identify a user.
  - Implement the notion of user credentials (e.g., username and a password)
  - Require a user to login using this credentials
  - Have a well-defined process by which a user enters these credentials,
  - Protect these credentials from capture by an attacker.
- Users are accountable for their activities
  - Audit any user activity.
- An owner of an object can grant permissions for access to the object for other users or groups. (what discretionary means)

C2 Security

- If all auditing counters are turned on for all objects, there could be a significant performance impact on the server.
- References: Implementing Database Security and Auditing By Ron Ben-Natan, Chapter 1, page 33-34

DML Action Auditing Architecture

- Data Manipulation Language (DML): companies use auditing architecture for DML changes
- DML changes can be performed on two levels:
  - Row level
  - Column level
- Fine-grained auditing (FGA)

DML Action Auditing Architecture (continued)

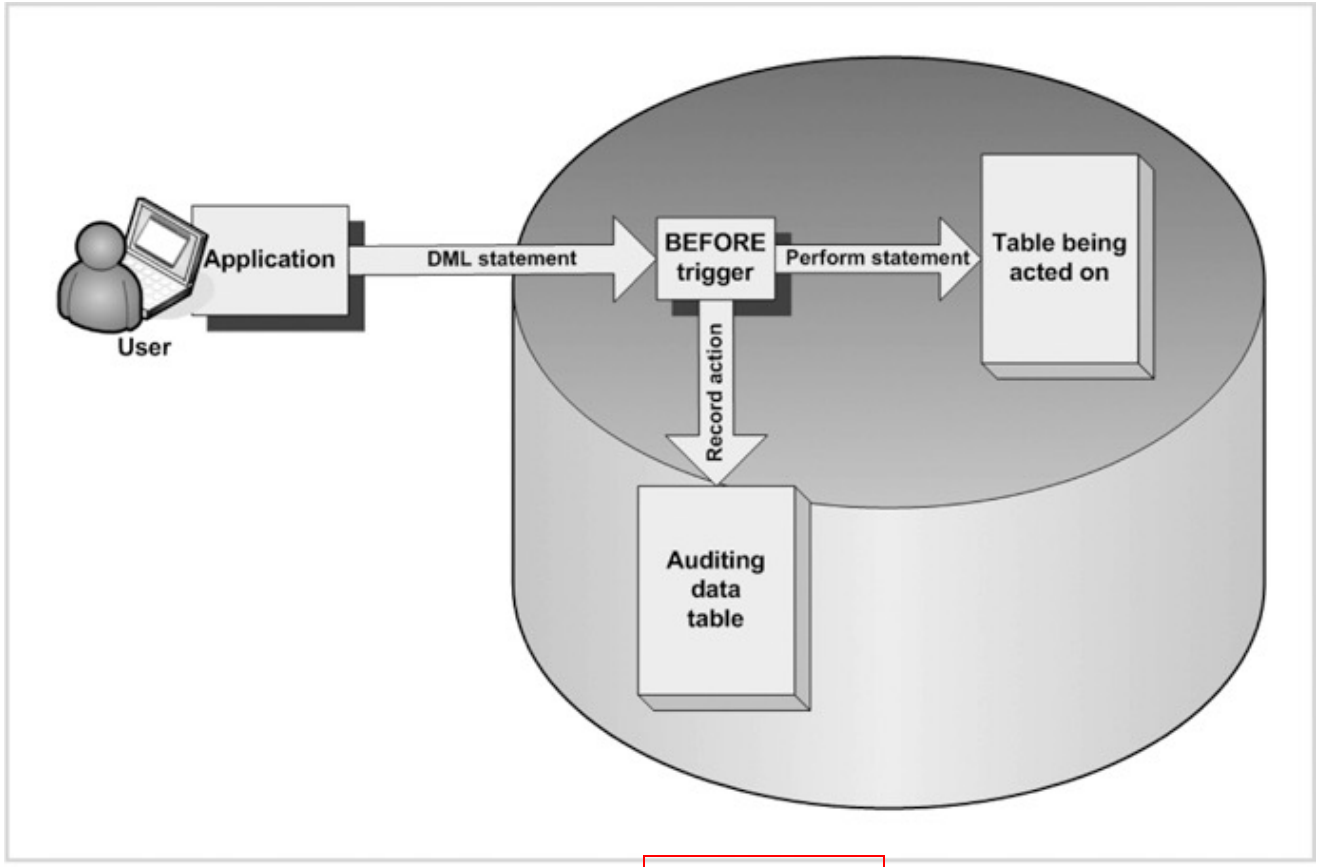

FIGURE 8-1 Auditing architecture for DML action

DML Action Auditing Architecture (continued)

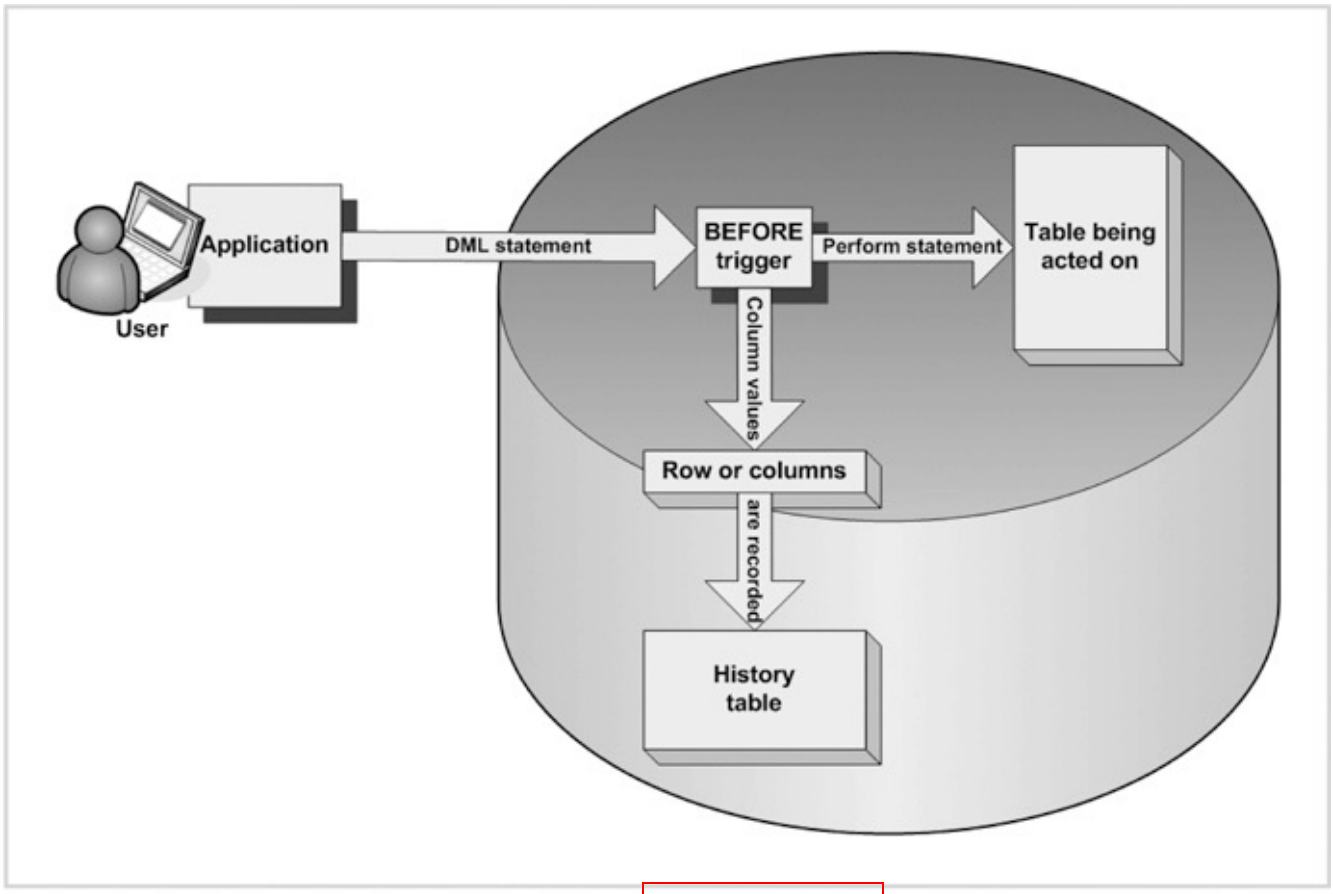

FIGURE 8-2 Auditing architecture for DML changes

Oracle Triggers

- Stored PL/SQL procedure executed whenever:
  - DML operation occurs
  - Specific database event occurs
- Six DML events (trigger timings): INSERT, UPDATE, and DELETE
- Purposes:
  - Audits, controlling invalid data
  - Implementing business rules, generating values

Oracle Triggers (continued)

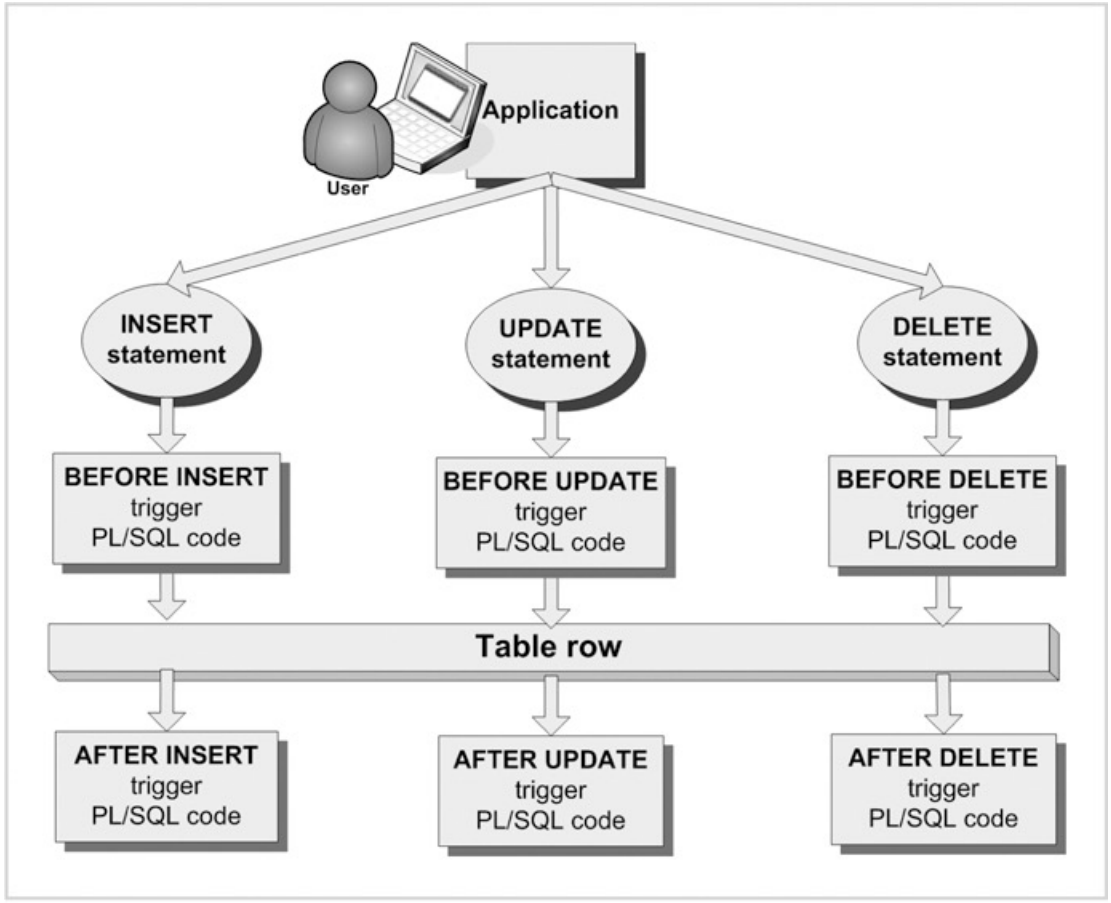

FIGURE 8-3 Trigger timings for DML statements

Oracle Triggers (continued)

- CREATE TRIGGER
- Executed in a specific order:
  - STATEMENT LEVEL triggers before COLUMN LEVEL triggers
  - BEFORE triggers before AFTER triggers
- USER_TRIGGERS data dictionary view: all triggers created on a table
- A table can have unlimited triggers: do not overuse them

Oracle Triggers (continued)

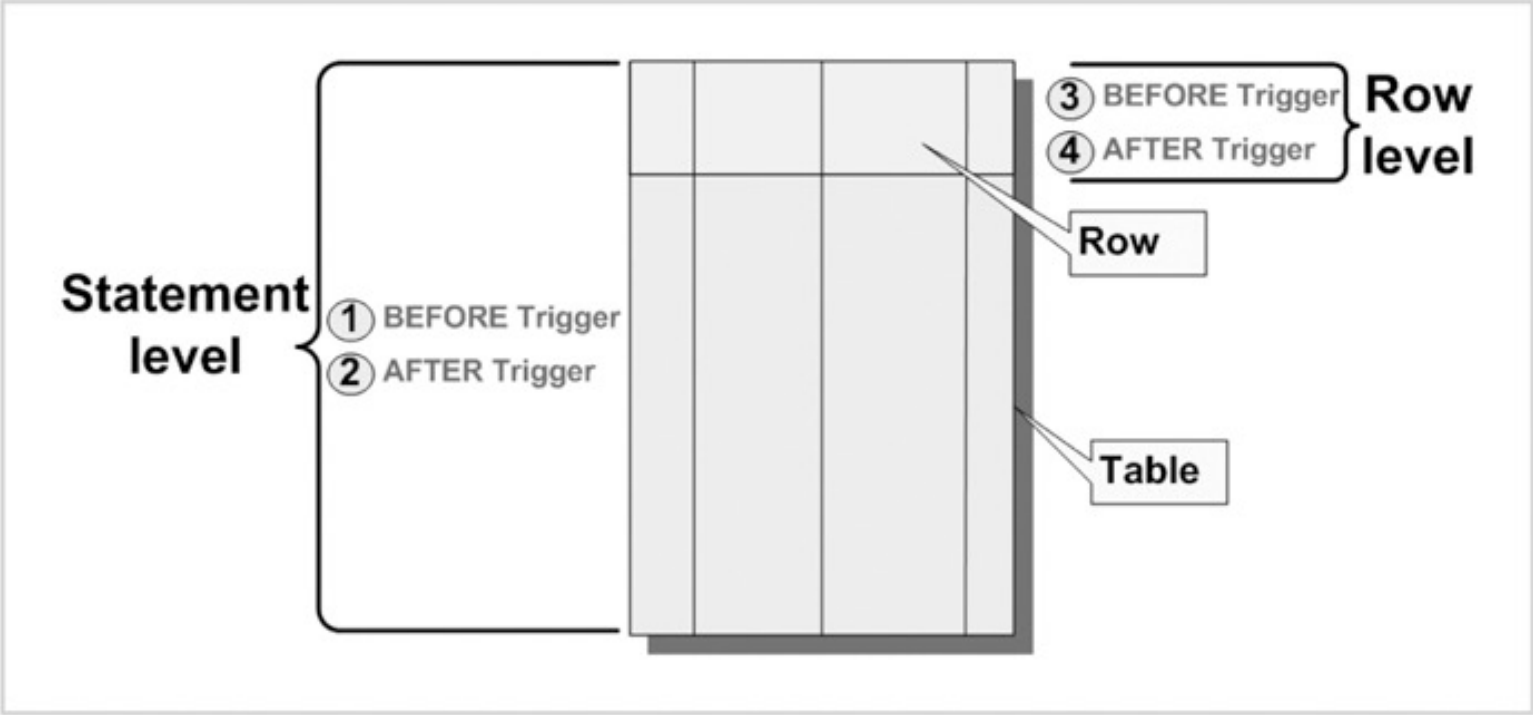

FIGURE 8-4 Order of trigger execution

Fine-grained Auditing (FGA) with Oracle

- Oracle provides column-level auditing: Oracle PL/SQL-supplied package DBMS_FGA
- DBMS_FGA procedures:
  - ADD_POLICY
  - DROP_POLICY
  - DISABLE_POLICY
  - ENABLE_POLICY

Fine-grained Auditing (FGA) with Oracle (continued)

- ADD_POLICY parameters:
  - OBJECT_SCHEMA
  - OBJECT_NAME
  - POLICY_NAME
  - AUDIT_CONDITION
  - AUDIT_COLUMN
  - HANDLER_SCHEMA
  - HANDLER_MODULE
  - ENABLE
  - STATEMENT_TYPES
- DBA_FGA_AUDIT_TRAIL: view the audit trail of the DML activities

DML Action Auditing with Oracle

- Record data changes on the table:
  - Name of the person making the change
  - Date of the change
  - Time of the change
- Before or after value of the columns are not recorded

DML Action Auditing with Oracle (continued)

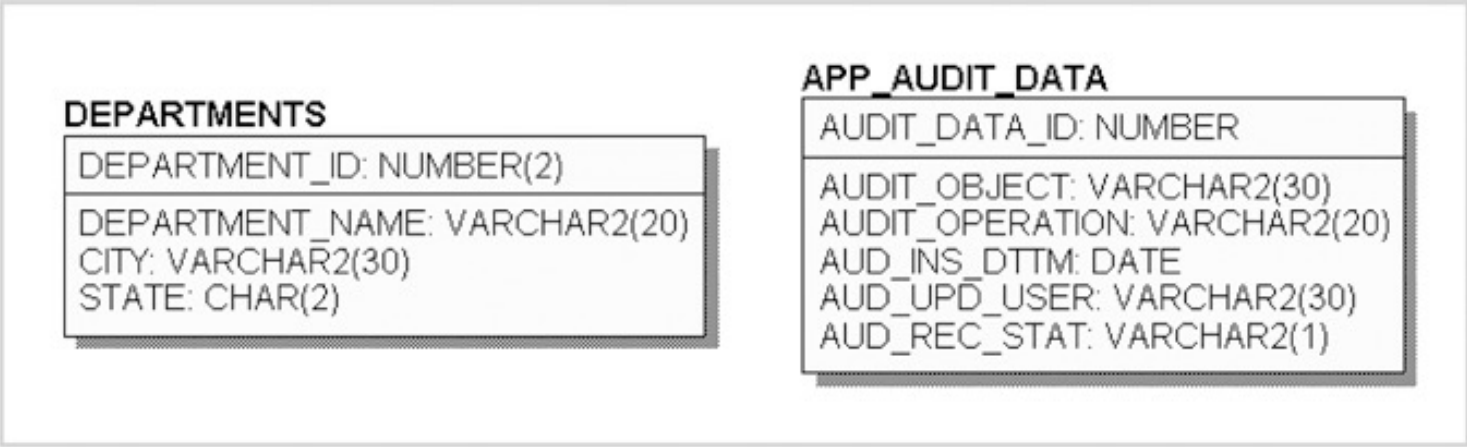

FIGURE 8-6 Auditing data model for the DML statements

DML Action Auditing with Oracle (continued)

- Steps:
  - Use any user other than SYSTEM or SYS; with privileges to create tables, sequences, and triggers
  - Create the auditing table
  - Create a sequence object
  - Create the trigger that will record DML operations
  - Test your implementation

History Auditing Model Implementation Using Oracle

- Historical data auditing is simple to implement; main components are TRIGGER objects and TABLE objects
- Keeps record of:
  - Date and time the copy of the record was captured
  - Type of operation applied to the record

History Auditing Model Implementation Using Oracle (continued)

- Steps:
  - Use any user other than SYSTEM or SYS; with privileges to create tables, sequences, and triggers
  - Create history table
  - Create the trigger to track changes and record all the values of the columns
  - Test your implementation

Project 6: Auditing

- Report your experiences on using fine-grained auditing.
- http://www.oracle.com/technetwork/articles/idm/fga-otn-082646.html

Summary

- Audit examines, verifies and validates documents, procedures, processes
- Auditing environment consists of objectives, procedures, people, and audited entities
- Audit makes sure that the system is working and complies with the policies, standards, regulations, and laws
- Auditing objectives established during development phase

Summary (continued)

- Objectives: compliance, informing, planning, and executing
- Classifications: internal, external, automatic, manual, hybrid
- Models: Simple Auditing 1, Simple Auditing 2, Advanced Auditing, Historical Data, Auditing Applications, C2 Security