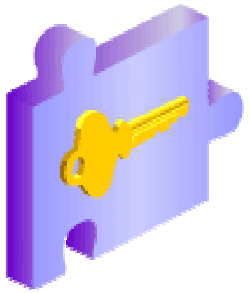
10

Implementing Oracle Database Security

Objectives

After completing this lesson, you should be able to do the following:

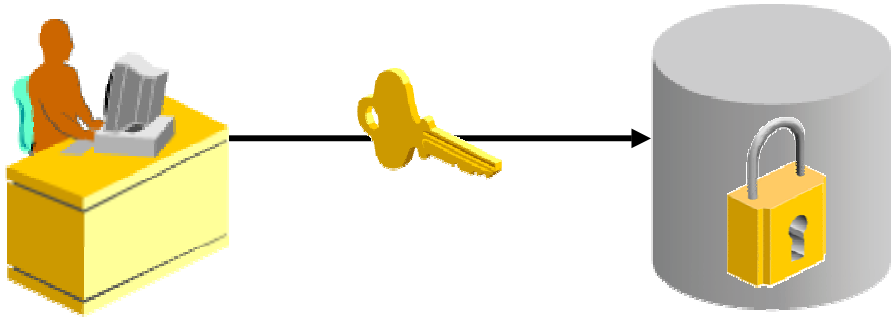
- Describe your DBA responsibilities for security
- Apply the principle of least privilege
- Enable standard database auditing
- Specify audit options
- Review audit information
- Maintain the audit trail



Industry Security Requirements

> Requirements
Least Privilege
Auditing
Value-based
FGA
DBA
Sec. Updates

- **Legal:**
  - **Sarbanes-Oxley Act (SOX)**
  - **Health Information Portability and Accountability Act (HIPAA)**
  - **California Breach Law**
  - **UK Data Protection Act**
- **Auditing**



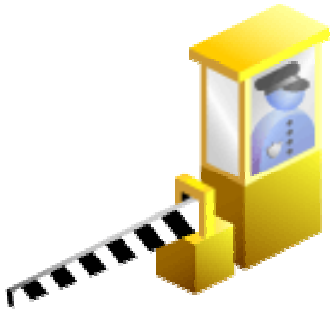
Separation of Responsibilities

- Users with DBA privileges must be trusted. Consider:
  - Abuse of trust
  - That audit trails protect the trusted position
- DBA responsibilities must be shared.
- Accounts must never be shared.
- The DBA and the system administrator must be different people.
- Separate operator and DBA responsibilities.

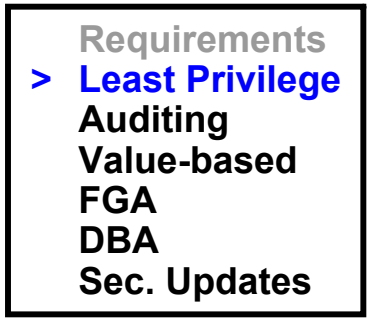
Database Security

A secure system ensures the confidentiality of the data that it contains. There are several aspects of security:

- Restricting access to data and services
- Authenticating users
- Monitoring for suspicious activity



Principle of Least Privilege



- Install only required software on the machine.
- Activate only required services on the machine.
- Give OS and database access to only those users that require access.
- Limit access to the root or administrator account.
- Limit access to the `SYSDBA` and `SYSOPER` accounts.
- Limit users' access to only the database objects required to do their jobs.

Applying the Principle of Least Privilege

- Protect the data dictionary:

```
O7_DICTIONARY_ACCESSIBILITY=FALSE
```

- Revoke unnecessary privileges from `PUBLIC`:

```
REVOKE EXECUTE ON UTL_SMTP, UTL_TCP, UTL_HTTP,
UTL_FILE FROM PUBLIC;
```

- Restrict the directories accessible by users.
- Limit users with administrative privileges.
- Restrict remote database authentication:

```
REMOTE_OS_AUTHENT=FALSE
```

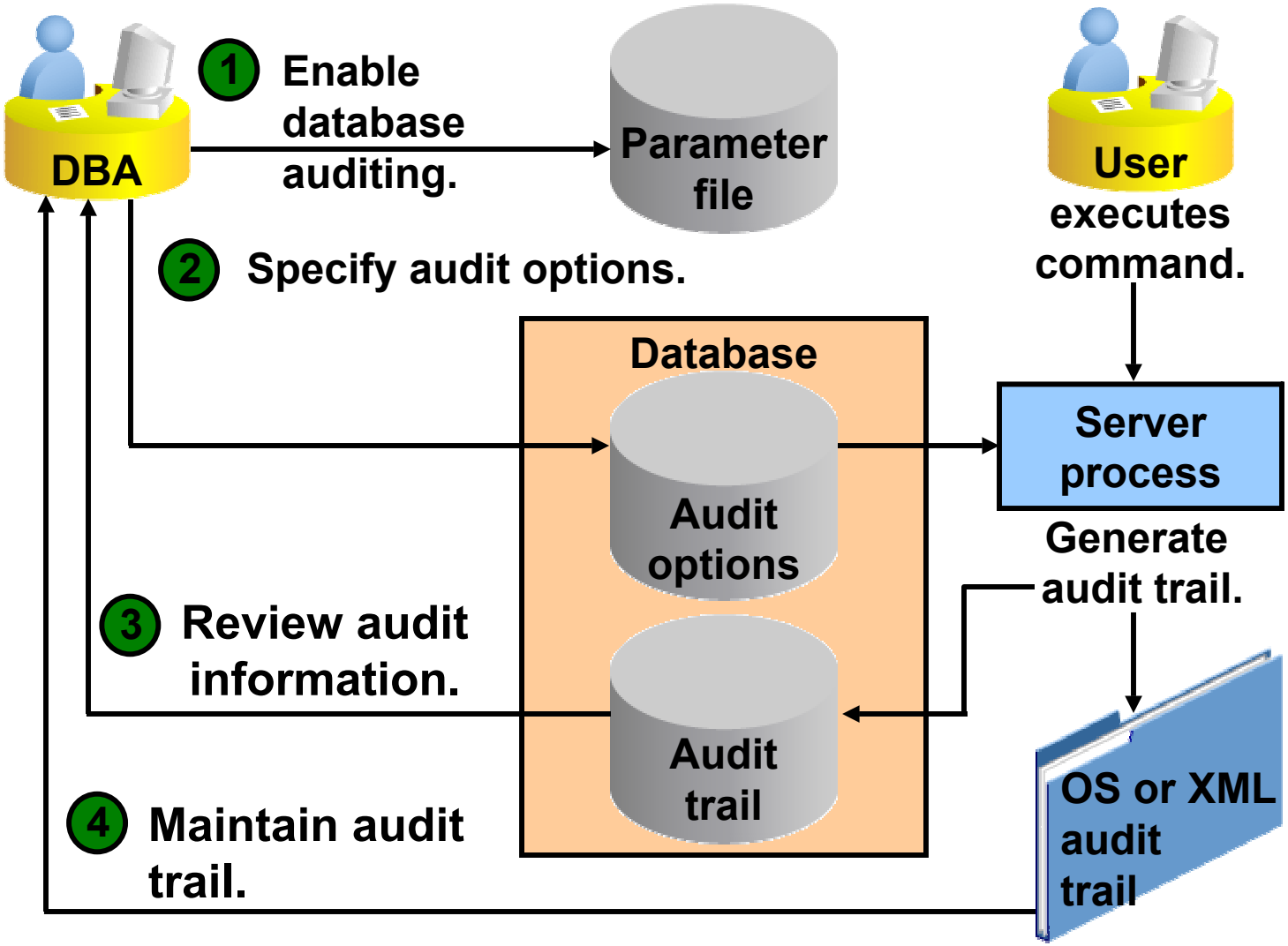
Monitoring for Suspicious Activity

- Requirements
- Least Privilege
- > Auditing
- Value-based
- FGA
- DBA
- Sec. Updates

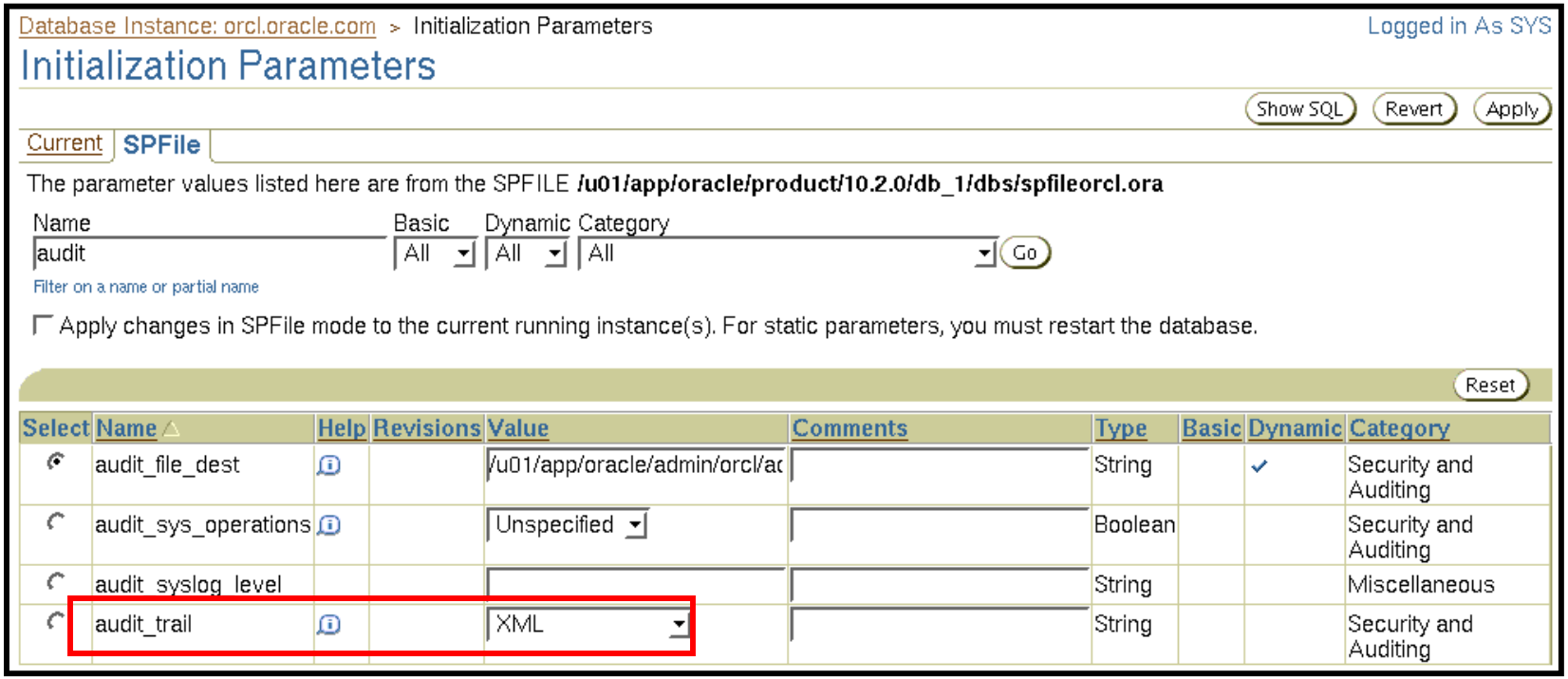
Monitoring or auditing must be an integral part of your security procedures. Review the following:

- Mandatory auditing
- Standard database auditing
- Value-based auditing
- Fine-grained auditing (FGA)
- DBA auditing

Standard Database Auditing



Enabling Auditing

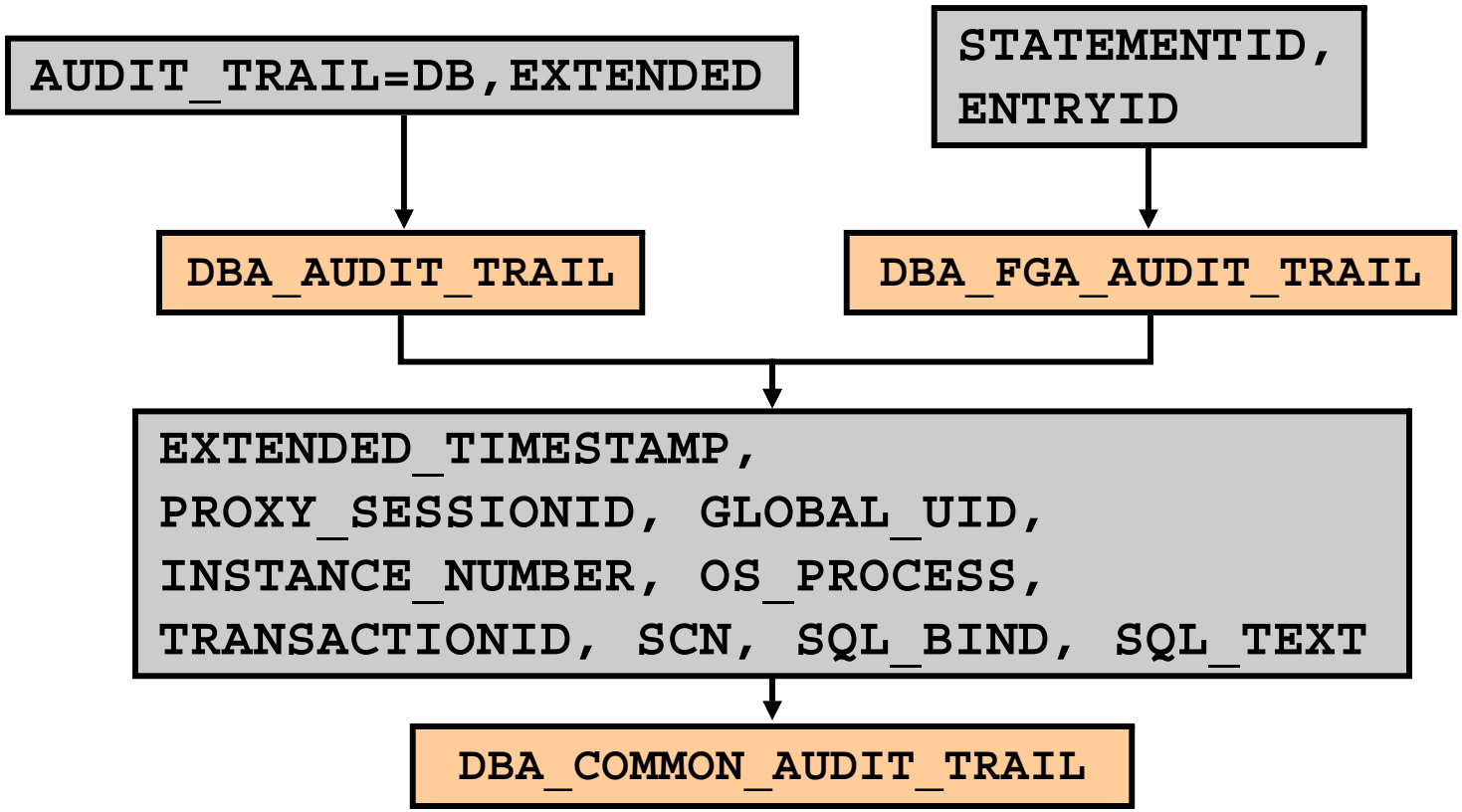



```
ALTER SYSTEM SET audit_trail="XML" SCOPE=SPFILE;
```

Restart database after modifying a static initialization parameter.

Uniform Audit Trails

Use AUDIT_TRAIL to enable database auditing



Enterprise Manager Audit Page

Specifying Audit Options

- **SQL statement auditing:**

```
AUDIT table;
```

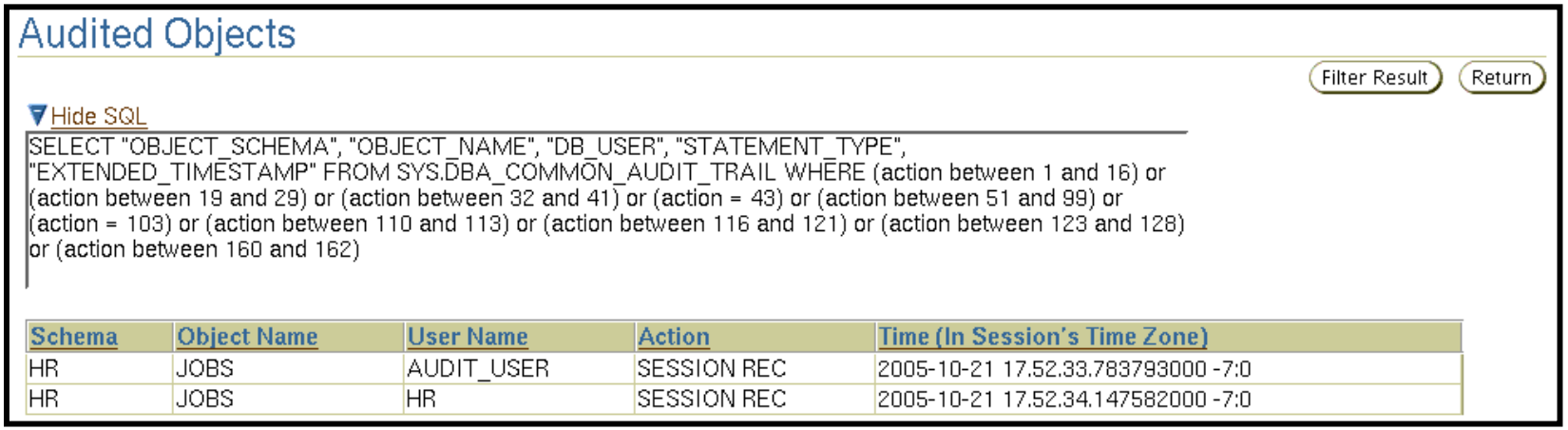
- **System-privilege auditing (nonfocused and focused):**

```
AUDIT select any table, create any trigger;
AUDIT select any table BY hr BY SESSION;
```

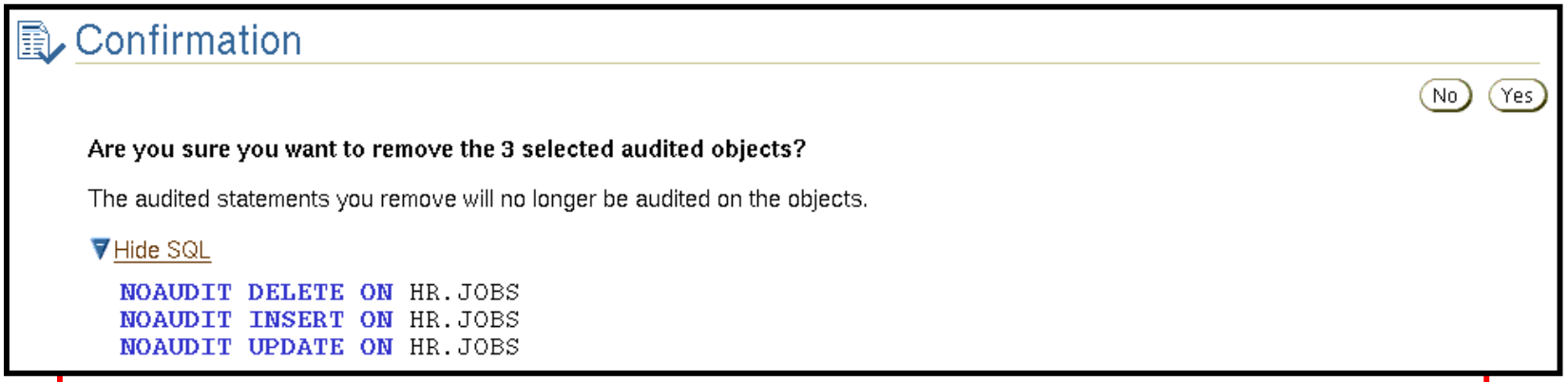
- **Object-privilege auditing (nonfocused and focused):**

```
AUDIT ALL on hr.employees;
AUDIT UPDATE,DELETE on hr.employees BY ACCESS;
```

Using and Maintaining Audit Information



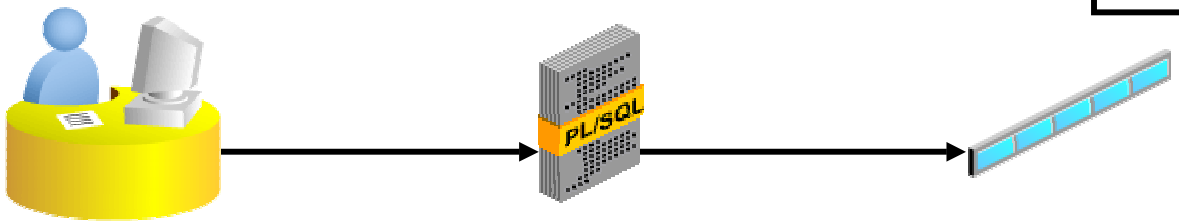
Disable audit options if you are not using them.




```
ALTER SYSTEM SET audit_trail = "NONE" SCOPE=SPFILE
```

Value-Based Auditing

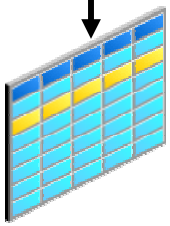
- Requirements
- Least Privilege
- Auditing
- > Value-based
- FGA
- DBA
- Sec. Updates



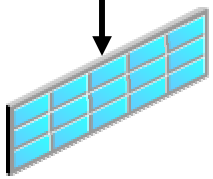
A user makes a change.

Trigger fires.

Audit record is created by the trigger.



User's change is made.



Audit record is inserted into an audit trail table.

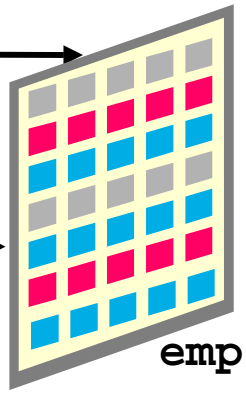
Fine-Grained Auditing

Requirements
Least Privilege
Auditing
Value-based
> FGA
DBA
Sec. Updates

- Monitors data access on the basis of content
- Audits `SELECT`, `INSERT`, `UPDATE`, `DELETE`, and `MERGE`
- Can be linked to a table or view, to one or more columns
- May fire a procedure
- Is administered with the `DBMS_FGA` package

Policy: `AUDIT_EMPS_SALARY`

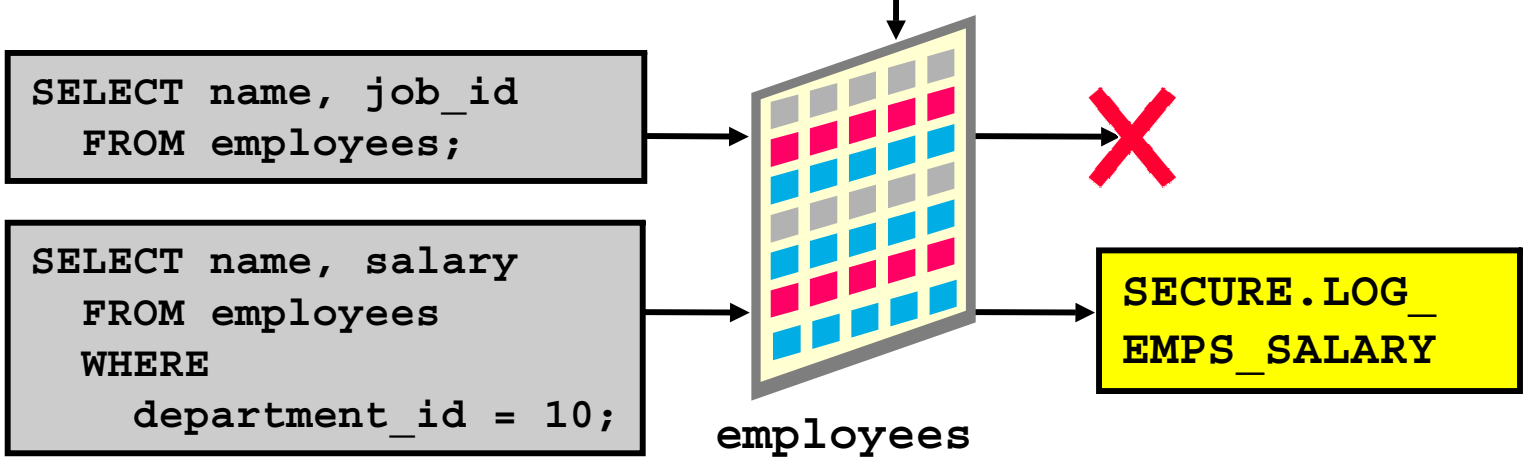
```
SELECT name, salary
  FROM employees
  WHERE
    department_id = 10;
```



FGA Policy

- Defines:
  - Audit criteria
  - Audit action
- Is created with DBMS_FGA .ADD_POLICY

```
dbms_fga.add_policy (
 object_schema   => 'HR',
 object_name     => 'EMPLOYEES',
 policy_name => 'audit_emps_salary',
 audit_condition=>  'department_id=10',
 audit_column    => 'SALARY',
 handler_schema  => 'secure',
 handler_module  => 'log_emps_salary',
 enable          => TRUE,
 statement_types => 'SELECT' );
```



Audited DML Statement: Considerations

- Records are audited if the FGA predicate is satisfied and the relevant columns are referenced.
- `DELETE` statements are audited regardless of any specified columns.
- `MERGE` statements are audited with the underlying `INSERT` or `UPDATE` generated statements.

```
UPDATE hr.employees
SET salary = 10
WHERE department_id = 10;
```

```
UPDATE hr.employees
SET salary = 10
WHERE employee_id = 111;
```

FGA Guidelines

- To audit all statements, use a `null` condition.
- Policy names must be unique.
- The audited table or view must already exist when you create the policy.
- If the audit condition syntax is invalid, an `ORA-28112` error is raised when the audited object is accessed.
- If the audited column does not exist in the table, no rows are audited.
- If the event handler does not exist, no error is returned and the audit record is still created.

DBA Auditing

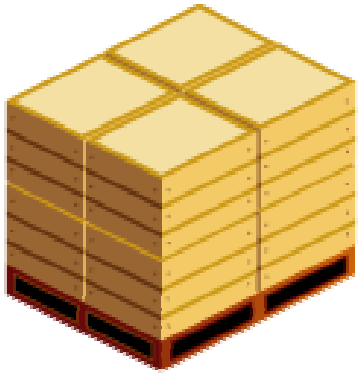
Users with the `SYSDBA` or `SYSOPER` privileges can connect when the database is closed.

- **Audit trail must be stored outside the database.**
- **Connections as `SYSDBA` or `SYSOPER` are always audited.**
- **You can enable additional auditing of `SYSDBA` or `SYSOPER` actions with `audit_sys_operations`.**
- **You can control the audit trail with `audit_file_dest`.**

Maintaining the Audit Trail

The audit trail should be maintained. Follow these best practice guidelines:

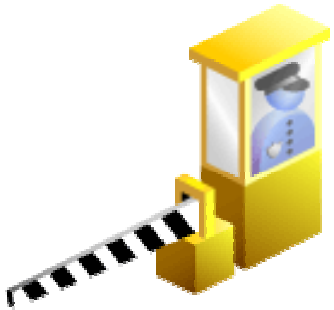
- **Review and store old records.**
- **Prevent storage problems.**
- **Avoid loss of records.**



Security Updates

Requirements
Least Privilege
Auditing
Value-based
FGA
DBA
> Sec. Updates

- Oracle posts security alerts on the Oracle Technology Network Web site at: http://www.oracle.com/technology/deploy/security/alerts.htm
- Oracle database administrators and developers can also subscribe to be notified about critical security alerts via e-mail by clicking the "Subscribe to Security Alerts Here" link.



Applying Security Patches

- Use the Critical Patch Update process.
- Apply all security patches and workarounds.
- Contact the Oracle security products team.

Summary

In this lesson, you should have learned how to:

- Describe your DBA responsibilities for security
- Apply the principle of least privilege
- Enable standard database auditing
- Specify audit options
- Review audit information
- Maintain the audit trail

Practice Overview: Implementing Oracle Database Security

This practice covers the following topics:

- Enabling standard database auditing
- Specifying audit options for the `HR.JOBS` table
- Updating the table
- Reviewing audit information
- Maintaining the audit trail