

Database IS Audit Checklist & Considerations

1. Access Control & User Management

- ☒ Review **user accounts** – ensure no generic/shared accounts (e.g., admin, test, root with default passwords).
- ☒ Verify **least privilege** – check role/privilege assignments against business requirements.
- ☒ Confirm **password policy** – length, complexity, expiry, lockout settings.
- ☒ Check **inactive/dormant users** – disabled or removed after a defined period (e.g., 90 days).
- ☒ Ensure **segregation of duties** – DBA vs. developer vs. application support.

Practical Test:

-- Find users with DBA privileges (Oracle example)
SELECT * FROM dba_role_privs WHERE granted_role = 'DBA';

-- MySQL example
SELECT user, host, authentication_string FROM mysql.user WHERE Super_priv='Y';

2. Database Configuration & Hardening

- ☒ Default accounts removed or disabled (scott/tiger, sa, root).
- ☒ Ensure **remote administrative access** is restricted.
- ☒ Verify **encryption** at rest (TDE, disk-level, file-system) & in transit (TLS/SSL).
- ☒ Disable **unnecessary services/ports** (e.g., Oracle XML DB HTTP, SQL Browser in SQL Server).
- ☒ Harden parameter settings (e.g., disable xp_cmdshell in SQL Server).

Practical Test:

-- SQL Server: check if xp_cmdshell is enabled
EXEC sp_configure 'xp_cmdshell';

3. Authentication & Authorization

- ☒ Integration with **LDAP/AD/SSO** (centralized auth).
 - ☒ Multi-factor authentication (MFA) for DBA/admin accounts.
 - ☒ No use of **hard-coded credentials** in application code/config files.
 - ☒ Database roles aligned with application roles (no excessive permissions).
-

4. Audit & Logging

- ☒ Database auditing enabled (e.g., Oracle Audit Vault, SQL Server Audit, MySQL Audit Plugin).
- ☒ Logs capture failed/successful logins, privilege escalation, schema changes, DML on sensitive tables.
- ☒ Logs are protected (not editable by DBAs without detection).

- ☒ Logs are integrated with **SIEM** or centralized log server.

 Practical Test:

-- SQL Server: check audit specification

```
SELECT * FROM sys.server_audit_specifications;
```

5. Backup & Recovery

- ☒ Regular backups (full, incremental, transaction log).
 - ☒ Backups **encrypted** and stored securely offsite.
 - ☒ Periodic **restore testing** to ensure recovery works.
 - ☒ Backup jobs monitored for failures.
 -  **Audit Consideration:** Verify evidence of **last restore test**.
-

6. Database Patch & Change Management

- ☒ DBMS version supported & updated with security patches.
- ☒ Documented **change management process** for schema updates.
- ☒ Test environment separate from production.
- ☒ Rollback plan exists for failed patches.

 Practical Check:

-- Oracle: check version & patch level

```
SELECT * FROM v$version;
```

7. Data Security & Privacy

- ☒ Data classification – sensitive vs. public data.
- ☒ Masking or encryption of sensitive PII/PCI data.
- ☒ Row-level or column-level security enabled where needed.
- ☒ GDPR/PCI-DSS/Bangladesh Bank compliance (where applicable).

 Practical Example:

-- SQL Server: check column-level encryption

```
SELECT name, is_encrypted FROM sys.columns WHERE is_encrypted = 1;
```

8. High Availability & Performance Monitoring

- ☒ HA/DR setup (Replication, AlwaysOn, RAC, Clustering).
 - ☒ Monitoring of performance issues (slow queries, blocking sessions).
 - ☒ Alerts configured for DB unavailability, space, CPU, memory.
-

9. Incident Response & Forensics

- ☒ Procedures defined for DB breach or suspicious activity.
- ☒ Regular review of privileged user activity reports.
- ☒ Capability to trace queries made by specific accounts (audit trails).

Key Audit Considerations

- **Risk-based auditing** → prioritize databases storing financial, customer, or regulatory data.
- **Sample-based review** → don't just trust documentation, run queries to verify.
- **Compliance mapping** → align with ISO 27001, NIST, PCI DSS, Bangladesh Bank circulars.
- **Practical testing** → auditors should perform **parameter queries, login attempts, and log reviews**.

Database IS Audit Checklist with Practical Examples

1. Access Control & User Management

Audit Objective: Ensure only authorized users exist, least privilege applied, and default accounts removed.

Oracle

-- List all users

```
SELECT username, account_status, created FROM dba_users;
```

-- Check users with DBA role

```
SELECT grantee FROM dba_role_privs WHERE granted_role = 'DBA';
```

MSSQL

-- List SQL logins

```
SELECT name, type_desc, is_disabled FROM sys.server_principals WHERE type IN ('S','U');
```

-- List users with sysadmin role

```
SELECT sp.name AS LoginName
```

```
FROM sys.server_role_members rm
```

```
JOIN sys.server_principals sp ON rm.member_principal_id = sp.principal_id
```

```
WHERE rm.role_principal_id = SUSER_ID('sysadmin');
```

MySQL

-- List all users

```
SELECT user, host, account_locked, password_expired FROM mysql.user;
```

-- List users with SUPER privilege

```
SELECT user, host FROM mysql.user WHERE Super_priv = 'Y';
```

2. Configuration & Hardening

Audit Objective: Verify DB is hardened, unnecessary services disabled, encryption enforced.

Oracle

-- Check if remote OS authentication is disabled (should be FALSE)

```
SHOW PARAMETER remote_os_authent;
```

MSSQL

-- Check if xp_cmdshell is enabled (should be disabled)

```
EXEC sp_configure 'show advanced options', 1; RECONFIGURE;
```

```
EXEC sp_configure 'xp_cmdshell';
```

MySQL

-- Check if symbolic-links are disabled (secure config)

```
SHOW VARIABLES LIKE 'symbolic-links';
```

-- Check SSL/TLS status

```
SHOW VARIABLES LIKE '%ssl%';
```

3. Authentication & Authorization

Audit Objective: Password policy, MFA, and least-privilege roles.

Oracle

-- Password profile details

```
SELECT profile, resource_name, limit FROM dba_profiles WHERE resource_name LIKE 'PASSWORD%';
```

MSSQL

-- Check password policy enforcement

```
SELECT name, is_policy_checked, is_expiration_checked  
FROM sys.sql_logins;
```

MySQL

-- Password expiration policy

```
SHOW VARIABLES LIKE 'default_password_lifetime';
```

4. Audit & Logging

Audit Objective: Ensure login attempts, privilege use, schema changes are logged.

Oracle

-- Check if auditing is enabled

```
SHOW PARAMETER audit_trail;
```

-- Review audit records

```
SELECT username, action_name, timestamp FROM dba_audit_trail;
```

MSSQL

-- Check server audits

```
SELECT * FROM sys.server_audits;
```

-- Failed login attempts (from default error log)

```
EXEC xp_readerrorlog 0, 1, 'Login failed';
```

MySQL

-- Check if audit log plugin is enabled

```
SHOW VARIABLES LIKE 'audit_log%';
```

-- Query audit logs (if enabled)

```
SELECT * FROM mysql.audit_log;
```

5. Backup & Recovery

Audit Objective: Ensure secure, regular, tested backups.

Oracle

-- Last RMAN backup

```
LIST BACKUP SUMMARY;
```

MSSQL

```
-- Last database backup date
SELECT d.name, MAX(b.backup_finish_date) AS LastBackup
FROM sys.databases d
LEFT JOIN msdb.dbo.backupset b ON d.name = b.database_name
GROUP BY d.name;
```

MySQL

(MySQL doesn't store backup metadata natively; check scripts/logs used for mysqldump or xtrabackup.)

6. Patch & Change Management

Audit Objective: Verify database is patched and supported.

Oracle

```
-- DB version and patch level
SELECT * FROM v$version;
```

MSSQL

```
-- SQL Server version
SELECT @@VERSION;
```

MySQL

```
-- MySQL version
SELECT VERSION();
```

7. Data Security & Privacy

Audit Objective: Sensitive data encrypted/masked.

Oracle

```
-- Check if column encryption is used
SELECT table_name, column_name, encryption_alg
FROM dba_encrypted_columns;
```

MSSQL

```
-- Columns with Always Encrypted
SELECT name, is_encrypted FROM sys.columns WHERE is_encrypted = 1;
```

MySQL

```
-- Check if tablespaces are encrypted
SELECT tablespace_name, encryption FROM information_schema.tablespaces;
```

8. High Availability & Monitoring

Audit Objective: Ensure HA/DR mechanisms are active.

Oracle

-- Check Data Guard / Standby databases

```
SELECT db_unique_name, open_mode, database_role FROM v$database;
```

MSSQL

-- Availability groups status

```
SELECT ag.name, ar.replica_server_name, ar.state_desc
```

```
FROM sys.availability_groups ag
```

```
JOIN sys.availability_replicas ar ON ag.group_id = ar.group_id;
```

MySQL

-- Replication status

```
SHOW SLAVE STATUS\G;
```

9. Incident Response & Forensics

Audit Objective: Ensure evidence collection and investigation capabilities.

Oracle

-- Audit privileged user sessions

```
SELECT username, action_name, returncode FROM dba_audit_trail WHERE priv_used IS NOT NULL;
```

MSSQL

-- Recent logins by sysadmin accounts

```
SELECT login_name, host_name, program_name, login_time
```

```
FROM sys.dm_exec_sessions
```

```
WHERE is_user_process = 1;
```

MySQL

-- General log (must be enabled)

```
SHOW VARIABLES LIKE 'general_log';
```

```
SELECT * FROM mysql.general_log ORDER BY event_time DESC LIMIT 10;
```

☒ Auditor Considerations Across All DBMS:

- Cross-check **policy vs. practice** (docs vs. queries).
- Pay attention to **default settings** (often insecure).
- Ensure **integration with SIEM** for centralized monitoring.
- Validate **restore testing** – not just backup existence.