TEMPLATE

Oracle Database Vulnerability Assessment and Hardening Template

A practical assessment and hardening template for Oracle Database teams to identify exposure, prioritize findings, and validate controls before production rollout.

Oracle Database Vulnerability Assessment and Hardening Template

Purpose

Use this template to assess Oracle Database exposure, privilege risk, audit coverage, and hardening readiness in a way that supports production operations.

How to use this template

- Complete the assessment sections for each database or environment.
- Record evidence, not assumptions.
- Rank issues by exploitability and business impact.
- Apply changes in a controlled test window.
- Revalidate and document exceptions before closing the review.

---

1) Environment overview

Field	Value
Database name	
Hostname / instance	
Environment	? Dev ? Test ? Staging ? Production
Owner team	
Business criticality	? Low ? Medium ? High ? Critical
Data sensitivity	? Public ? Internal ? Confidential ? Restricted
Review date	
Reviewer	
Change window available	? Yes ? No

---

2) Scope and dependencies

In scope

- Oracle Database instance(s):

-

- Listener(s) / endpoints:

-

- Application connections:

-

- Reporting or batch jobs:

-

- Replication / standby / backup dependencies:

-

Known dependencies that must not break

- - -

Notes on operational constraints

- Maintenance window:
- Rollback requirements:
- Vendor-supported limitations:
- Legacy components that must remain enabled:

---

3) Exposure inventory

Item	Status	Evidence / notes
Supported release in use	? Yes ? No	
Patch level acceptable by policy	? Yes ? No	
Listener restricted to trusted networks	? Yes ? No	

Unnecessary ports closed | ? Yes ? No |
Alternate access paths reviewed | ? Yes ? No |
Management interfaces restricted | ? Yes ? No |
Unused services identified | ? Yes ? No |
Optional features reviewed | ? Yes ? No |

Exposure observations

- - -

---

4) Authentication and account posture

Control | Status | Evidence / notes
Password policy aligned to standard | ? Yes ? No |
Account lockout behavior configured | ? Yes ? No |
Stale accounts reviewed | ? Yes ? No |
Shared credentials eliminated or justified | ? Yes ? No |
Remote access rules reviewed | ? Yes ? No |
Privileged accounts separately managed | ? Yes ? No |

Findings

- Accounts with unexplained access:

-

- Accounts requiring review or removal:

-

- Exceptions approved:

-

---

5) Privilege and role review

Check for the following conditions

- Broad system privileges assigned to application accounts
- Direct privilege grants that should be role-based
- Excessive object ownership where a dedicated schema is safer
- Roles with more access than required for routine operations
- Privileged accounts used for non-administrative tasks
- Administrative accounts shared across multiple operators

Privilege review table

Account / role	Required?	Risk level	Evidence	Action
	? Yes ? No	? Low ? Med ? High		
	? Yes ? No	? Low ? Med ? High		
	? Yes ? No	? Low ? Med ? High		

Recommended actions

- Remove unnecessary grants.
- Separate application ownership from administrative access.
- Replace shared credentials with named accounts where possible.
- Document compensating controls when privileges cannot be reduced.

---

6) Audit and evidence coverage

Audit area	Status	Evidence / notes
Administrative actions captured	? Yes ? No	
Role changes captured	? Yes ? No	
Privilege use captured	? Yes ? No	
Authentication events captured	? Yes ? No	
Session / client context available	? Yes ? No	
Logs retained per policy	? Yes ? No	
Alerts routed to monitoring / SIEM	? Yes ? No	

Evidence gaps

- - -

Validation question

Can you reconstruct who changed security settings, who used elevated privileges, and from which session or client context?

- ? Yes
- ? No
- Notes:

---

7) Feature and service sprawl review

Item	Status	Notes
Unused services disabled	? Yes ? No	
Optional components reviewed	? Yes ? No	
Legacy access methods reviewed	? Yes ? No	
Unneeded interfaces removed	? Yes ? No	
Nonessential packages or jobs reviewed	? Yes ? No	

Findings

- - -

---

8) Data and object protection

Control	Status	Evidence / notes
Sensitive tables and columns protected	? Yes ? No	

Backup access restricted | ? Yes ? No |
Export paths controlled | ? Yes ? No |
Dump files secured | ? Yes ? No |
Staging directories protected | ? Yes ? No |
Nonproduction copies sanitized | ? Yes ? No |

Notes

- - -

---

9) Hardening actions checklist

Network

- [ ] Restrict listener exposure to trusted client networks and application tiers
- [ ] Close unnecessary ports and endpoints
- [ ] Verify management interfaces are not reachable from untrusted segments

Authentication and access

- [ ] Enforce password and lockout controls consistent with policy
- [ ] Remove stale or unused accounts
- [ ] Eliminate shared credentials where possible
- [ ] Use least privilege for application and service accounts

Configuration and services

- [ ] Disable unused services and optional features after validation
- [ ] Review legacy access paths and remove them when no longer needed
- [ ] Confirm changes do not affect scheduled jobs or replication

Auditing and detection

- [ ] Capture administrative actions
- [ ] Capture role and privilege changes
- [ ] Capture elevated privilege use
- [ ] Confirm log retention and alert routing

Backups and exports

- [ ] Restrict access to backups and dump files
- [ ] Secure staging and export locations
- [ ] Verify nonproduction data handling requirements

---

10) Risk ranking

Use this scale to prioritize remediation:

- High: reachable and likely exploitable, with significant business impact
- Medium: reachable or risky, but dependent on additional conditions
- Low: limited reachability or low impact, can be scheduled later

Finding	Reachable?	Exploitable?	Business impact	Priority	Target date
	? Yes ? No	? Yes ? No	? Low ? Med ? High	? Low ? Med ? High	
	? Yes ? No	? Yes ? No	? Low ? Med ? High	? Low ? Med ? High	
	? Yes ? No	? Yes ? No	? Low ? Med ? High	? Low ? Med ? High	

---

11) Change plan and validation

Planned changes

Change	Owner	Window	Rollback point	Status
			? Planned ? In progress ? Done	
			? Planned ? In progress ? Done	
			? Planned ? In progress ? Done	

Validation steps after change

- [ ] Confirm application connectivity
- [ ] Confirm reporting and batch jobs complete successfully
- [ ] Confirm audit events are generated as expected
- [ ] Confirm restricted services and endpoints are no longer reachable
- [ ] Confirm exception handling and rollback points are documented

Validation evidence

- - -

---

12) Exceptions register

Exception	Reason	Compensating control	Approver	Review date

---

13) Final readiness decision

Overall status

- ? Ready for production use
- ? Ready with exceptions
- ? Not ready

Summary of material risks

- - -

Summary of completed hardening

- - -

Sign-off

Name	Role	Signature / approval	Date

Quick assessment prompts

Use these questions to sanity-check the result:

- What is exposed that does not need to be reachable?
- What can be exploited with the current configuration?
- Which changes are safe to apply before production rollout?
- Can you prove who used elevated privileges and when?
- Have backups, exports, and staging paths been protected?
- Are any controls dependent on undocumented legacy behavior?

Suggested companion topics

- Oracle Database auditing and unified audit policy design
- Privilege escalation detection and alerting
- Secure handling of backups, exports, and staging data
- Change validation for database hardening in production environments

---

Notes

This template is intentionally vendor-neutral in process and evidence style, while remaining practical for Oracle Database operational reviews. Adapt the checklist items to your version, deployment model, and application dependencies.