CYBERSIGMA · CERT-In EMPANELLED · PCI QSA AUTHORISED

Database Security Hardening Checklist

Vendor-neutral database security configuration review — Oracle, SQL Server, MySQL/MariaDB, PostgreSQL & MongoDB.

About this checklist

This is the working paper our CERT-In empanelled auditors use to review database builds. It covers 42 controls across ten domains — governance, identity, privilege, network exposure, encryption, patching, secure configuration, auditing, backup and data protection — each with a test method, the evidence to collect, the risk if it fails and remediation guidance, mapped to CIS, NIST CSF 2.0, ISO/IEC 27001:2022 and PCI DSS v4.0.1. The control questions are vendor-neutral; a dedicated OEM Command Reference gives the exact query or console path for Oracle, SQL Server, MySQL/MariaDB, PostgreSQL and MongoDB.

41 controls · 10 domains

Frameworks: PCI DSS v4.0.1 | ISO/IEC 27001:2022 | NIST CSF 2.0 | CIS Benchmarks & Controls v8.1 | UAE IA / KSA ECC | CERT-In

Platforms: Oracle Database · Microsoft SQL Server · MySQL / MariaDB · PostgreSQL · MongoDB

Scoring: Pass = 100, Partial = 50, Fail = 0, Not Applicable excluded. Control wording and framework mappings are practical audit mappings authored by CyberSigma; use current licensed standards for formal control text.

Governance, Inventory & Baseline

DB-GOV-01 High

Is every in-scope database instance captured in an approved inventory with owner, environment, version and data classification?

Test: Reconcile the CMDB against directory/host discovery, cloud consoles and DB listener/port scans; sample for coverage.
Evidence: Database inventory with owner, environment, engine, version, classification.
Risk if failed: Unknown/shadow databases hold sensitive data outside monitoring, patching and backup.
NIST ID.AM-1; ID.AM-2 · ISO A.5.9; A.8.9 · CIS CIS 1.1; 2.1 · PCI 2.4; 12.5.1

DB-GOV-02 High

Is there a documented, version-specific database hardening standard, and is each instance built to it with exceptions tracked?

Test: Review the hardening standard; compare a sample of instances; check the exception register.
Evidence: Hardening standard, build records, exception register.
Risk if failed: Inconsistent, ad-hoc builds leave exploitable misconfigurations.
NIST PR.PS-1; GV.PO · ISO A.8.9 · CIS CIS 4.1; 4.2 · PCI 2.2

DB-GOV-03 High

Are production, test and development databases segregated, with no production data in non-production without protection?

Test: Confirm environment separation; check for cloned production data in test/dev and its masking status.
Evidence: Environment topology, data-refresh/masking procedure.
Risk if failed: Unmasked production data in weakly-controlled environments causes breaches.
NIST PR.AA-5; PR.DS · ISO A.8.31; A.8.11 · CIS CIS 3.12 · PCI 6.5.3

DB-GOV-04 Medium

Are third-party/managed database services (DBaaS) covered by the same hardening, monitoring and shared-responsibility understanding?

Test: Review DBaaS configuration, provider shared-responsibility mapping and monitoring coverage.
Evidence: DBaaS configuration and responsibility matrix.
Risk if failed: Assumed provider coverage leaves customer-side controls (access, encryption, logging) unaddressed.
NIST GV.SC; ID.AM · ISO A.5.19; A.5.23 · CIS CIS 15.1 · PCI 12.8; 2.2

Identity & Authentication

DB-IAM-01 Critical

Have all default, sample and demo accounts been removed or disabled and their default passwords changed?

Test: Enumerate accounts; check for vendor defaults and sample schemas; test default credentials.
Evidence: Account list, default-account remediation record.
Risk if failed: Default credentials are the first thing an attacker tries.
NIST PR.AA-1 · ISO A.8.5 · CIS CIS 4.7; 5.2 · PCI 2.2.2; 8.3.5

DB-IAM-02 Medium

Is authentication integrated with the enterprise directory (Kerberos/LDAP/IAM) rather than relying only on local DB accounts?

Test: Review authentication configuration and the proportion of local vs federated accounts.
Evidence: Auth configuration, directory integration evidence.
Risk if failed: Local-only accounts bypass central lifecycle, MFA and disablement.
NIST PR.AA-1; PR.AA-2 · ISO A.5.16; A.8.5 · CIS CIS 6.7 · PCI 8.3

DB-IAM-03 High

Is a strong password/credential policy enforced (length, complexity, lockout, rotation) for all database accounts?

Test: Inspect password profiles/policies and account lockout settings.
Evidence: Password policy configuration.
Risk if failed: Weak credentials enable brute-force and credential-stuffing.
NIST PR.AA-1 · ISO A.5.17 · CIS CIS 5.2 · PCI 8.3.6; 8.3.4

DB-IAM-04 High

Do application connections use dedicated service accounts with least privilege and securely stored, rotated credentials?

Test: Review app connection accounts, their grants and how secrets are stored (vault vs config file).
Evidence: Service-account list, secrets-management evidence.
Risk if failed: Shared/over-privileged app accounts with hard-coded secrets enable lateral movement.
NIST PR.AA-1; PR.AA-5 · ISO A.8.2; A.8.5 · CIS CIS 5.4; 6.8 · PCI 8.6.1; 8.6.2

DB-IAM-05 High

Is MFA enforced for administrative and remote/interactive access to database management interfaces?

Test: Test admin login paths and bastion/jump-host access for MFA enforcement.
Evidence: MFA configuration for DBA access.
Risk if failed: Single-factor DBA access is a high-value takeover target.
NIST PR.AA-2 · ISO A.8.5 · CIS CIS 6.3; 6.4 · PCI 8.4; 8.5

DB-IAM-06 Medium

Are dormant, orphaned and leaver database accounts detected and disabled promptly?

Test: Review last-login data and the joiner/mover/leaver process for DB accounts.
Evidence: Dormant-account report, deprovisioning evidence.
Risk if failed: Stale accounts are an easy, low-noise foothold.
NIST PR.AA-1 · ISO A.5.18 · CIS CIS 5.3 · PCI 8.2.6

Privilege & Access Control

DB-PRV-01 Critical

Is least privilege enforced — are broad system privileges (DBA, SYSADMIN, superuser, PUBLIC grants) restricted and justified?

Test: List holders of admin roles and PUBLIC/ANY privileges; validate business justification.
Evidence: Privilege report, role membership, justification.
Risk if failed: Excess privilege turns any account compromise into full database compromise.
NIST PR.AA-5 · ISO A.8.2; A.8.3 · CIS CIS 6.8; 3.3 · PCI 7.2; 7.3

DB-PRV-02 Medium

Are database privileges assigned through roles and reviewed periodically (access recertification)?

Test: Review role design and evidence of periodic access reviews.
Evidence: Role model, last access-review record.
Risk if failed: Privilege creep leaves users with access they no longer need.
NIST PR.AA-5; GV.RR · ISO A.5.18 · CIS CIS 6.1; 6.2 · PCI 7.2.4

DB-PRV-03 High

Are DBA and privileged activities performed via named individual accounts (no shared admin logins)?

Test: Check for shared admin accounts; confirm named-account use and accountability.
Evidence: Admin account list, session attribution evidence.
Risk if failed: Shared admin accounts destroy accountability and audit trails.
NIST PR.AA-1 · ISO A.5.16 · CIS CIS 5.4 · PCI 8.2.1

DB-PRV-04 Medium

Is direct interactive access to production data restricted, with break-glass access logged and time-bound?

Test: Review who can query production directly; check break-glass process and logging.
Evidence: Access matrix, break-glass procedure and logs.
Risk if failed: Unfettered production access enables data theft and unaudited change.
NIST PR.AA-5 · ISO A.8.2; A.8.18 · CIS CIS 6.8 · PCI 7.2; 10.2

Network Exposure & Segmentation

DB-NET-01 Critical

Is the database reachable only from authorised application/admin networks and not exposed to the internet?

Test: Scan the DB port from external and untrusted internal ranges; review firewall/security-group rules.
Evidence: Port scan results, firewall/SG rules.
Risk if failed: Internet-exposed databases are routinely discovered and breached.
NIST PR.IR-1; PR.AA-5 · ISO A.8.20; A.8.22 · CIS CIS 4.4; 12.2 · PCI 1.3; 1.4

DB-NET-02 High

Are all client-to-database and replication connections encrypted in transit (TLS) with strong protocols and ciphers?

Test: Confirm TLS is required; test for cleartext fallback; check protocol/cipher configuration.
Evidence: TLS configuration, connection capture / cipher scan.
Risk if failed: Cleartext connections expose credentials and data to sniffing.
NIST PR.DS-2 · ISO A.8.24 · CIS CIS 3.10 · PCI 4.2.1

DB-NET-03 Low

Are the database listener/management ports changed from well-known defaults where feasible and access rate-limited?

Test: Check listener/port configuration and any connection throttling.
Evidence: Listener configuration.
Risk if failed: Default ports ease automated discovery and attack.
NIST PR.IR-1 · ISO A.8.20 · CIS CIS 4.6 · PCI 1.4

DB-NET-04 Medium

Are administrative/management connections restricted to a hardened bastion or management network, not direct from user LAN?

Test: Review admin access paths and jump-host enforcement.
Evidence: Admin access architecture.
Risk if failed: Direct admin access from user networks widens the attack path.
NIST PR.AA-5; PR.IR-1 · ISO A.8.20; A.8.5 · CIS CIS 12.7; 6.3 · PCI 1.3; 8.5

Encryption & Key Management

DB-CRY-01 High

Is sensitive data encrypted at rest (TDE / tablespace / column / filesystem encryption) per data classification?

Test: Confirm encryption-at-rest is enabled for in-scope data stores and backups.
Evidence: Encryption configuration, key inventory.
Risk if failed: Stolen disks, snapshots or backups expose data if unencrypted.
NIST PR.DS-1 · ISO A.8.24 · CIS CIS 3.11 · PCI 3.5.1

DB-CRY-02 High

Are encryption keys managed securely (HSM/KMS), separated from data, rotated and access-controlled?

Test: Review key storage, custodianship, rotation schedule and access.
Evidence: Key-management procedure, KMS/HSM configuration.
Risk if failed: Keys stored with data or unrotated defeat encryption.
NIST PR.DS-1; PR.AA-5 · ISO A.8.24 · CIS CIS 3.11 · PCI 3.6; 3.7

DB-CRY-03 Medium

Are particularly sensitive fields (PAN, secrets, credentials) protected by column-level encryption, tokenisation or hashing?

Test: Identify sensitive columns and confirm field-level protection.
Evidence: Data map, field-protection configuration.
Risk if failed: Sensitive fields readable by anyone with table access.
NIST PR.DS-1 · ISO A.8.11 · CIS CIS 3.11 · PCI 3.5.1; 3.4

Patch & Vulnerability Management

DB-PAT-01 Critical

Is the database engine on a supported version and patched to current security levels within a defined SLA?

Test: Check version/patch level against vendor releases and EOL dates; review patch SLA compliance.
Evidence: Version/patch report, patch SLA.
Risk if failed: Unpatched/EOL databases carry known, exploitable vulnerabilities.
NIST ID.RA-1; PR.PS-2 · ISO A.8.8 · CIS CIS 7.3; 7.4 · PCI 6.3.1; 6.3.3

DB-PAT-02 Medium

Are databases included in authenticated vulnerability scanning and configuration assessment?

Test: Review scan scope and recent authenticated DB scan / config-assessment results.
Evidence: Scan reports, remediation tracking.
Risk if failed: Misconfigurations and missing patches go undetected.
NIST ID.RA-1; DE.CM-8 · ISO A.8.8 · CIS CIS 7.5; 7.6 · PCI 11.3.1

Secure Configuration & Attack Surface

DB-CFG-01 High

Have unnecessary features, packages, procedures and sample databases been removed or disabled (attack-surface reduction)?

Test: Review enabled features/extensions; check for risky procedures and sample databases.
Evidence: Feature/extension inventory.
Risk if failed: Unneeded features (e.g. command execution, external routines) expand attack surface.
NIST PR.PS-1 · ISO A.8.9 · CIS CIS 4.8 · PCI 2.2.4

DB-CFG-02 High

Are risky capabilities that allow OS/command execution or arbitrary file access restricted (e.g. xp_cmdshell, external tables, UDFs)?

Test: Check configuration flags governing OS interaction and external access.
Evidence: Configuration of OS-interaction features.
Risk if failed: Such features enable OS compromise from within the database.
NIST PR.PS-1 · ISO A.8.9 · CIS CIS 4.8 · PCI 2.2.4

DB-CFG-03 Medium

Does the database service run under a dedicated least-privilege OS account (not root/Administrator/LocalSystem)?

Test: Check the OS account the DB process runs as and its privileges.
Evidence: Service-account configuration.
Risk if failed: A DB compromise inherits excessive OS privilege.
NIST PR.AA-5; PR.PS-1 · ISO A.8.2 · CIS CIS 4.8 · PCI 2.2.1

DB-CFG-04 Medium

Are file-system permissions on data files, configuration, and key/credential files restricted to the DB service account?

Test: Inspect permissions on data directories, config and key files.
Evidence: File permission listing.
Risk if failed: Loose permissions allow local users to read or tamper with data/keys.
NIST PR.AA-5 · ISO A.8.3 · CIS CIS 3.3 · PCI 3.5.1

DB-CFG-05 Low

Are error messages and metadata prevented from leaking sensitive detail to applications/clients?

Test: Review verbose-error settings and access to system catalogs.
Evidence: Error-handling configuration.
Risk if failed: Verbose errors aid SQL injection and reconnaissance.
NIST PR.PS-1 · ISO A.8.9 · CIS CIS 16.11 · PCI 6.2.4

DB-CFG-06 Medium

Are secure configuration parameters set (resource limits, timeouts, host-based access rules, trusted-connection settings)?

Test: Review key configuration parameters against the hardening baseline.
Evidence: Configuration export vs baseline.
Risk if failed: Insecure defaults enable DoS, trust-relationship abuse and weak auth.
NIST PR.PS-1 · ISO A.8.9 · CIS CIS 4.1 · PCI 2.2

DB-CFG-07 High

Is the database protected against SQL injection at the application boundary (parameterised queries, least-privilege app accounts, input validation)?

Test: Review app data-access patterns and account privileges; corroborate with recent app pen-test findings.
Evidence: Code review / pen-test evidence, app account grants.
Risk if failed: SQL injection remains a leading cause of database breaches.
NIST PR.PS-1 · ISO A.8.28 · CIS CIS 16.11 · PCI 6.2.4

Auditing, Logging & Monitoring

DB-LOG-01 High

Is database auditing enabled to capture logins, privilege use, schema/config changes and access to sensitive data?

Test: Review audit configuration and sample audit records for required events.
Evidence: Audit policy and sample logs.
Risk if failed: Without audit trails, misuse and breaches cannot be detected or investigated.
NIST DE.CM-3; PR.PS-4 · ISO A.8.15 · CIS CIS 8.2; 8.5 · PCI 10.2

DB-LOG-02 High

Are audit and database logs forwarded to a protected, central SIEM where the DBA cannot alter them?

Test: Confirm log forwarding and that local admins cannot edit central copies.
Evidence: SIEM ingestion evidence, retention configuration.
Risk if failed: Locally-held logs can be tampered with by an attacker or insider.
NIST PR.PS-4; DE.CM-1 · ISO A.8.15; A.8.16 · CIS CIS 8.9; 8.11 · PCI 10.3.4; 10.5.1

DB-LOG-03 Medium

Are alerts configured for high-risk database events (failed logins, privilege escalation, bulk data export, config change)?

Test: Review detection/alert rules and evidence of triage.
Evidence: Alert rules, sample alerts/tickets.
Risk if failed: Undetected attacks progress to data exfiltration.
NIST DE.CM-1; DE.AE-2 · ISO A.8.16 · CIS CIS 8.11; 13.1 · PCI 10.4; 10.7

DB-LOG-04 Low

Is time synchronised (NTP) across database hosts so logs correlate reliably?

Test: Check NTP configuration and clock drift on DB hosts.
Evidence: NTP configuration/status.
Risk if failed: Unsynchronised clocks undermine forensic correlation.
NIST PR.PS-4 · ISO A.8.17 · CIS CIS 8.4 · PCI 10.6.1

Backup & Recovery

DB-BAK-01 High

Are regular backups taken per RPO, encrypted, access-controlled, and are at least one copy offline/ immutable (ransomware-resilient)?

Test: Review backup schedule, encryption, storage location and immutability/offline copy.
Evidence: Backup policy, job logs, immutability configuration.
Risk if failed: No resilient backup means ransomware or corruption causes permanent data loss.
NIST PR.DS-11; RC.RP · ISO A.8.13 · CIS CIS 11.1; 11.2; 11.3 · PCI 3.5.1; 12.10

DB-BAK-02 Medium

Are database restores tested periodically to validate recoverability within the RTO?

Test: Review evidence of test restores and recovery-time measurement.
Evidence: Restore-test records.
Risk if failed: Untested backups routinely fail when needed.
NIST RC.RP-1 · ISO A.8.13 · CIS CIS 11.5 · PCI 12.10.1

DB-BAK-03 Medium

Are database backups and exports covered by the same access controls, classification and monitoring as the live data?

Test: Check who can access backups/exports and whether access is logged.
Evidence: Backup access controls and logs.
Risk if failed: Backups are a common, poorly-guarded route to bulk data theft.
NIST PR.DS-1; PR.AA-5 · ISO A.8.13 · CIS CIS 3.3; 11.2 · PCI 9.4; 3.5.1

Data Protection & Retention

DB-DAT-01 Medium

Is sensitive data discovered and classified so protection controls can be applied where they matter?

Test: Review data-discovery/classification output for in-scope databases.
Evidence: Data map / classification report.
Risk if failed: Unclassified sensitive data goes unprotected.
NIST ID.AM-7; PR.DS · ISO A.5.12; A.8.11 · CIS CIS 3.1; 3.2 · PCI 3.2; 12.5.2

DB-DAT-02 Low

Is data masking/redaction or row/column-level security applied so users see only the data they need?

Test: Review masking/RLS/column-security configuration for sensitive datasets.
Evidence: Masking/RLS configuration.
Risk if failed: Broad read access exposes more data than necessary.
NIST PR.AA-5; PR.DS · ISO A.8.11; A.8.3 · CIS CIS 3.3 · PCI 7.2; 3.4

DB-DAT-03 Medium

Are retention and secure-deletion rules enforced so data is not kept beyond need and is destroyed securely?

Test: Review retention schedule and evidence of secure deletion/purging.
Evidence: Retention policy, purge job evidence.
Risk if failed: Over-retention increases breach exposure and compliance risk (incl. DPDP/GDPR).
NIST PR.DS; GV.PO · ISO A.5.33; A.8.10 · CIS CIS 3.4; 3.5 · PCI 3.2.1; 9.4.6

DB-DAT-04 Medium

Are database changes (schema and privileged data changes) subject to change control and traceable to an approval?

Test: Review change-management records for a sample of database changes.
Evidence: Change tickets, approvals, audit trail.
Risk if failed: Unmanaged changes cause outages, drift and undetected malicious modification.
NIST PR.PS-1; GV.SC · ISO A.8.32 · CIS CIS 4.2 · PCI 6.5.1

Framework Mapping

Governance & baseline
NIST GV.PO; GV.RR; PR.PS · ISO A.5.1; A.8.9 · CIS CIS 4.1; 4.2 · PCI 2.2; 12.5 · 1-3-3; 2-3-1
Evidence: Hardening standard, inventory, exception register

Identity & authentication
NIST PR.AA-1; PR.AA-2 · ISO A.5.16; A.8.5 · CIS CIS 5.2; 6.3; 6.7 · PCI 8.3; 8.4 · 2-2-1
Evidence: Account list, password policy, MFA config

Privilege & access control
NIST PR.AA-5 · ISO A.8.2; A.8.3 · CIS CIS 6.1; 6.8 · PCI 7.2; 7.3 · 2-6-1
Evidence: Privilege report, role model, access review

Network exposure
NIST PR.IR-1; PR.DS-2 · ISO A.8.20; A.8.24 · CIS CIS 4.4; 3.10 · PCI 1.3; 4.2.1 · 2-5-1
Evidence: Firewall/SG rules, port scan, TLS config

Encryption & keys
NIST PR.DS-1 · ISO A.8.24 · CIS CIS 3.11 · PCI 3.5; 3.6; 3.7 · 2-7-1
Evidence: Encryption config, KMS/HSM, key rotation

Patch & vulnerability
NIST ID.RA-1; PR.PS-2 · ISO A.8.8 · CIS CIS 7.3; 7.6 · PCI 6.3; 11.3.1 · 2-10-1
Evidence: Patch report, authenticated scan results

Secure configuration
NIST PR.PS-1 · ISO A.8.9 · CIS CIS 4.8 · PCI 2.2 · 2-3-1
Evidence: Config export vs baseline, feature inventory

Auditing & logging
NIST DE.CM-3; PR.PS-4 · ISO A.8.15; A.8.16 · CIS CIS 8.2; 8.9 · PCI 10.2; 10.3 · 2-12-1
Evidence: Audit policy, SIEM ingestion, alert rules

Backup & recovery
NIST PR.DS-11; RC.RP · ISO A.8.13 · CIS CIS 11.1; 11.5 · PCI 12.10 · 2-9-1
Evidence: Backup jobs, immutability, restore tests

Data protection & retention
NIST ID.AM-7; PR.DS · ISO A.5.12; A.8.10; A.8.11 · CIS CIS 3.1; 3.4 · PCI 3.2; 3.4 · 2-8-1
Evidence: Data map, masking/RLS, retention & purge

info@cybersigmacs.com