CLOUDSWITCHED

FREE RESOURCE — SECURITY CHECKLIST

Database Security Assessment Checklist

A thorough security assessment of your database infrastructure across access control, encryption, audit logging, network isolation, vulnerability management and UK GDPR compliance — 50+ items across six sections to harden your data tier and close exposure.

6	50+	/10	Fillable
ASSESSMENT AREAS	ITEMS TO VERIFY	SCORE EACH SECTION	TICK & TYPE IN ANY VIEWER

ACCESS CONTROL · ENCRYPTION · NETWORK ISOLATION · UK GDPR

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this checklist

Work through each of the six sections with your DBA, security team or managed service provider. Verify each item against your **live database configuration** rather than relying on documentation alone, and tick only the controls that are **fully in place** — in production and verifiable today, not "we're working on it".

Flag any section scoring **below 6** for immediate remediation and carry it into a prioritised action plan on the summary pages. This is an **interactive PDF** — tick the boxes and type your scores, owners and notes directly in any modern PDF viewer.

WHAT THIS CHECKLIST IS

A practical security baseline covering the controls that actually reduce the risk of a data breach — authentication, encryption, audit logging, network isolation, patching and UK GDPR governance. It is not a substitute for a full penetration test on a specific environment, but it is a fast way to surface the exposures worth closing first.

SCORING GUIDANCE

Award points where you have evidence the control is in place — a configuration, an audit log, a policy, a tested procedure. Half measures do not score. Round each section to a whole number out of 10 and carry it to the summary table.

The six sections

- **01 Access Control & Authentication** — least privilege, MFA, named logins, JIT elevation.
- **02 Encryption & Data Protection** — TLS, TDE, key management, column-level encryption.
- **03 Audit Logging & Monitoring** — tamper-proof logs, alerting, SIEM, retention.
- **04 Network Security & Isolation** — private subnets, firewalls, bastion hosts, private endpoints.
- **05 Vulnerability Management** — supported versions, patching SLAs, scanning, pen testing.
- **06 Compliance & Data Governance** — data inventory, SARs, erasure, ROPA, breach response.

01

Access Control & Authentication

Controlling who can access your database and how they authenticate is the first line of defence against data breaches. Verify each control against your live access configuration before scoring.

- ☐ All database accounts use **named individual logins** rather than shared service accounts for accountability and audit trail integrity.
- ☐ The **principle of least privilege** is enforced — every user and application account has only the minimum permissions required for their role.
- ☐ **Default database accounts** (sa, root, postgres, admin) are disabled or renamed with strong, unique passwords managed in a secrets vault.
- ☐ **Multi-factor authentication** is enforced for all administrative access to the management console and direct SQL connections *(non-negotiable for production)*.
- ☐ **Service accounts** used by applications have restricted permissions limited to specific schemas, tables and operations (SELECT, INSERT, UPDATE) as required.
- ☐ A **quarterly access review** verifies all database accounts are still required and permissions are appropriate for current roles.
- ☐ **Password policies** enforce minimum complexity, rotation and lockout thresholds for all database authentication methods.
- ☐ Privileged access to production uses **just-in-time (JIT) elevation** with time-limited sessions and approval workflows.
- ☐ All **direct production access by developers** is prohibited except through controlled, audited break-glass procedures.

WHAT GOOD LOOKS LIKE

Every login maps to a named person, every permission is the minimum needed, and standing admin rights have been replaced by time-limited JIT elevation. Default accounts are gone, and a quarterly review proves the access list still reflects who actually needs in.

SECTION 01 SCORE _____ / **10** *Aim for 8+. Below 6 = access-control gap.*

OWNER _____ **TARGET DATE** _____

02

Encryption & Data Protection

Encryption protects data at rest and in transit. Ensure sensitive information is never exposed in plaintext — on the wire, on disk, or in your backups.

- ☐ All database connections use **TLS 1.2 or higher** with strong cipher suites — unencrypted connections are blocked at the server level.
- ☐ **Transparent Data Encryption (TDE)** or equivalent at-rest encryption is enabled on all production databases containing personal or sensitive data.
- ☐ **Encryption keys** are stored in a dedicated key management service (Azure Key Vault, AWS KMS, HashiCorp Vault) separate from the database server.
- ☐ Sensitive columns containing PII, financial or health data use **column-level or application-level encryption** for defence in depth.
- ☐ **Backup files are encrypted** with AES-256 before storage, and encryption keys are stored separately from the backup media.
- ☐ Database **connection strings and credentials** are stored in secrets management tools rather than in application config files or source code.
- ☐ **Data masking or dynamic anonymisation** is applied in non-production environments to prevent exposure of real personal data during development and testing.
- ☐ **Encryption key rotation** schedules are documented and enforced — keys are rotated at least annually or upon any suspected compromise.

WATCH OUT FOR

Encryption enabled in transit but not at rest, keys sitting on the same server they protect, or backups written in plaintext to a share. Encryption is only as strong as where you keep the keys — separate the key from the data.

SECTION 02 SCORE _____ / 10 *Aim for 8+. Below 6 = encryption / key gap.*

OWNER _____ **TARGET DATE** _____

03

Audit Logging & Monitoring

Comprehensive audit logging enables detection of unauthorised access and data exfiltration — and provides the compliance evidence UK GDPR requires when an incident happens.

- ☐ **Database audit logging** is enabled for all authentication events (successful and failed logins), schema changes and permission modifications.
- ☐ All **privileged operations** (GRANT, REVOKE, CREATE, ALTER, DROP, TRUNCATE) are logged with the executing user, timestamp and affected objects.
- ☐ Access to tables containing **personal data** (UK GDPR scope) is logged to support Subject Access Requests and breach investigations.
- ☐ **Audit logs are stored in a tamper-proof location** separate from the database server — administrators cannot modify or delete audit records.
- ☐ **Real-time alerting** is configured for suspicious activity including failed logins, privilege escalation, bulk data exports and after-hours access.
- ☐ **Audit logs are retained** for a minimum of 12 months in readily accessible storage and archived for the duration required by your compliance framework.
- ☐ A **SIEM integration** correlates database audit events with network, application and identity logs for comprehensive threat detection.
- ☐ **Log review** is performed at least monthly by the security team to identify anomalous patterns that automated alerting may not catch.
- ☐ The **audit configuration is tested quarterly** by simulating detectable events and verifying they appear correctly in logs and trigger appropriate alerts.

WHAT GOOD LOOKS LIKE

Logs land somewhere the database admins cannot reach, alerts fire in real time on the events that matter, and a quarterly test proves the pipeline still works. Untested logging is a false sense of security — verify the alerts actually fire.

SECTION 03 SCORE _____ / **10** *Aim for 8+. Below 6 = audit / detection gap.*

OWNER _____ **TARGET DATE** _____

04

Network Security & Isolation

Database servers should never be directly accessible from the internet. Network isolation limits the blast radius of any breach — verify reachability with an external scan, not the config alone.

- ☐ Database servers are deployed in a **private subnet or VLAN** with no direct internet access — all traffic routes through application servers or bastion hosts.
- ☐ **Firewall rules** restrict database access to only authorised application servers and management hosts by IP address and port.
- ☐ **Database management ports** (1433, 3306, 5432) are never exposed to the public internet — verify with external port scans quarterly.
- ☐ **Administrative access** uses a bastion host or VPN with multi-factor authentication rather than direct connections from workstations.
- ☐ **Network segmentation** ensures production, staging and development databases are on separate segments with no cross-environment access.
- ☐ **Cloud-hosted databases** use private endpoints (AWS PrivateLink, Azure Private Endpoint) rather than public IP addresses.
- ☐ **OS hardening** has been applied to the database server — unnecessary services disabled, unused ports closed, host-based firewall configured.
- ☐ **DNS resolution** for database hostnames uses internal DNS only — database addresses are not resolvable from external networks.

THE CLASSIC FAILURE

A database spun up ‘temporarily’ with a public IP and a permissive security group, then forgotten. Automated scanners find exposed 1433/3306/5432 within hours. If you cannot prove it is unreachable from the internet, assume it is reachable.

SECTION 04 SCORE _____ / **10** *Aim for 8+. Below 6 = network exposure gap.*

OWNER _____

TARGET DATE _____

05

Vulnerability Management

Unpatched databases are a primary attack vector. Proactive vulnerability management closes security gaps before they are exploited — patch on a clock, not on an incident.

- ☐ The database engine is on a **supported version** receiving active security patches from the vendor *(check end-of-life dates annually)*.
- ☐ **Security patches** are applied within 30 days of release for critical vulnerabilities and within 90 days for non-critical updates.
- ☐ A **patching process** includes staging tests, backup before applying, documented rollback procedures and post-patch validation.
- ☐ **Regular vulnerability scans** are performed against database servers using tools such as Nessus, Qualys or database-specific scanners like DbProtect.
- ☐ The **database attack surface is minimised** — unnecessary features, components, sample databases and default schemas have been removed.
- ☐ **Stored procedures and application SQL** are reviewed for SQL injection vulnerabilities as part of the secure development lifecycle.
- ☐ **Configuration baselines** are defined and deviations are detected automatically using configuration management or CIS benchmark scanning.
- ☐ **Third-party extensions, plugins and linked servers** are inventoried, risk-assessed and kept updated.
- ☐ An **annual penetration test** includes the database tier in scope to identify vulnerabilities that automated scanning may miss.

THE CHEAPEST WIN

Staying on a supported version with a patching SLA closes the majority of database CVEs before anyone has to think about them. End-of-life software is the gap attackers count on — track the EOL date a year out.

SECTION 05 SCORE _____ / **10** *Aim for 8+. Below 6 = patching / vuln gap.*

OWNER _____ **TARGET DATE** _____

06

Compliance & Data Governance

UK GDPR and industry regulations require demonstrable controls over personal data stored in databases. Document and evidence your compliance — an undocumented control is no control at all.

- ☐ A **data inventory** identifies every database and table containing personal data, categorised by data type and lawful basis for processing under UK GDPR.
- ☐ **Data retention policies** are enforced at the database level with automated purging or anonymisation of personal data that has exceeded its retention period.
- ☐ Procedures exist to fulfil **Subject Access Requests (SARs)** within the statutory 30-day deadline, including locating all personal data across databases.
- ☐ A documented process supports the **right to erasure** — deletion from live databases, backups and replicas where feasible.
- ☐ **Data Protection Impact Assessments (DPIAs)** have been completed for databases processing high-risk personal data categories.
- ☐ Database access and processing activities are documented in the organisation's **Record of Processing Activities (ROPA)** as required by UK GDPR Article 30.
- ☐ **Cross-border data transfers** are assessed for adequacy — replication to non-UK regions complies with UK GDPR transfer provisions.
- ☐ A **data breach response procedure** specific to database incidents is documented, tested and includes ICO notification within 72 hours where required.
- ☐ **Annual compliance audits** review database security controls against applicable standards (UK GDPR, ISO 27001, Cyber Essentials Plus) with findings tracked to remediation.

EVIDENCE BEATS INTENTIONS

When the ICO or an auditor asks, 'we delete old data' is not enough — you need the policy, the automated job and the log that proves it ran. Build the data inventory first; every other GDPR control depends on knowing where the personal data actually lives.

SECTION 06 SCORE _____ / **10** *Aim for 8+. Below 6 = compliance / governance gap.*

OWNER _____ **TARGET DATE** _____

Σ

Assessment score summary

Transfer the score for each section into the table. Set a priority (H/M/L) based on the gap to target. Anything below 6 is a candidate for the top-3 actions on the next page.

#	AUDIT AREA	SCORE / 10	PRIORITY
01	Access Control & Authentication	_____ / 10	☐ H ☐ M ☐ L
02	Encryption & Data Protection	_____ / 10	☐ H ☐ M ☐ L
03	Audit Logging & Monitoring	_____ / 10	☐ H ☐ M ☐ L
04	Network Security & Isolation	_____ / 10	☐ H ☐ M ☐ L
05	Vulnerability Management	_____ / 10	☐ H ☐ M ☐ L
06	Compliance & Data Governance	_____ / 10	☐ H ☐ M ☐ L
Σ	**TOTAL SCORE**	_____ / 60	—

READING THE TOTAL

Six sections, ten points each — a maximum of 60. Treat the total as a direction of travel, but let the individual section scores drive the work: one section at 3 matters more than a balanced 7 across the board.

Interpretation & priority actions

Translate your total score into a risk band, then commit to a small number of next steps. The goal is one page of decisions, not a wish list.

Score interpretation

48–60	**Excellent.** Your database security is well-managed. Focus on continuous monitoring and emerging threats.
36–47	**Good foundation, gaps exist.** Prioritise any section scoring below 6 with owners and deadlines.
Below 36	**Significant gaps.** The breach risk is material — consider an urgent review with a database security specialist.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

AUDIT COMPLETED BY _____ DATE _____ NEXT REVIEW DUE _____

CLOUDSWITCHED

IT SUPPORT & PROJECT SERVICES

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom