CLOUDSWITCHED

FREE RESOURCE — CHECKLIST

Database Security Assessment Checklist

Thorough security assessment of your database infrastructure covering access control, encryption, audit logging, network isolation, vulnerability management, and UK GDPR compliance — 50+ items across 6 sections.

6	50+	Score	Free
ASSESSMENT AREAS	ITEMS TO VERIFY	EACH SECTION OUT OF 10	PRINT & USE NO STRINGS

How to Use This Checklist

Work through each section with your DBA, security team, or managed service provider. Verify each item against your live database configuration rather than relying on documentation alone. Score each section honestly and prioritise any area below 6 for immediate remediation.

Need Help With Your IT?

Our team can help you implement the recommendations in this resource.

info@cloudswitched.com
+44 2030 043 450
[redacted]

1 Access Control & Authentication

Controlling who can access your database and how they authenticate is the first line of defence against data breaches.

- □ 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 database 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 databases uses **just-in-time (JIT) elevation** with time-limited sessions and approval workflows
- □ All **direct database access by developers** to production is prohibited except through controlled, audited break-glass procedures

Section Score: /10

2 Encryption & Data Protection

Encryption protects data at rest and in transit. Ensure sensitive information is never exposed in plaintext.

- □ 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 data, or health information use **column-level encryption** 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 configuration files or source code
- □ Data masking or **dynamic data 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

Section Score: ____/10

3 Audit Logging & Monitoring

Comprehensive audit logging enables detection of unauthorised access, data exfiltration, and compliance evidence for UK GDPR.

- □ 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 login attempts, 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

Section Score: ____ /10

4 Network Security & Isolation

Database servers should never be directly accessible from the internet. Network isolation limits the blast radius of any breach.

- □ 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 network segments with no cross-environment access
- □ Cloud-hosted databases use **private endpoints** (AWS PrivateLink, Azure Private Endpoint) rather than public IP addresses
- □ Database server **operating system hardening** has been applied — 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

Section Score: ____/10

5 Vulnerability Management

Unpatched databases are a primary attack vector. Proactive vulnerability management closes security gaps before they are exploited.

- □ 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 testing in a staging environment, 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
- □ Database **configuration baselines** are defined and deviations are detected automatically using configuration management or CIS benchmark scanning
- □ Third-party database extensions, plugins, and **linked server connections** 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

Section Score: ____/10

6 Compliance & Data Governance

UK GDPR and industry regulations require demonstrable controls over personal data stored in databases. Document and evidence your compliance.

- □ 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** (right to be forgotten) including deletion from live databases, backups, and replicas where feasible
- □ Data Processing Impact Assessments (**DPIAs**) have been completed for databases processing high-risk personal data categories
- □ Database access and **data 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** — database 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

Section Score: ____ /10

7 Audit Summary & Action Plan

#	AUDIT AREA	SCORE	PRIORITY
1	Access Control & Authentication	/ 10	H / M / L
2	Encryption & Data Protection	/ 10	H / M / L
3	Audit Logging & Monitoring	/ 10	H / M / L
4	Network Security & Isolation	/ 10	H / M / L
5	Vulnerability Management	/ 10	H / M / L
6	Compliance & Data Governance	/ 10	H / M / L
TOTAL SCORE		**/ 60**	

Score Interpretation

80–100: Excellent. Your IT setup is well-managed. Focus on continuous improvement and emerging threats.
60–79: Good foundation but gaps exist. Prioritise areas scoring below 6 and create an action plan.
Below 60: Significant gaps that put your business at risk. Consider an urgent review with an IT specialist.

Top 3 Priority Actions:

1

2

3

Additional Notes

Audit completed by: __________________________ Date: __________________________ Next review due: __________________________

Need Help With Your IT?
Our team can help you implement the recommendations in this resource.

info@cloudswitched.com
+44 2030 043 450
[redacted]