

FREE RESOURCE — TEMPLATE

# Database Backup & **Recovery** Template

A structured template for documenting your database backup strategy, recovery procedures, disaster recovery planning and compliance testing — essential for UK business continuity and GDPR accountability.

**4**

PLANNING  
AREAS

**20+**

RECOVERY  
CRITERIA

**3**

FILLABLE  
TABLES

**Fillable**

TICK & TYPE  
IN ANY VIEWER

BACKUP STRATEGY

RECOVERY RUNBOOKS

DISASTER RECOVERY

COMPLIANCE

PREPARED FOR

Cloudswitched KnowledgeCloudswitched Ltd.  
Library

PREPARED BY

VERSION

2026 Edition

FORMAT

Interactive PDF

# 00

## How to use this template

Complete each of the four sections with your database team or your managed service provider. Fill in every field, document each recovery scenario step-by-step, and log your test results in the tables provided. The goal is a single living document that any team member can follow under pressure — not a form you complete once and file away.

This is an **interactive PDF**: tick the boxes and type directly into the underscore fields in any modern PDF viewer, or print it and complete by hand. Review and re-test on the cadence you set below — backups and recovery plans decay silently, and an untested backup is not a backup.

### WHAT THIS TEMPLATE COVERS

Backup configuration and schedules, recovery procedures and runbooks for the four most common failure modes, disaster recovery planning for site-loss and ransomware scenarios, and the testing and compliance evidence that satisfies UK GDPR, ISO 27001 and Cyber Essentials Plus.

### THE GOLDEN RULE

A backup you have never restored is a hope, not a plan. Schedule a real restore test on a non-production instance at least quarterly, record the time taken in Section 4, and have the result signed off. Recovery Time and Recovery Point objectives mean nothing until they are proven.

### DOCUMENT CONTROL

Effective Date

\_\_\_\_\_

Document Owner

\_\_\_\_\_

Version / Revision

\_\_\_\_\_

Next Review Date

\_\_\_\_\_

Reviewed & approved this cycle?

☐ Yes ☐ No Approver: \_\_\_\_\_

# 01

## Backup Strategy & Schedule

*Document every database backup configuration to ensure complete coverage and no single point of failure in your data protection strategy.*

**Database Name & Engine** *(e.g. SQL Server 2022, PostgreSQL 16)*

**Database Size (Current)**

**Growth Rate (Monthly)**

**Full Backup Schedule** *(Day / Time / Frequency)*

**Differential or Incremental Backup Schedule**

**Transaction Log Backup Frequency**

**Retention — On-Site**

**Retention — Off-Site / Cloud**

**Backup Storage Location(s) — Primary**

**Backup Storage Location(s) — Secondary / Off-Site**

**Backup Encryption Method & Key Management**

**Backup Monitoring Tool & Alert Recipients**

# 01

## Backup Strategy — Verification

**Backup Verification Process** *(How and when are backups tested for restorability?)*

\_\_\_\_\_  
Last Successful Full Backup (Date & Time)

\_\_\_\_\_  
Last Successful Restore Test (Date & Time)

### Backup configuration log

*Record each backup type, its schedule and retention, where it is stored, whether it is encrypted, and when it was last verified.*

| BACKUP TYPE      | SCHEDULE | RETENTION | STORAGE LOCATION | ENCRYPTED                | LAST VERIFIED |
|------------------|----------|-----------|------------------|--------------------------|---------------|
| Full             | _____    | _____     | _____            | <input type="checkbox"/> | _____         |
| Differential     | _____    | _____     | _____            | <input type="checkbox"/> | _____         |
| Transaction log  | _____    | _____     | _____            | <input type="checkbox"/> | _____         |
| Off-site copy    | _____    | _____     | _____            | <input type="checkbox"/> | _____         |
| Archive (yearly) | _____    | _____     | _____            | <input type="checkbox"/> | _____         |

#### TIP — 3-2-1 RULE

Keep at least three copies of your data, on two different media types, with one copy off-site and ideally immutable. Tick the Encrypted column only where encryption-at-rest is confirmed and the keys are managed separately from the backups.

# 02

## Recovery Procedures & Runbooks

*Step-by-step recovery procedures ensure any team member can restore the database under pressure. Document every scenario.*

### Objectives & contacts

Recovery Time Objective (RTO) — *max downtime*

Recovery Point Objective (RPO) — *max data loss*

Primary DBA / Recovery Contact (*Name & Phone*)

Secondary DBA / Recovery Contact (*Name & Phone*)

Escalation Contact (*IT Manager / CTO*)

### Scenario 1 — Full Database Restore from Backup

*Step-by-step procedure including backup location, restore commands, integrity checks and application reconnection.*

### Scenario 2 — Point-in-Time Recovery

*Procedure for restoring to a specific transaction using full + log backups.*

## 02

# Recovery Procedures — continued

### Scenario 3 — Single Table or Object Recovery

*Procedure for recovering individual objects without a full database restore.*

---

---

---

---

### Scenario 4 — Corruption Recovery

*Steps for detecting corruption with DBCC / pg\_checksums, restoring clean pages and validating integrity.*

---

---

---

---

### Post-Recovery Validation Checklist

*Confirm each check before declaring the database recovered and returning it to service.*

- ☐ Row counts reconciled against expected / pre-incident figures.
- ☐ Integrity checks (DBCC CHECKDB / pg\_checksums) pass clean.
- ☐ Application smoke tests pass against the recovered database.
- ☐ Key users have verified critical records and recent transactions.
- ☐ Incident, downtime and data-loss window recorded for review.

# 03

## Disaster Recovery Planning

*Plan for worst-case scenarios including complete site loss, ransomware and regional cloud outages.*

**DR Site Location** *(UK Region / Data Centre)*

---

**DR Database Replication Method** *(Async / Sync / Log Shipping)*

---

**Replication Lag Monitoring & Acceptable Threshold**

---

**DR Failover Type**

☐ Automatic   ☐ Manual   Estimated failover time (mins): \_\_\_\_\_

---

**DR Environment Specification** *(CPU / RAM / Storage)*

---

**Ransomware Recovery Strategy** *(immutable backups, air-gapped copies, recovery from clean backup)*

---

**Complete Site Loss Procedure** *(provision new infrastructure, restore from off-site backups)*

---

**Cloud Region Outage Procedure** *(failover to secondary region, DNS updates, app reconfiguration)*

---

**Last DR Failover Test — Date & Result**

**Next Scheduled DR Test Date**

---

---

---

# 03

## Disaster Recovery — Scenario Matrix

Set an RTO and RPO target for each failure scenario, record when it was last tested and the result, and schedule the next test.

| DR SCENARIO              | RTO TARGET | RPO TARGET | LAST TESTED | TEST RESULT | NEXT TEST |
|--------------------------|------------|------------|-------------|-------------|-----------|
| Primary server failure   | _____      | _____      | _____       | _____       | _____     |
| Storage failure          | _____      | _____      | _____       | _____       | _____     |
| Complete site loss       | _____      | _____      | _____       | _____       | _____     |
| Ransomware attack        | _____      | _____      | _____       | _____       | _____     |
| Cloud region outage      | _____      | _____      | _____       | _____       | _____     |
| Accidental data deletion | _____      | _____      | _____       | _____       | _____     |

### RANSOMWARE — ASSUME THE BACKUPS ARE TARGETED

Modern ransomware actively hunts and encrypts backup repositories before triggering. Maintain at least one immutable or air-gapped copy that the production credentials cannot reach, and rehearse recovery from that clean copy specifically — not just from your nearest snapshot.

# 04

## Testing & Compliance Documentation

Regular testing and compliance documentation satisfy UK GDPR, audit requirements and business continuity standards.

Backup Restore Test Frequency *(Monthly / Quarterly)*

DR Failover Test Frequency *(Quarterly / Bi-Annual)*

Last Audit Date & Auditor

Compliance Standards Applicable

☐ UK GDPR ☐ ISO 27001 ☐ Cyber Essentials Plus ☐ Other: \_\_\_\_\_

Data Classification & Retention Policy *(categories of data stored, retention periods, deletion procedures per UK GDPR)*

Right to Erasure Procedure *(how personal data is identified and permanently deleted from databases and backups on request)*

Data Protection Officer (DPO) Contact

ICO Registration Number

# 04

## Backup & Recovery Test Log

Log every restore and failover test. Tick "Verified" once the recovered data has been confirmed correct, and have each test signed off.

| TEST DATE        | TEST TYPE | DATABASE | TIME TO RESTORE | VERIFIED                 | ISSUES FOUND | SIGNED OFF BY |
|------------------|-----------|----------|-----------------|--------------------------|--------------|---------------|
| Full restore     | _____     | _____    | _____           | <input type="checkbox"/> | _____        | _____         |
| Point-in-time    | _____     | _____    | _____           | <input type="checkbox"/> | _____        | _____         |
| DR failover      | _____     | _____    | _____           | <input type="checkbox"/> | _____        | _____         |
| Table recovery   | _____     | _____    | _____           | <input type="checkbox"/> | _____        | _____         |
| Ransomware drill | _____     | _____    | _____           | <input type="checkbox"/> | _____        | _____         |

### PLAN SIGN-OFF

Reviewed By (Name & Role)

\_\_\_\_\_

Signature

\_\_\_\_\_

Date Signed

\_\_\_\_\_

Plan tested & approved?

☐ Yes ☐ No

### Need help with your backup & recovery?

Our team can design, test and manage a resilient backup and disaster recovery strategy for your databases.

[info@cloudswitched.com](mailto:info@cloudswitched.com)

+44 2030 043 450



CLOUDSWITCHED

IT SUPPORT & PROJECT SERVICES

[info@cloudswitched.com](mailto:info@cloudswitched.com)

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