Database Backup & Recovery Template

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

4	20+	Runbooks	Free
PLANNING AREAS	RECOVERY CRITERIA	INCLUDED THROUGHOUT	PRINT & USE NO STRINGS

How to Use This Template

Complete each section with your team. Fill in the fields, use the comparison tables to evaluate options, and document your decisions. Print this template or complete it digitally.

1 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

BACKUP RETENTION PERIOD (ON-SITE)

BACKUP RETENTION PERIOD (OFF-SITE / CLOUD)

BACKUP STORAGE LOCATION(S) — PRIMARY

BACKUP STORAGE LOCATION(S) — SECONDARY / OFF-SITE

BACKUP ENCRYPTION METHOD & KEY MANAGEMENT

BACKUP VERIFICATION PROCESS (HOW AND WHEN ARE BACKUPS TESTED FOR RESTORABILITY?)

BACKUP MONITORING TOOL & ALERT RECIPIENTS

LAST SUCCESSFUL FULL BACKUP (DATE & TIME)

LAST SUCCESSFUL RESTORE TEST (DATE & TIME)

BACKUP TYPE	SCHEDULE	RETENTION	STORAGE LOCATION	ENCRYPTED	LAST VERIFIED
Full					
Differential					
Transaction log					
Off-site copy					
Archive (yearly)					

2 Recovery Procedures & Runbooks

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

RECOVERY TIME OBJECTIVE (RTO) — MAXIMUM ACCEPTABLE DOWNTIME

RECOVERY POINT OBJECTIVE (RPO) — MAXIMUM ACCEPTABLE 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)

SCENARIO 3: SINGLE TABLE OR OBJECT RECOVERY (PROCEDURE FOR RECOVERING INDIVIDUAL OBJECTS WITHOUT 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 (ROW COUNTS, INTEGRITY CHECKS, APPLICATION SMOKE TESTS, USER VERIFICATION)

3 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 (MINUTES)

DR ENVIRONMENT SPECIFICATION (CPU / RAM / STORAGE)

RANSOMWARE RECOVERY STRATEGY (IMMUTABLE BACKUPS, AIR-GAPPED COPIES, RECOVERY PROCEDURE FROM CLEAN BACKUP)

COMPLETE SITE LOSS PROCEDURE (STEPS TO PROVISION NEW INFRASTRUCTURE AND RESTORE FROM OFF-SITE BACKUPS)

CLOUD REGION OUTAGE PROCEDURE (FAILOVER TO SECONDARY REGION, DNS UPDATES, APPLICATION RECONFIGURATION)

LAST DR FAILOVER TEST DATE & RESULT

NEXT SCHEDULED DR TEST DATE

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					

4 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)

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)

BACKUP TEST RESULTS LOG (DATE, TYPE OF TEST, DATABASE RESTORED, TIME TAKEN, ISSUES FOUND, SIGN-OFF)

DATA PROTECTION OFFICER (DPO) CONTACT

ICO REGISTRATION NUMBER

TEST DATE	TEST TYPE	DATABASE	TIME TO RESTORE	DATA VERIFIED	ISSUES FOUND	SIGNED OFF BY
	Full restore					
	Point-in-time					
	DR failover					
	Table recovery					
	Ransomware drill					