

Backup-Strategie: 1-Seiter für IT-Leitung (KMU)

Merksatz: Eine Backup-Lösung ist das Werkzeug (Sichern/Restore). Die Backup-Strategie ist das Betriebsmodell (Prioritäten, Rollen, Freigaben, Tests, Nachweise).

1) Scorecard (Reifegrad)

Bewerten Sie jeden Punkt mit **0 / 1 / 2** (0 = nicht geregelt, 1 = teilweise, 2 = klar geregelt & geübt).

Bereich	0	1	2
Kritische Datenbereiche priorisiert (Top 3–5)	☐	☐	☐
Wiederanlauf-Ziel in Business-Sprache festgelegt (RTO)	☐	☐	☐
Max. tolerierbarer Datenverlust definiert (RPO)	☐	☐	☐
Entscheidungsweg im Incident klar (Wer priorisiert?)	☐	☐	☐
Restore-Rechte & Freigabeprozess geregelt (z. B. 4-Augen)	☐	☐	☐
Vollständigkeits-Check definiert (Wer bestätigt was?)	☐	☐	☐
Offboarding inkl. Wissenssicherung integriert	☐	☐	☐
Aufbewahrung & Löschung (DSGVO/RTBF) geregelt	☐	☐	☐
Backup-Systemzugriffe minimiert & regelmäßig geprüft	☐	☐	☐
Realistische Tests inkl. Zeitmessung etabliert	☐	☐	☐

Interpretation: 0–8 = Risiko / Ad-hoc, 9–14 = solide Basis, 15–20 = hohe Wiederanlauf-Fähigkeit.

2) Entscheidungsweg (Incident → Wiederanlauf)

Ziel: Im Incident nicht diskutieren, sondern abarbeiten. Minimaler Ablauf, der als Runbook taugt.

1	Incident erkannt Auslöser/Ticket, betroffene Workloads grob klären
2	Triage (IT) Scope eingrenzen, Daten/Identität/Config unterscheiden
3	Prioritäten (IT + Business Owner) Top 3 zuerst; RTO/RPO beachten
4	Restore-Freigabe (IT-Leitung) Freigabeprinzip (z. B. 4-Augen) anwenden
5	Restore durchführen (IT) in-place/alternativ; Logging aktiv
6	Validierung (Owner) Vollständigkeit + Zugriff bestätigen
7	Abschluss Kommunikation: was ist wieder verfügbar?
8	Lessons Learned Zeitwerte/Playbook aktualisieren (1–3 Maßnahmen)

Rollen (minimal): Incident Lead (IT), Entscheider (IT-Leitung), Business Owner je Bereich (optional: Dokumentation/Comms).

3) Test-Rhythmus (damit aus Hoffnung Planbarkeit wird)

Monatlich (15–30 min): Rechte-Check (Restore/Export), Alarmierung & Kontakte, Änderungen an kritischen Projekten/Owners (Offboarding).

Quartalsweise (60–120 min): Restore-Test: 1 Projekt-Site/Ordner + 1 Mailbox/Shared Mailbox oder anderes kritisches Objekt. Zeit messen & dokumentieren.

Halbjährlich (45–60 min): Praxis-Check/Tabletop: Szenario durchspielen (Massenlöschung, Ransomware, Fehlkonfiguration). Prioritäten- & Freigabekette testen.

Jährlich (60 min): Nachweis-Check: Scorecard aktualisieren, letzte Testergebnisse, Lessons Learned, Maßnahmenliste fürs kommende Jahr.

Dokumentieren Sie pro Test: Datum, Umfang, Dauer, Ergebnis, Abweichungen, Verantwortliche, nächste Verbesserung (1–3 Punkte).