

BR-SYSTEMS · ENGLISH EDITION

Backup and the 3-2-1 principle

Design recovery around business impact, protected copies and proven restoration.

Personally accountable · clearly documented · vendor-transparent

From concern to an owned action plan

This guide is designed for small and medium-sized organisations that need practical decisions rather than generic fear or a product-first answer.

How to use it

Work through the actions with the people who own the affected business processes. Mark what is already evidenced, assign an owner to every gap and agree a realistic review date.

Decision principles

01	Start from business impact and responsibility.
02	Prefer written evidence over assumed status.
03	Keep alternatives and exit paths visible.
04	Test recovery and operating processes, not only settings.

Important

This publication provides technical orientation. It is not legal advice, a certification or a guarantee of security. Current law, contracts, manufacturer documentation and the organisation's specific risk context remain authoritative.

Practical action checklist

Use the right-hand side of a printed copy for owner, evidence and due date.

01	Keep at least three copies of important data.
02	Use at least two different storage types or failure domains.
03	Maintain one copy that is offline, immutable or independently protected.
04	Separate backup administration from daily administration.
05	Define retention from recovery and legal requirements.
06	Monitor jobs, capacity and failed protection windows.
07	Test file, application and full-system restoration.
08	Record recovery time and unresolved dependencies.
09	Protect encryption keys and recovery credentials.
10	Review the design after major infrastructure changes.

A sensible next step

BR-Systems can help establish the baseline, prioritise the gaps and implement or operate the agreed measures. A short initial consultation is enough to determine whether that would be useful.

br-systems.eu · info@br-systems.eu · +49 179 160 1700