



Backup Checklist

Are your backups really ready for 2027?

Most companies assume their backups are working—until disaster strikes.

This checklist helps you check in just a few minutes whether your backup strategy is secure, complete and recoverable.

1. Backup completeness

- ☐ Are all critical systems included in your backups (servers, SaaS, cloud, endpoints)?
- ☐ Is there a process to identify new systems, SaaS services and applications that were not centrally procured, and add them to the backup strategy?
- ☐ Is data from Microsoft 365 / Google Workspace also backed up?
- ☐ Is there an up-to-date overview of all backed-up systems?

2. Backup frequency

- ☐ Does your backup frequency meet your business requirements?
- ☐ For critical systems, have you defined both the maximum recovery time (RTO) and the maximum acceptable data loss (RPO)?

3. Protection against ransomware and attacks

- ☐ Is at least one backup copy immutable and protected against deletion?
- ☐ Are backup locations physically or logically separated?
- ☐ Are backup accounts protected separately (MFA, role-based permissions)?
- ☐ Can backups be protected from deletion or encryption in an emergency?

4. Recoverability (the most important point)

- ☐ Have restore tests been carried out in the last 6–12 months?
- ☐ Is it clearly defined how quickly systems must be restored (RTO)?
- ☐ Can data also be restored selectively (file / email / user)?
- ☐ Is there a documented recovery scenario for emergencies?
- ☐ Is the integrity of backup data checked regularly?
- ☐ Are recovery and disaster recovery procedures documented and tested regularly for different failure scenarios?





Backup Checklist

5. Offsite backups and geographic redundancy

Are backups protected against the following risks?

- | | | | | | | | |
|--------------------------|------|--------------------------|--------------|--------------------------|------------------|--------------------------|------------|
| ☐ | Fire | ☐ | Power outage | ☐ | Natural disaster | ☐ | Ransomware |
|--------------------------|------|--------------------------|--------------|--------------------------|------------------|--------------------------|------------|

Many companies follow the 3-2-1-1-0 rule:

3 copies of the data / 2 different storage media / 1 offsite copy / 1 immutable backup / 0 errors after a recovery test

6. Monitoring and alerts

- | | |
|--------------------------|---|
| ☐ | Are backup jobs monitored automatically? |
| ☐ | Are errors reported immediately? |
| ☐ | Does someone review the reports regularly? |
| ☐ | Is the backup strategy documented and up to date? |

7. Capacity and growth

- | | |
|--------------------------|---|
| ☐ | Is there enough backup storage for the coming year? |
| ☐ | Is there an archiving strategy for old data? |

8. Compliance and retention

- | | |
|--------------------------|--|
| ☐ | Is there an archiving strategy for old data? |
| ☐ | Are there clear deletion policies? |

9. Hidden risks in the backup strategy

- | | |
|--------------------------|---|
| ☐ | Are there any single points of failure (e.g. a backup system without redundancy)? |
| ☐ | Are backups only "stored" but never actively checked? |
| ☐ | Is it clear who will have access to restore data in an emergency? |

If you cannot confidently check off several items, there may be no immediate risk – but there is a clear gap in your IT resilience.

