Cloud Backup vs Local Backup Explained for UK Businesses

Executive Summary

- All UK Small Medium Enterprises should have a Backup Plan.
- Backups are essential protection for your business to ensure you do not lose data through accidental deletion or malicious attacks, such as Ransomware.
- A Cloud Backup stores your data in a secure location away from your premises, while Local Backup stores data on physical devices in your premises.
- Cloud Backup provides high-level redundancy and disaster recovery, while Local Backup gives you the ability to quickly recover your data.
- The primary risk for SMEs is using only one method of backup.
- Cyber criminals are increasingly targeting connected Local Backups to encrypt your files – infection through Ransomware.
- The UK General Data Protection Regulation specifies "Appropriate Technical and Organisational Measures" must be in place, and back-ups are a critical aspect of this.
- Using a Hybrid Backup solution (Cloud + Local) can provide the most effective and safest means of protecting your data.
- Having a structured 30-day Resilience Plan will increase your Resilience substantially without incurring any significant costs.

Who This Guide Is For

- Small and Medium-Sized Enterprises in the UK (1-50 Employees).
- Directors, Owners & Office Manager.
- SME's without dedicated internal IT Security Teams.
- SME's reviewing their Cyber Insurance or fulfilling their UK GDPR requirements for Compliance.

What You'll Achieve

- You will have a more complete understanding of Cloud and Local Back-up in plain language.
- You will be able to Compare Costs, Times, Risks and Compliance between Cloud, Local & Hybrid Back-up methods
- You will be able to identify the key mistakes that most SMEs make.
- You will determine whether Cloud, Local or Hybrid Back-up is best for your business.
- You will be able to implement the minimum necessary Backup Standards into your practice.
- You will have a thorough knowledge of how your Back-up will help your business achieve compliance with the UK GDPR.

Why Backup Matters for UK SMEs

Backups help protect businesses from:

- Ransomware attacks
- Accidental deletion of files
- Hardware failure
- A fire, flood or theft
- Mistakes made by humans

If a business does not have reliable backups in place, they may take days or weeks to recover from an incident, and in some cases, they may not fully recover at all.

The UK General Data Protection Regulation (GDPR) requires businesses to maintain the availability and resilience of all systems that process personal data. Backups directly assist with these requirements.

What Is Cloud Backup?

With cloud backup, your files, databases, or entire systems are continuously backed up to remote data centres that a provider (Microsoft 365, Google Workspace, Backblaze, IDrive, Acronis or Dropbox Business) manages and maintains securely.

Benefits of Cloud Backup

- Automatic and no manual effort on the user's part.
- Off-site and protected from fire, flood, theft or ransomware encryption of local copies by default.
- Accessable from anywhere (home, office, or different device).
- Versioning and ransomware protection, many offer immutable backups (cannot change/destroy).
- Scales easily with your growth.

Challenges of Cloud Backup

- Monthly or annual subscription cost (average £5–£20/user/month).
- Speed of recovery relies on the speed of your internet connection (for very big recoveries it may take hours/days).
- Provider will rely on their services while you cannot access the information locally.
- Your information will leave your company. You would want to select a cloud provider (UK/EU based) for legal security under GDPR.

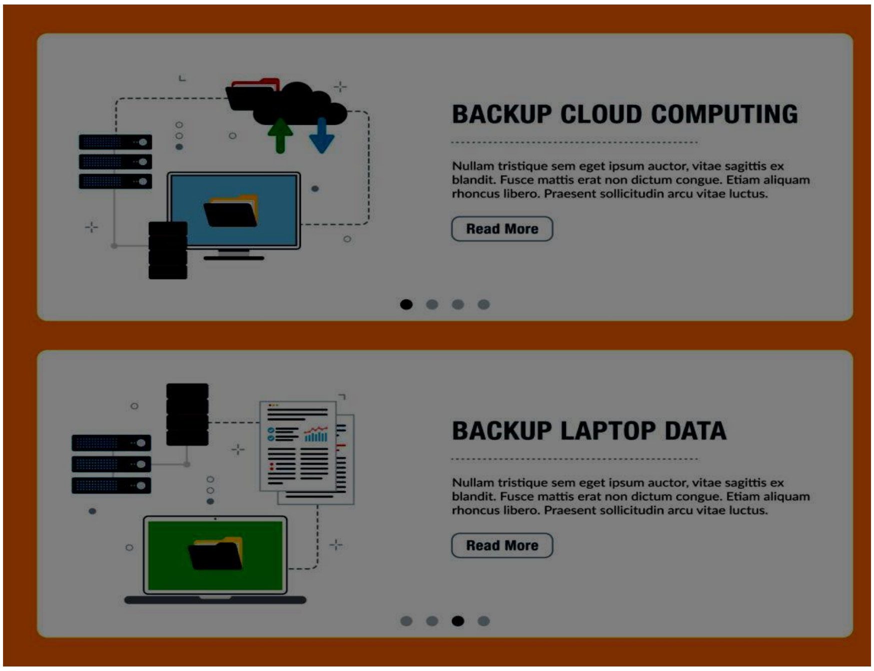
Common Errors

- Assuming that using "OneDrive/Google Drive sync = backup". Sync will mirror deletions made onyour computer.
- Not having versioning or immutability enabled on their account.

- Using consumer pricing plans that lack required business features.

Quick Wins

- If using Microsoft 365 enable OneDrive Known Folder Move (will back up Desktop/Documents automatically).
- Set up versioning in your account (majority of cloud storage solutions keep 30-180 days by default).


BACKUP CLOUD COMPUTING
Nullam tristique sem eget ipsum auctor, vitae sagittis ex blandit. Fusce mattis erat non dictum congue. Etiam aliquam rhoncus libero. Praesent sollicitudin arcu vitae luctus.
Read More
BACKUP LAPTOP DATA
Nullam tristique sem eget ipsum auctor, vitae sagittis ex blandit. Fusce mattis erat non dictum congue. Etiam aliquam rhoncus libero. Praesent sollicitudin arcu vitae luctus.
Read More

What Is Local Backup?

Local Backup is a way to copy your data to a device that you own and control (such as an external hard drive, a NAS, USB drive, or on site server).

Advantages of this backup system:

- Fast restore time — no waiting on an internet connection; just plug in and copy data back.
- Pay once for hardware, with no ongoing fees.
- You always have complete control over your data (no data leaves your building).
- Great if you have very large amounts of data (terabytes), since uploading over the cloud would be a slow process.

Disadvantages of this backup system:

- Vulnerable to physical hazards (fire, flood, theft, and ransomware if the hard drive is still plugged in).
- Must have adequate discipline (someone must plug the hard drive into the computer to run the backup and then take it offsite at least once per week).

- You will not have an automatic copy of your data offsite unless you manually move the hard drive.
- The hardware can fail; require some regular maintenance, testing and eventual replacement.

Some common mistakes when setting up local backup systems are:

- Leaving hard drive plugged in at all times; ransomware can find and encrypt it.
- No copy of your data off-site; creates a single point of failure.
- Never test restoring data using your backup; looks good on screen but will not work if lost.
- To make it easier, buy one external hard drive (£60–£120) and run one manual backup to it each week, keeping it disconnected/offsite while not in use.

Side-by-Side Comparison

Factor	Cloud Backup	Local Backup
Location	Off-site data centre	On-site device
Recovery Speed	Slower for large data	Very fast locally
Disaster Protection	Excellent	Limited
Ransomware Risk	Lower (if configured properly)	Higher if connected
Cost Model	Monthly subscription	Hardware upfront
Scalability	Easy	Limited by hardware
Maintenance	Managed by provider	Your responsibility
GDPR Support	Strong if configured correctly	Depends on setup

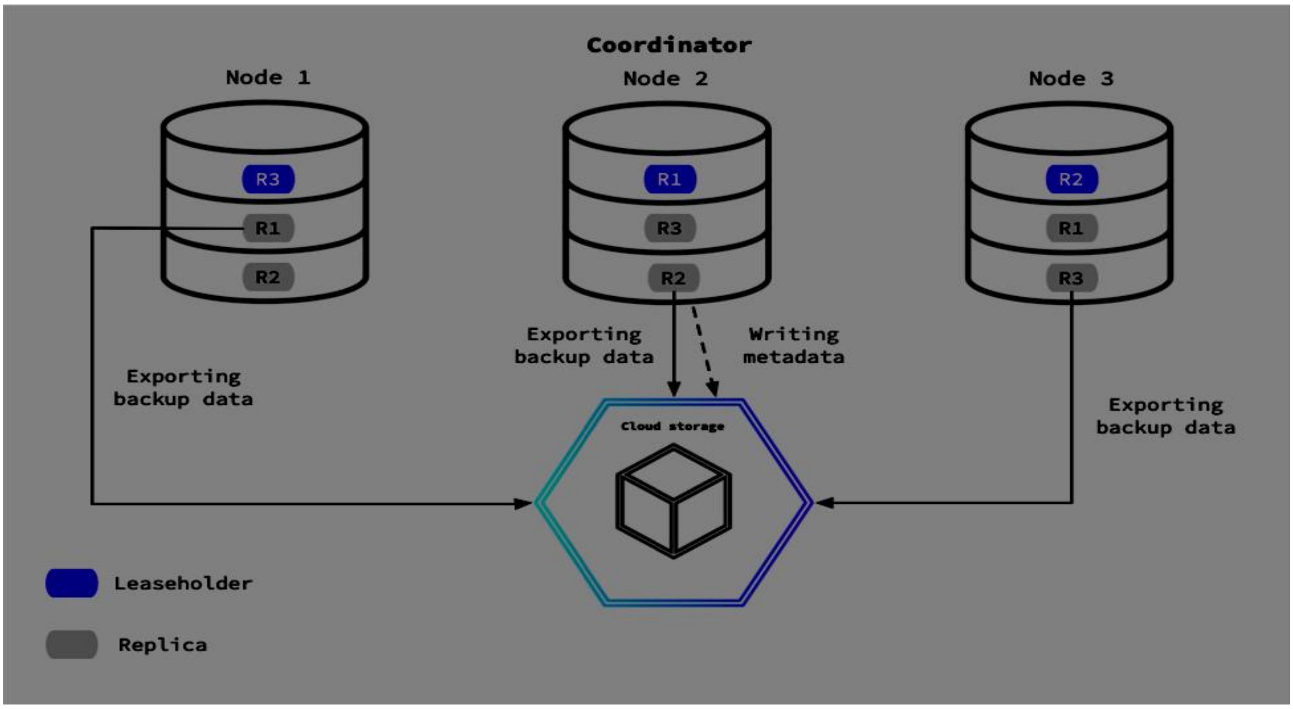
10-User vs 30-User Mini Case Example

10-User Office Example	30-User Office Example
Company • Small accounting firm **Risk Profile** • High exposure personal data • Medium amount of data • Limited IT Staff **Option Chosen** • Cloud Backup for Microsoft 365 • Local Encrypted NAS Backup • Weekly Off-site Offline Copy **Reason** • Balance of Cost, Speed, and Compliance Protection	**Company** • Engineering Company Sharing Design Files **Risk Profile** • Large File Sizes • CAD Drawings • Server Based Systems **Option Chosen** • Local Backup Appliance for Fast Restore • Cloud Immutable Backup Copy • Quarterly Restore Tests **Reason** • Speed Required to Recover Operations.

Recommended Minimum Backup Standard for UK SMEs

For the majority of SMEs, it has been suggested that there is a minimum of:

- 3 copies of your data
- 2 different types of storage for your data
- 1 copy of your data stored off-site



As an example:

- Live system
- Local NAS backup
- Cloud backup (preferably immutable)

Additionally:

- Daily automated copy of all data
- Use MFA for all backup accounts
- Perform a quarterly test restore of data from backup
- Document your data recovery plan
- Have a clearly defined Recovery Time Objective (RTO) for data recovery

Decision Framework: Which Option Is Right for You?

Ask Yourself:

- How quickly do we need to restore data?

- What would a single day of downtime Cloud come for our business?
- Do we have reliable broadband?
- Are we processing highly sensitive personal data?
- Do we have ransomware protection?

If You Are Considered:

- Micro business (1 - 5 employees): Cloud backup should normally be sufficient.
- Small business (5 - 20 employees): Hybrid is highly recommended.
- Medium business (20 - 50 employees): Hybrid is almost essential.

Most SMEs will see savings by using a hybrid solution.

30-Day Backup Improvement Checklist

Week 1: To evaluate	Week 2: To strengthen	Week 3: To test	Week 4: To formalise
• Evaluate existing backup process • Check the last successful backup • Find out what systems are backed up • Investigate the retention policy	• Add 2FA to the backup user's credentials • Make an off-site copy of the data • Encrypt data on local drives	• Restore one file from backup • Restore one folder from backup • File a report of how long it took to restore	• Write a backup policy • Assign roles and responsibilities for recovery • Schedule tests at least every 3 months • Review the additional coverage needed for cyber insurance

Common SME Backup Mistakes

- “We think it is backing up”
- No testing of how to restore data
- Only one copy of backup
- Backup is beside the server
- No encryption of backups
- No documentation of backup process

FAQ

1. Can I expect my cloud backups to be secure?

They will be secure if properly set up with encryption and multi-factor authentication (MFA).

2. Are on-site backups no longer necessary?

No, on-site backups still play an important role for quick restores.

3. There is such a thing as “immutable backups,” right?

An immutable backup is a backup that cannot be changed or deleted for a specified duration.

4. How frequently do we need to perform backup operations?

Backups must be completed as least every day, and more frequently for critical systems.

5. Do we need to maintain both cloud and on-site backups?

Most small to medium sized companies will need both types of backups.

6. We only use Microsoft 365, do we still need a backup solution?

Yes, you need a separate backup solution.

7. How often should we conduct “restore tests”?

At least every 90 days.

8. What is the biggest risk associated with backup solutions?

Using only one backup copy.

9. Is backup required for cyber insurance?

Yes, and the backups must be tested.

10. What is the retention period for backups?

Typically a minimum of 30-90 days, with a longer retention period for regulated industries.

About This Guide

This resource was developed by **Computer Support Centre,** an IT and security consultancy in the UK with 15 years of experience working with SMEs. We assist clients from a variety of sectors create practical and cost-effective methods for backing up data and recovering from disaster that will comply with their operational needs.

It is important to us that this guide presents easy-to-understand, plain English information to help business owners and managers without technical backgrounds feel confident when choosing how to protect their company’s data. All of the recommendations made in this guide are based on first-hand experience providing assistance to SMEs improving their resiliency, meeting compliance requirements, and reducing costs by implementing backup and recovery best practices that are not overly complicated or overly expensive.

If you learn more about **Computer Support Centre**, our services, and our approach, please visit
our official website:
□ **https://computersupportcentre.com**

Conclusion

It isn't about picking sides between cloud and cloudless; it's about your level of risk, how fast you can recover if something goes wrong, and whether you can keep your business running for many years or just for a few weeks. The majority of small-to-medium-size UK businesses will find that the best option is not "either/or" but an integrated hybrid approach that offers both local and remote protection. Your primary goal should be to have consistency. To do this, you'll want to have backup jobs set on auto, backups tested on a regular basis, clearly defined retention periods for your backups, and compliance with the UK GDPR as well as the guidance provided by the ICO (Information Commissioner's Office). Assume that you haven't tested your backups, because if you haven't, they won't be an assumption at all.

A well-structured backup plan will decrease the amount of time a business will be down, help maintain trust with customers, and increase the business's resistance to hardware failures, human errors, ransomware and viruses. Backups do not only belong to the IT department; they are an essential part of managing your business responsibly by 2026.