# 7 Cloud Storage Best Practices

## 1. Assess Your Current Cloud Risk Posture

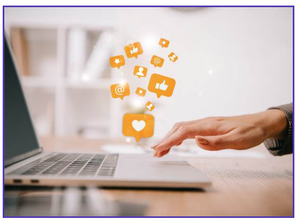
Before you can build resilience, you need to assess your existing risks. How is your data structured? Who has access? Do you know what's backed up and what's not? Take time to audit your storage setup. Review how permissions are granted and whether former employees or vendors still have access.

## 2. Implement a Layered Security Strategy

Cloud resilience requires multiple layers: access controls, encryption, monitoring, and response planning. Start by limiting access through role-based permissions. Every user should only see what's necessary for their job. Then, you can apply encryption at rest and in transit so your data isn't exposed even if systems are breached.

## 3. Embrace Redundancy Without Duplication

Resilience doesn't mean saving every file twice in the same folder. It means building a structure where critical data exists in multiple secure locations and is recoverable quickly. Use automated backup schedules that send data to geographically distributed regions. This ensures your data stays safe even if a regional cloud server fails.



## 4. Optimize for Business Continuity

You need a plan when disaster strikes (whether it's ransomware, system failure, or human error). Cloud resilience depends on your storage system's clear business continuity strategy. Outline which data is mission-critical and how quickly it must be restored.

## 5. Align with Compliance and Legal Requirements

Check if your cloud provider meets the legal standards for your industry. They should be able to show you documentation proving they follow the rules. You'll also need clear policies about how long you keep files and when you delete them. Please keep track of who accesses your files and when they do it.

## 6. Train Your Team (They're the Front Line)

Your security is only as strong as your weakest link, and that's usually human error. Even the best cloud setup won't protect you if someone on your team accidentally shares sensitive files or falls for a phishing email. Set clear rules about sharing files, creating passwords, and using devices for work.

## 7. Regularly Audit and Improve

Cloud resilience isn't one-and-done. Threats evolve, and your business changes and storage tools get updated. Schedule regular audits to verify that your backups are running, your access controls are current, and your policies are still relevant.

ProClient

Presented by:
ProClient.com