LEARNING MADE EASY

5 Essentials to Google Cloud Backup and Recovery

It's a big decision for your organization to store its data with Google Cloud. You'll reap a lot of advantages by doing so — some of which include lower capital costs, scalability, and agility. But it also comes with risks — the biggest being simply keeping your data safe.

Keep these five essentials in mind and you'll have no problem making smart decisions about how to safeguard your cloud data.

☐ Know who's responsible for your data

It's natural to think that any of your organization's data that's in Google Cloud is automatically protected with backups, snapshots, and data redundancy. But that's not necessarily the case.

Google Cloud runs on a shared responsibility matrix, which means that Google is responsible for its data centers, operating systems, servers, and the OS virtualization layer that hosts your VM and other cloud resources. You're responsible for everything you deploy in the cloud — including apps, accounts, settings, and your data.

☐ Understand the risks that come with the cloud

Additional risks fall into four categories: 1) the Google Cloud infrastructure — although this one is pretty low risk; Google estimates there is just a 0.000000001% chance that you could lose data permanently due to a problem with its infrastructure — 2) cloud configuration (your cloud resources are set up and configured correctly), 3) on-premises (your network, encryption keys, and employees), and 4) accidents (user error, script error, or misconfigured Google Cloud processes)

☐ Plan for high availability

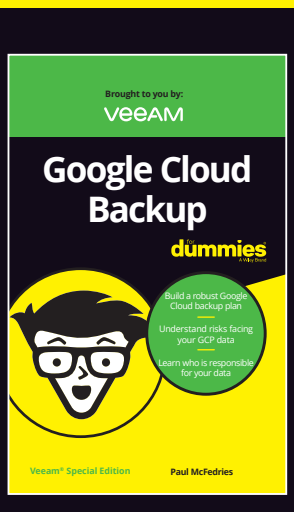
High availability refers to the ability of a cloud resource to remain functional and responsive despite the failure of one or more of its components or dependencies. Google Cloud ensures high availability by storing data in a dual-regional or multi-regional bucket location, which makes the data geo-redundant — the data is replicated in two (or more) geographic areas that are separated by at least 100 miles (160 kilometers). Google Cloud also offers bucket retention, object holds, and object versions to minimize data loss.

☐ Create a backup plan

Disasters happen, but you can get back and running faster with a backup and recovery plan. You'll want to set your recovery time objective (how long it's acceptable to be offline) and recovery point objective (how long it's acceptable for data to be temporarily lost). The faster you want your data storage to recover — that is, the lower the RTP and RPO times — the more expensive it is to store the data.

☐ Future proof your data

If you're serious about cloud data security then here are a few more best practices to consider: automate your backups, encrypt your data, create multiple backups in multitple places, use a firewall, revoke access when it's not needed, patch what you can, and watch your backup costs.



To learn more about backing up and the recovery of your data in Google Cloud, try *Google Cloud Backup For Dummies, Veeam Special Edition*.

READ THE E-BOOK

VEEAM

for dummies®
A Wiley Brand

For Dummies is a registered trademark of John Wiley & Sons, Inc. VEEAM is a trademark or registered trademark of Veeam. All other trademark are the property of their respective owners.

Wiley part no.: 978-1-119-91375-7