Google Cloud

# Disaster recovery planning in Google Cloud: Implement a DRP

So far, you've learned that recovery is important as a final resource, and your last line of defense is the Disaster Recovery Plan (DRP). You've also learned that as a cloud security professional, you and your team need to build and manage a cloud-hosted DRP. The DRP needs to outline the steps your team needs to follow to recover critical cloud resources and define Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

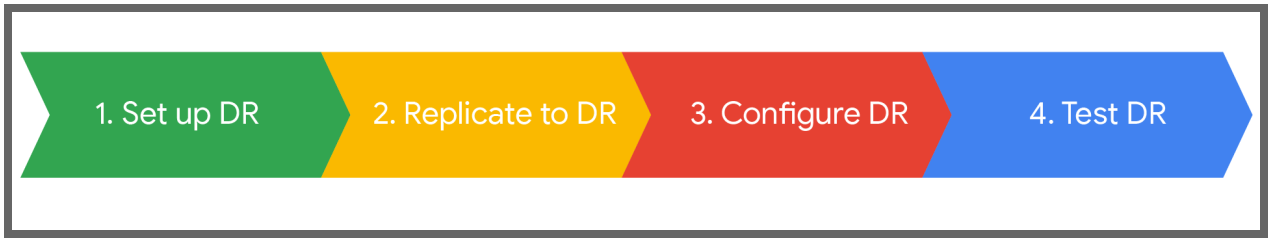
In this reading, you'll learn more about Google Cloud services and tools you can use to implement a DRP and best practices for monitoring and maintaining a DRP. You'll also get an example of an effective DRP in action.

## How to access a cloud-based DRP

You typically access a cloud-based DRP through a web browser or a dedicated client application. The specific access method will vary depending on the DRP solution that you're using.

## Steps to implement a DRP

Once you've designed your DRP, follow these steps to implement it:




1. **Set up your DR environment:** Create the necessary Google Cloud resources like virtual machines, storage, and networking.
2. **Replicate your data and workloads to your DR environment:** Use a variety of Google Cloud services and tools like Cloud Spanner, Cloud Storage, Cloud Backup and DR, and Cloud Interconnect.
3. **Configure your DR environment:** Configure your DR environment to meet your specific requirements like availability, performance, and security.

4. **Test your DR plan regularly:** Try to identify any problems with your DR plan and make sure that it's working as you expect it to.

**Pro tip**: You can use Cloud Functions to automate tasks like triggering your DRP in the event of a disaster. This will help you reduce the risk of human error and ensure that your DRP is executed quickly and efficiently.

## Best practices for monitoring and maintaining a DRP

Here are some best practices for monitoring and maintaining a DRP in Google Cloud:

- **Use a layered approach:** A layered approach to a DRP involves implementing multiple layers of protection, including data replication, application failover, and site failover. This will help you ensure that your applications and data are protected from a variety of disasters.
- **Use a managed service:** Google Cloud offers a variety of managed services that can help you build and implement your DRP. Managed services can save you time and effort, and they can help you ensure that your DRP is secure and compliant.
- **Automate your DRP:** You can use Google Cloud's automation tools to automate your DRP tasks. This will help you reduce the risk of human error and ensure that your DRP is implemented consistently.
- **Involve key stakeholders:** It's important to involve key stakeholders, like business leaders, IT staff, and security staff, in the development and implementation of your DRP. This will help ensure that your DRP meets the needs of the business and that it's aligned with your organization's overall security posture
- **Test your DRP regularly:** You need to make sure that your DRP is working as you expect it to. You should test your DRP at least once a quarter—or three months—and more often if you've made any changes to your applications or workloads.

**Pro tip:** It's important to have an offline copy in a different location of your DRP in case the internet fails or a fire occurs. This will ensure that you can still access your DRP and execute it in the event of a disaster. You can store a copy of your DRP offline on a local device, or as a printed copy in a secure location, like a fireproof safe or a cloud storage account.

## Example of an effective DRP in action

Now consider an example: A company has a DRP in place for its Google Cloud-based database. The DRP includes these steps:

1. **Identify the threat:** The company receives an alert that its database is under attack.

2. **Isolate the affected system:** The company isolates the database from the network to prevent the attack from spreading.
3. **Restore the database from the DR site:** The company restores the database from the DR site, which is a replica of the production database.
4. **Test the restored database:** The company tests the restored database to ensure that it's working properly.
5. **Switch traffic to the restored database:** The company switches traffic to the restored database so that users can resume using the application.

**Pro tip:** It's important to communicate your DRP to all relevant stakeholders, including employees, customers, and vendors. This will help ensure that everyone knows what to do in the event of a disaster.

## Key takeaways

When designing a DRP, it's important to implement a DRP that meets your business' needs. Once you've implemented your DRP, it's important to monitor and maintain it on a regular basis. You'll also need to test your DRP regularly to ensure that it's still working as you expect it to.

## Resources for more information

For more information on DRP in Google Cloud, please visit these resources:

- Devops provides a list of cloud disaster recovery best practices
- Google Cloud provides guidelines on disaster recovery for data
- The Google Cloud Backup and DR Service documentation provides guidelines and support
- Google Cloud's Disaster Recovery Planning Guide discusses DR in Google Cloud
- TechTarget provides a comprehensive cloud disaster recovery definition