



1

Identify the different backup methods.

2

Define the scope of your work.

3

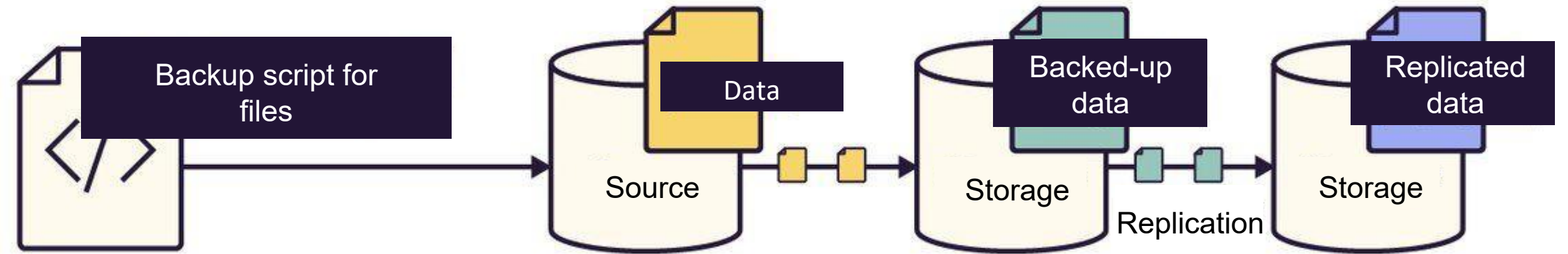
Select the appropriate backup media.

4

Integrate security measures into your backup plan.

5

Deploy your backup tools.



Best Practices 👍

- ✅ Perform regular backups to ensure data continuity.
- ✅ Test backups frequently to confirm their reliability.
- ✅ Adapt your backup methods to your specific needs.
- ✅ Use a variety of media, such as hard drives, SSDs, and cloud storage.
- ✅ Develop a backup policy that clearly defines your strategies.
- ✅ Classify data by its criticality level to guide your backup strategy.
- ✅ Encrypt backups to protect them from unauthorized access.
- ✅ Integrate backups into the BCP/DRP to ensure business continuity.

Common Mistakes 🙅

- ❌ Forgetting to test backups.
- ❌ Failing to consider storage capacity.
- ❌ Ignoring security updates.
- ❌ Choosing unsuitable backup media.
- ❌ Leaving backups unencrypted.
- ❌ Underestimating the importance of data classification.
- ❌ Risking data loss due to a lack of backup storage diversity.
- ❌ Ignoring ANSSI/CNIL recommendations.

Definitions 🔍

Backup

A computer backup is a copy of data stored on a separate medium so it can be restored in the event of loss or corruption of the original data.

IT Backup Plan

An IT backup plan is a detailed strategy for copying, storing, and restoring digital data to prevent data loss in the event of an incident.

3-2-1-1-0 Strategy

The 3-2-1-1-0 strategy means maintaining 3 copies of your data on 2 different types of media, with 1 copy stored off-site, 1 stored offline, and 0 errors during restoration.