

Backup-as-a-Service Solution Migration Checklist

You're migrating to a new managed backup solution.

Whether your existing backup platform lacks the support, speed, or flexibility you require, or whether you've simply outgrown it, sometimes change is necessary. Your goal in this process is to protect critical data throughout the process of migrating your customers over to a new backup solution. To navigate this transition, this checklist outlines key steps that help ensure a smooth process. Our goal is to help you fulfill all the capability that your new backup solution has to offer.

↳ Backup Administrator

↳ Project Name

↳ Project Start Date

↳ Projection Completion Date



Review Customer Backup Strategies

It's critical to create a cohesive plan for transitioning clients to the new backup solution. Often important lessons are learned from your early adopters that can be applied throughout the entire client migration process.

- Document RTO for each customer to be considered successfully restored.
- Document RPO for each customer to be considered successfully restored.
- Review job types currently being utilized by each customer for restore (full, differential, incremental, image, continuous, virtual, etc) and consider any necessary changes.
- Identify and document industry compliance requirements for each customer.
- Note whether client is following 3-2-1 backup rule for Cyber Insurance requirements.
- Prioritize clients to be moved to the new solution based on size and complexity.
- Verify that each customer has a restorable backup under the existing solution.
- Create or update customer Service Level Agreements to match backup objectives.



Hardware and Storage Evaluation

Now is the time to evaluate whether existing storage hardware is sufficient to meet current and future backup needs for both you and your customers.

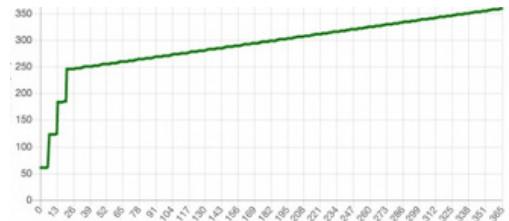
- Calculate customer backup data storage requirements for the next several years.
- Determine bandwidth required for client to make a full data transfer to the cloud.
- Document the life-cycle stage of your own on-site data storage devices.
- Identify slowest storage devices and bandwidth points for potential bottlenecks.

Example: 3 Servers with 20GB backup data each, and 200MB new data per week over one 1 year.

Total current data: **60 GB**

Total data size after 1 year: **90.55 GB**

Backup storage space requirements during year 1: **359.82 GB**



There are tools available to help calculate backup time, storage, and bandwidth requirements. Visit www.BackupCalculator.com for a more complete understanding of future needs.



Data Archival

Customers must define business data as either archival or production recovery data. Data is then assigned to storage targets based on access requirements.

- Identify all data that has been accessed in the last 30-days for each customer.
- Verify that clients have production and archival data targeting appropriate storage.
- Consider regulatory requirements for archival data (format, location, encryption, etc).
- If client backups are locked in a proprietary format, consider pooling them into a central archive.

Common Regulatory Data Retention Specifications

HIPAA: Compliance documents should be retained for a minimum of six years, while medical record retention is mandated at the state level.

CCPA/CPRA: No set retention minimum but a maximum retention period must be created to avoid holding personal data indefinitely.

PCI DSS: Cardholder data storage must be minimized to only what is required for business or legal use.



Migration Planning

With a clear understanding of data retention requirements and how archived data will be maintained moving forward, we can now detail the specifics of your transition to a new solution.

- Decide upon either a plunge, parallel, or phased implementation of backup systems.
- Create a visual timeline that details when databases and applications will be backed up from the new system.
- Determine specific media and formats data will be stored on following the migration.
- Map migration groups to new storage destinations and document process.
- Build scenarios of how migration could affect downtime within your schedule.
- Create fall-back plan to return to legacy backup system in the event that the switch-over fails.



Testing and Training

Lack of adequate training and preparation is the most cited reason for a backup migration failure. From system administrators to general employees - all must take steps to ensure a smooth transition.

- Administrators have tested and achieved comfortability with new backup solution.
- Documented prior backup jobs / policies / client configurations as a cross-reference.
- Conduct internal trainings to roll-out new backup protocols and procedures.
- Notify clients of upcoming benefits and requirements associated with new solution.
- Perform data restore testing across all storage destinations to identify possible performance bottlenecks.
- Build a backup restore-test-schedule, listing all business assets and the frequency in which restore tests must take place (weekly, monthly, bi-monthly, quarterly, annually).



PRO TIP: Request a direct line to your backup vendor support staff who can offer additional insight regarding testing, training and customer on-boarding prior to purchase.



Migrate a Data Segment

Performing a migration of a less critical business asset can offer valuable insight into your workflow for additional backup migration.

- Restore any legacy archived data as needed to temporary storage.
- Prepare migration group (objective, timeline, new backup process).
- Perform final backup(s) using legacy backup system.
- Perform backup with new solution and test restore.
- Verify that encryption levels and data retention meets audit requirements.
- Document migration process and new backup routine.
- Decommission legacy backup and workflows for this segment (if applicable).



Distribute Information



Communicating information about your progress, new procedures, and who to contact in a data emergency, is an important part of completing your backup migration.

- Build a new disaster recovery action plan for a data breach scenario.
- Hand over documentation / instructions to emergency response team.
- Review whether migration objectives have been met.
- Send final organizational announcements about backup migration completion.

Final Thoughts

Migrating yourself and your clients to a new managed backup solution is a complex process that will vary based on your environment. The NovaBACKUP team works closely with MSPs to help provide the smoothest possible transition. [Schedule a call](#) with one of our data protection experts for assistance with your backup migration today.



 NovaBACKUP
 29209 Canwood Street
 Agoura Hills, California 91301
 Tel.: (805) 579-6700
 Fax: (805) 579-6710
 Monday-Friday 9AM-5PM Pacific Time

SCHEDULE A CALL

Visit novabackup.com to schedule a call with a US-based backup expert.

ASK US ABOUT BACKUP

Email us at [msp@novabackup.com](mailto:mSP@novabackup.com)