Salesforce Backup & Restore Partner Checklist

CapStorm

Below you'll find 25 key features and considerations you can use to help in your search for a Salesforce backup and restore partner.

Backup Checklist

Process to validate that backup is complete	YES ☐	NO ☐
Limits on data types included in backup (common problematic data includes Knowledge (versions), images, BigObjects, Files	YES ☐	NO ☐
Limits on metadata types included in the backup (common exclusions include profiles, apex classes, triggers, flows)	YES ☐	NO ☐
Backup Frequency	YES ☐	NO ☐
Full or Incremental Backups , or both	YES ☐	NO ☐
Process to access the backup data	YES ☐	NO ☐
Length of backup retention	YES ☐	NO ☐
Length of point-in-time data snapshot retention	YES ☐	NO ☐
API Use - Ensure solution aligns with your rolling 24 hour limit	YES ☐	NO ☐
Backup accessibility for additional business purposes	YES ☐	NO ☐

Restore Checklist

Ease of use of Production Restore	YES ☐	NO ☐
Sandbox Seeding for production restore testing	YES ☐	NO ☐
Limits on data relationships / hierarchies	YES ☐	NO ☐
Point-in-time data restore	YES ☐	NO ☐
Limits on data types available for restore	YES ☐	NO ☐
Limits on restore of data in managed packages	YES ☐	NO ☐
Limits on metadata types available for restore	YES ☐	NO ☐
Ability to turn off SFDC validation, flows, triggers etc	YES ☐	NO ☐
Pre-restore data validation to ensure that only needed data is restored	YES ☐	NO ☐
Restore speed to meet RPO and RTO objectives	YES ☐	NO ☐

Beyond the Basics - Compliance

Data security and access controls - critical when selecting a SaaS approach (How do you know that nobody has accessed your data!)	YES ☐	NO ☐
Data masking of obfuscation with Restore	YES ☐	NO ☐
Data encryption at rest- either 'whole database' or 'field level'	YES ☐	NO ☐
Compatibility with compliance regulations like GDPR or geographic data retention requirements	YES ☐	NO ☐
Process to migrate to a new vendor if your selected vendor goes out of business	YES ☐	NO ☐

Learn more about CapStorm's capabilities at www.capstorm.com