

DATA BACKUP STRATEGY ASSESSMENT: A COMPREHENSIVE CHECKLIST

The Top 14 Areas of Your Backup and Recovery Strategy
You Should Evaluate

One-third of businesses haven't evaluated their [backup and recovery strategy](#) in the last six months. However, a proactive and regular evaluation of your backup and recovery strategy is essential to adapt to technological advancements, security threats, and a dynamic and frequently changing data environment.

To help you get started, here's a checklist of what to consider when evaluating your current backup and recovery strategy.

Data Assessment

✓ Identify Critical Data

List and prioritize data based on its criticalness to business operations. Business data is dynamic and constantly changing. As new data is created, old data may become less relevant. Your backup strategy needs to adapt to these changes to ensure that the most critical data is backed up and can be recovered when needed.

✓ Classify Your Data

By classifying your data into sensitive and non-sensitive categories, you can prioritize the backup and recovery of sensitive data—such as personally identifiable information (PII)—to help ensure compliance with any industry or government regulations. This also helps provide tailored security measures—such as encryption and access controls—to reduce the risk associated with data loss or unauthorized access of your most sensitive data.

Backup Procedures

✓ Assess the Frequency of Backups

When considering how often data backup is required, take into consideration your recovery point object (RPO), how critical the data is to business operations, the rate at which data changes within your organization, whether certain processes or workflows are time-sensitive, recovery time objective (RTO), and storage and capacity costs. Then, assess whether the frequency of backups for each category of data (e.g., daily, weekly, real-time) is still appropriate.

✓ Determine When to Use Full or Incremental Backups

The choice between full and incremental backups should align with your organization's specific needs, including RTOs, storage and network constraints, and operational considerations. In many cases, a combination of both full and incremental backups—known as differential backups—may provide the most balanced approach.

✓ Assess Your Backup Location Strategy

Data can be backed up in a number of ways, including on-premises servers, external hard drives, network attached storage (NAS) devices, tape drives/libraries, remote data centers, or in the cloud (which can include hybrid cloud solutions or distributed/multi-cloud storage). Off-site backup service providers or remote offices are also options for organizations with multiple locations. When deciding on backup locations, it's important to conduct a thorough risk assessment and consider factors such as data sensitivity, compliance requirements, recovery objectives, and overall infrastructure and budget constraints. A well-designed backup strategy often involves a combination of locations.

Data Retention and Archiving

✓ Implement Retention Policies

A thorough assessment of retention policies is important to ensure alignment with compliance requirements and good data governance. Well-defined retention policies enhance operational efficiency by streamlining backup processes, balancing business needs regarding data relevance, and contributing to legal preparedness in case of audits or litigation. Retention policies can also help optimize resources and minimize data exposure.

✓ Evaluate Archiving Procedures

A holistic evaluation of archiving procedures should include an assessment of the format and compatibility of archived data, migration strategies for evolving technology, and thorough documentation with regular audits. Additionally, be sure to establish procedures for data verification and integrity.

Security and Compliance

✓ Maintain Robust Security Measures

Ensuring you have the right security measures in place is critical. Start by evaluating and confirming the presence of robust encryption protocols to safeguard data during both transmission and storage. In addition, assess access controls to ensure that only authorized personnel have the necessary privileges.

✓ Compliance

Confirmation that the backup strategy aligns with specific compliance requirements—such as GDPR, HIPAA, or other industry-specific regulations—is essential. The evaluation process should also include an assessment of audit trail capabilities, as they are also crucial for regulatory compliance, internal governance, and post-incident analysis.

Documentation and Monitoring

✓ Documentation and Training

Comprehensive documentation of backup and recovery procedures is crucial for reference, knowledge transfer, and troubleshooting. Regular training sessions also contribute to skill development, ensuring that staff members are proficient in operating monitoring tools and responding effectively to any alerts or data loss incidents.

✓ Monitoring and Reporting

By regularly assessing the capabilities of monitoring tools, you can proactively identify and address potential issues, ensuring the reliability and efficiency of your data protection tools. Consider whether your monitoring tools provide robust alerts and automated reporting, as this can eliminate the need to log into systems daily and ensure issues are quickly addressed.

Future-proofing

✓ Scalability and Flexibility

Evaluating your backup and recovery strategy for scalability and flexibility involves examining whether the backup infrastructure can effectively grow in tandem with the increasing volume of data generated by the organization. This is essential for avoiding disruptions, optimizing resource allocation, and maintaining the efficiency of backup operations as data volumes expand.

✓ Testing and Validation

Scheduling and conducting routine tests to validate the effectiveness of your backup and recovery process is a critical component of a comprehensive backup and recovery strategy. Regular testing helps identify potential weaknesses, finetune procedures, and ensure the readiness of your system to swiftly recover critical data in the event of an actual data loss incident.

✓ Review and Continuous Improvement

Periodic reviews ensure that your backup strategy remains aligned with evolving business needs, technological advancements, and changing data landscapes. In addition, gathering insights from end users and IT personnel provides valuable input for refining your backup and recovery processes. This feedback loop contributes to a culture of continuous improvements and allows you to address user concerns, enhance usability, and adapt the backup strategy based on real-world experiences.



Need help evaluating your backup and recovery strategy?

Reach out to your Connection Account Team for more information.

Business Solutions
1.800.800.0014

Enterprise Solutions
1.800.369.1047

www.connection.com/BackupRecovery