Data Backup Integrity Self Audit Checklist

My Company Manages its Own Backups

1. There is a single person in our organization who is ultimately responsible for the execution of our backup and disaster recovery plan. Yes___No___
2. The success or failure of the backup system is monitored daily. Yes___No___
3. Backup selections have been verified for inclusiveness in the last 90 days. Yes___No___
4. Backup frequency is at least daily for critical data sets. Yes___No___
5. Our backup system meets all applicable regulatory requirements. Yes___No___
6. If any of our critical devices holding data fail, the maximum downtime would not exceed X. (X= our acceptable level of downtime. This varies from organization to organization, but is typically measured in hours for small businesses that do not provide electronic data as a service to their clients.) Yes___No___
7. The location(s) where backed up data is stored (i.e. on a local backup server and in a secure offsite data center). Yes___No___
8. We verify the integrity of the backup sets on a regular basis (typically through a test restore process) to ensure they are valid. Yes___No___
9. Our data is encrypted before any offsite transfers occur. Yes___No___

A Managed Service Provider (MSP) Manages Our Backups

My MSP is able to confirm and provide the following in writing:

1. Monitoring is completed daily. Yes___No___. If Yes, by whom? _____
2. A detailed list of the specific data being backed up has been provided to you and you understand it and know that it is complete. Yes___No___
3. Backup frequency is at least daily for critical data sets. Yes___No___
4. The MSP's backup system meets all applicable regulatory requirements. Yes___No___
5. If any of our critical devices holding data fail, the maximum downtime would not exceed X. (X= our acceptable level of downtime. This varies from organization to organization, but is typically measured in hours for small businesses that do not provide electronic data as a service to their clients.) Yes___No___
6. The location(s) where backed up data is stored (i.e. on a local backup server and in a secure offsite data center). Yes___No___
7. Integrity testing is performed regularly against the backed up data. Yes___No.___
8. Confirmation that data is encrypted before any offsite transfers occur. Yes___No___

If you answered "No" or are unsure of the answer to any of these questions, your data may be at risk. Contact GreenLoop today for a free Risk Profile Analysis. Phone: 1-888-877-4395