Business Continuity Checklist

What is currently covered by your continuity systems and plans? Check all that apply:

- ☐ Mission-critical applications only
- ☐ All other applications regardless of priority
- ☐ Essential data only
- ☐ Non-essential data and essential data

What's your current method of business continuity?

- ☐ Replication of files between two SANs (on-prem mirror image) with onsite recovery management application to manage the instances (warm standby with no load balancing)
- ☐ Multiple redundant data centers / tape restoration (hot standby / load balanced)
- ☐ Cloud applications (i.e. Azure Backup and Site Recovery) — (hot standby in the cloud, no load balancing)

How many vendors do you manage for your continuity environment?

Software vendors: _____

Hardware vendors: _____

We recommend 3 or fewer. A Microsoft cloud environment can bring you down to one supplier and eliminate hardware needs.

Do you need to coordinate with all departments and persons to fail over?

- ☐ IT Department
- ☐ Telecom provider
- ☐ Data center

How easy is it to add protected instances to your disaster recovery?

Last time protected instances were added: _____

Can you easily change your continuity plan?

- ☐ Can you upgrade components of your continuity infrastructure?
- ☐ Do you have to rebuild the whole thing to update pieces?

Rebuilding is expensive and should not be necessary.

Is your team running patches and updates on your disaster recovery at least every month?

☐ Yes ☐ No

What is your current outage window? _____

Newer cloud-based models negate the need for this.

What is the end of life for all hardware related to your current disaster recovery solution?

_____

Have you done a full failover test in the last 12 months? _____

Jot down any notes about what was problematic, you will want to address this.