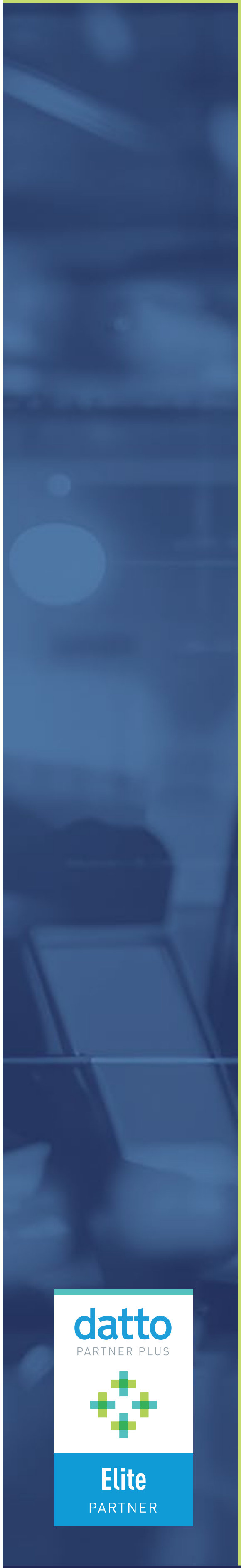
The Ultimate Disaster Recovery Checklist

Stay One Step Ahead of Potential Disasters

datto
PARTNER PLUS
Elite
PARTNER

Ascend
TECHNOLOGIES



datto
PARTNER PLUS
Elite
PARTNER

Prepare yourself before disaster strikes.

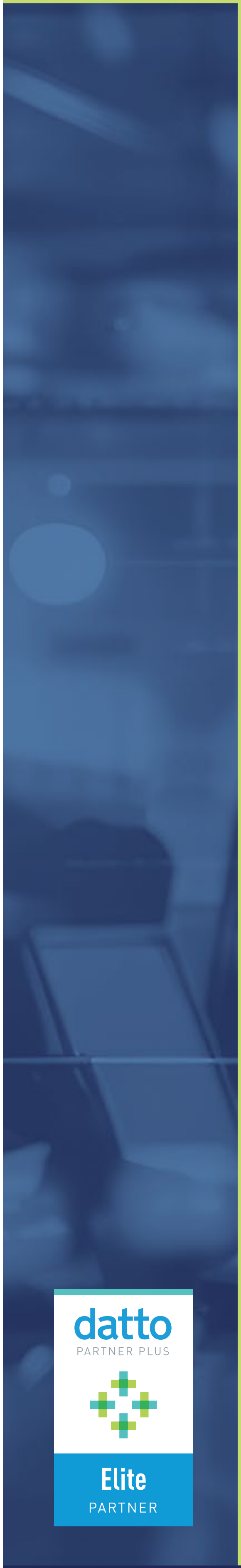
When it comes to data backup and disaster recovery, being prepared for potential disasters is key to keep your business running.

It's not only important to have a disaster recovery solution you trust, but to make sure you test it as well.

Keep this disaster recovery checklist on hand.

Prior to a disaster ever occurring (and unfortunately it's a matter of when and not if) ask yourself the following:

- Do you have a disaster recovery solution in place?
- Do you trust it?
- When was the last time your backup was tested?
- How long does it take to recover from your current backup solution?
- How long can you realistically be down? 1 hour? 1 day?
- What is the financial cost of downtime to your business?
- When a disaster occurs, is there an offsite copy?



The disaster moment has occurred — time to walk through the following steps:

1. Assess the problem and its impact on your business

Every disaster is different. Before doing anything, understand the underlying issue and how it may affect you.

- Is the issue local to one machine, or does it affect your entire system?
- Have files been deleted or are servers/workstations down?

2. Establish recovery goals

Recovery is what makes a disaster recovery solution different from a simple backup product. Plan out your road to recovery.

- Do you need to restore the system, the data, or both? Should time be spent recovering files and folders before system recovery?
- Have you identifed critical systems and prioritize recovery tasks?
- What date/time should you recover from?
- How long can your recovery take?

3. Select the appropriate recovery type(s)

To get to your “road to recovery”, the appropriate recovery procedure must be followed. Think about which approach will best get you to your end goal.

- **File restore** - Recovering specific files lost, corrupted, or deleted during an incident, ensuring quick access to critical data without requiring a full system restoration. It offers granularity, speed, and flexibility, supporting recovery from various backup sources while enabling versioning & secure access to maintain data integrity.
- **Local virtualization** - Enables rapid recovery by running virtualized versions of systems on local hardware, ensuring minimal downtime during incidents. It is cost-effective, flexible, & allows businesses to maintain operations while physical systems are repaired or restored.
- **Off-site virtualization** - Uses remote virtualized systems to maintain business operations when local infrastructure is compromised. It ensures geographic redundancy, scalability, and secure remote access, protecting critical systems from disruptions like natural disasters or cyberattacks.

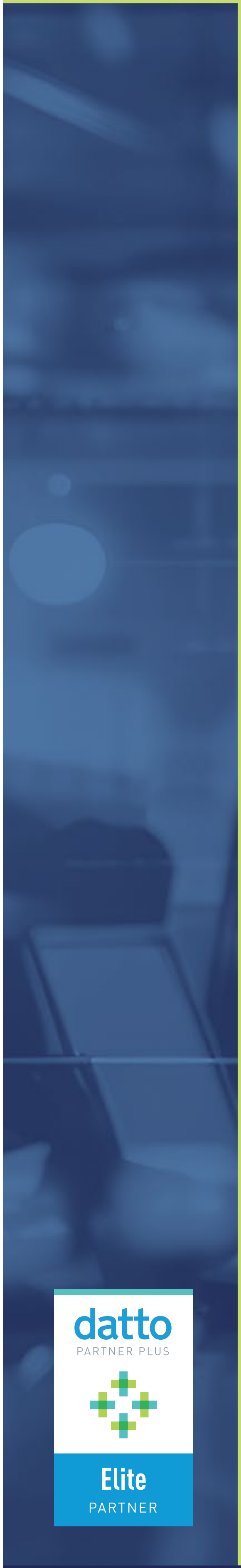
4. Verify the recovery and confirm functionality with users

Once a recovery is verified, confirm that it interacts positively with users.

- Test network connectivity
- Ensure all users can access resources and applications in the virtual environment

5. Restore the original system(s), if needed

If the original system(s) needs to be restored, decide which restoration process will work best.



- **Bare metal restore** - Process that reinstates an entire system—operating system, applications, and data—onto blank (bare metal) hardware or virtual machines. It ensures comprehensive recovery after major failures, supports restoration to different hardware, and minimizes downtime by automating system setup.
- **Virtual machine restore** - A process that reinstates a virtual machine to its operational state using backups or snapshots, ensuring quick recovery with minimal downtime. It provides flexibility to restore VMs to the same or different infrastructure and uses snapshots for targeted recovery to specific points in time.

6. Self-assess afterwards

After it's all said and done, take a step back and think about it: How well did your team do? What could you have done differently?

- What precipitated the failure?
- What ongoing issues need to addressed?
- What can be done better in future disaster recovery scenarios?