

CONTINUITY WORKSHEET

Disaster Recovery Readiness Worksheet

Most businesses discover their backup does not work on the day they need it. This worksheet walks you through proving yours does - before it matters.

01	Calculate your real recovery time and data-loss tolerance
02	The restore test almost nobody runs (and how to run it)
03	A one-page continuity plan your team can follow

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology

Owner-led IT, security, and compliance support.

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

☐ Critical services are ranked by business impact, not technical preference.	☐ Yes ☐ Partial ☐ No
☐ Each service has an approved recovery time objective (RTO).	☐ Yes ☐ Partial ☐ No
☐ Each data set has an approved recovery point objective (RPO).	☐ Yes ☐ Partial ☐ No
☐ Dependencies include identity, DNS, internet, power, vendors, devices, and people.	☐ Yes ☐ Partial ☐ No
☐ Backup jobs are monitored and failures create owned tickets.	☐ Yes ☐ Partial ☐ No
☐ At least one backup copy is isolated or immutable from production credentials.	☐ Yes ☐ Partial ☐ No
☐ Cloud applications are covered by explicit backup and retention decisions.	☐ Yes ☐ Partial ☐ No
☐ Recovery credentials and runbooks are accessible when normal systems are down.	☐ Yes ☐ Partial ☐ No
☐ A restore test has proven application usability, not just file extraction.	☐ Yes ☐ Partial ☐ No
☐ The plan includes alternate communication when email and phones are unavailable.	☐ Yes ☐ Partial ☐ No
☐ Vendors, cyber insurer, legal counsel, and leadership contacts are current.	☐ Yes ☐ Partial ☐ No
☐ The last exercise produced corrective actions with owners and due dates.	☐ Yes ☐ Partial ☐ No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

Calculate the tolerance the business can actually afford

RTO is the maximum acceptable time to restore a service. RPO is the maximum acceptable amount of data loss measured backward from the incident.

Service / data	RTO	RPO
Identity and sign-in	___ hours	___ minutes / hours
Email and collaboration	___ hours	___ minutes / hours
Core line-of-business app	___ hours	___ minutes / hours
Shared files / records	___ hours	___ minutes / hours
Phones / contact center	___ hours	___ minutes / hours
Website / customer portal	___ hours	___ minutes / hours
Finance / payroll	___ hours	___ minutes / hours

Reality check: recovery time includes detection, decision, access, data transfer, repair, validation, and user communication - not just the restore job.

Run the restore test most teams skip

A successful backup notification proves a job ran. A restore exercise proves the business can work again.

1	Choose a representative service and define success: users can sign in, open records, create a transaction, and produce an expected output.
2	Restore into an isolated environment using only the documented runbook and emergency credentials.
3	Record start time, data point recovered, errors, missing dependencies, and total validation time.
4	Have a business user validate the restored application and data rather than relying only on IT.
5	Update the one-page continuity plan: incident lead, alternate communications, workarounds, vendor contacts, restore order, and next test date.

What to watch for

WATCH: The only test is opening one file from a backup.

WATCH: The runbook is stored only inside the system it is meant to recover.

WATCH: Production administrator credentials can delete every backup copy.

WATCH: No business user participates in validation.

WATCH: The RTO is shorter than the time required to download or rebuild the data.

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	_____
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	_____
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	_____
NEXT QUARTER	Test the process, document results, and assign improvements.	_____

Notes / decisions / questions for your provider

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.

Reference points: NIST SP 800-34 Rev. 1: csrc.nist.gov/pubs/sp/800/34/r1/final | CISA StopRansomware: cisa.gov/stopransomware

This guide is educational and is not legal, regulatory, tax, or insurance advice. Confirm requirements and pricing for your organization with qualified advisors and vendors.