Is Your Document Infrastructure Disaster-Proof?

A 10-Minute Self-Assessment

By Raymond Brooks
Co-Founder, MaxRecall Technologies

The Thing Everyone Forgets

Companies plan for disasters. They have evacuation routes, backup generators, insurance policies, and IT recovery procedures.

What they often forget: the documents.

Contracts, invoices, permits, insurance policies, payroll records, compliance documentation - the paperwork that lets a business prove, pay, rebuild, and recover. When a flood, fire, cyberattack, or hurricane hits, these documents become either strategic assets or crippling liabilities.

I've seen companies survive disasters because their documents were accessible. I've seen others struggle for months because their records were underwater, locked on destroyed servers, or scattered across inaccessible locations.

This checklist helps you assess your document disaster readiness in about 10 minutes. Answer honestly. The gaps you find now are much easier to fix than the ones you discover during an emergency.

Section 1: Do You Know What's Critical?

In a disaster, you can't recover everything at once. You need to know which documents keep the business running - and which ones can wait.

Check each box that applies:

☐	We have a documented list of critical document types (contracts, insurance policies, payroll records, permits, etc.)
☐	Critical documents are prioritized by recovery urgency (e.g., payroll = immediate, old contracts = can wait)
☐	We know exactly where each critical document type is stored (physical location, server, cloud system)
☐	Someone other than the owner/creator knows where critical documents are and how to access them

Score: ____ / 4

If you checked fewer than 3: You may not be able to prioritize recovery effectively. Start by listing your top 10 critical document types and where they live.

Section 2: Are Your Documents Backed Up?

Paper files in one location. A server in one building. A backup drive in the same office as the server. These are all single points of failure.

Check each box that applies:

☐	Critical documents exist in at least two separate physical locations
☐	Digital backups are stored in a different geographic region (not just a different building)
☐	We have tested restoring documents from backup within the last 12 months
☐	Paper-only documents have been scanned and stored digitally
☐	Backups happen automatically (not manually when someone remembers)

Score: ____ / 5

If you checked fewer than 3: You have single points of failure. A flood, fire, or ransomware attack could take out your only copy.

Section 3: Can You Access Documents Remotely?

If your building is inaccessible - flooded, evacuated, or structurally damaged - can your team still get to the documents they need to keep operations running?

Check each box that applies:

☐	Critical documents can be accessed from any location with an internet connection
☐	Key personnel can access documents from personal devices if company equipment is unavailable
☐	We have documented who has access to what, and those permissions are current
☐	Access doesn't depend on a single person (e.g., only the IT admin can grant access)

Score: ____ / 4

If you checked fewer than 3: Your operations may grind to a halt if your office is inaccessible. Consider cloud-based document access.

Section 4: Can You Actually Operate?

Access isn't enough. You need to be able to actually run payroll, pay vendors, file claims, and communicate with customers - all of which require specific documents.

Check each box that applies:

☐	We could run payroll within 48 hours of a disaster (access to payroll records, bank info, tax docs)
☐	We could file an insurance claim within 72 hours (access to policy, inventory records, photos/documentation)
☐	We could continue paying critical vendors (access to contracts, payment info, open invoices)
☐	We could communicate with customers about orders (access to customer records, order history)
☐	We could prove regulatory compliance if inspectors showed up during recovery

Score: ____ / 5

If you checked fewer than 3: You may not be able to maintain critical operations during recovery. Map out exactly which documents each function requires.

Section 5: Do Your People Know What to Do?

Technology is only part of the equation. In a crisis, people need to know who's responsible for what, where to go, and what to prioritize.

Check each box that applies:

☐	We have designated "recovery champions" who know the document systems and can act in a crisis
☐	More than one person knows how to access and retrieve critical documents
☐	Contact information for key personnel is stored somewhere accessible outside the office
☐	We have run a drill or tabletop exercise involving document recovery in the last 24 months

Score: ____ / 4

If you checked fewer than 2: You're relying on people figuring it out under pressure. Confusion and delay are almost guaranteed.

Your Total Score

Section	Your Score
1. Critical Documents	_____ / 4
2. Backup & Redundancy	_____ / 5
3. Remote Access	/ 4
4. Recovery Operations	_____ / 5
5. People & Process	/ 4
TOTAL	**_____ / 22**

What Your Score Means

18-22: Strong position. Your document infrastructure is resilient. Review annually and after any major system changes.

12-17: Moderate gaps. You have some protection, but significant vulnerabilities remain. Prioritize the sections where you scored lowest.

6-11: Significant risk. A serious disaster would likely disrupt operations for weeks or longer. Address backup and access issues first.

0-5: Critical vulnerability. Your document infrastructure is a single point of failure. This should be an urgent priority.

Quick Wins: What You Can Do This Week

You don't need to fix everything at once. Here are the highest-impact actions you can take immediately:

1. **List your top 10 critical document types.** Include insurance policies, payroll records, key contracts, permits, and compliance docs. Write down where each one lives right now.
2. **Identify your single points of failure.** Paper-only files? Server in one location? Backup drive in the same building? These are your biggest vulnerabilities.
3. **Test your backup.** Actually try to restore a document from backup. If you've never tested it, you don't know if it works.
4. **Verify remote access.** Can you access your critical documents from home right now? Try it.
5. **Designate a backup person.** Make sure at least one other person knows how to access your document systems and has the credentials to do so.

The Bottom Line

Disasters are unpredictable. Document readiness is not.

The companies that recover quickly aren't lucky - they're prepared. Their documents are backed up, accessible, and organized so that when something goes wrong, they can keep running payroll, file claims, pay vendors, and communicate with customers.

The gaps you identified in this checklist are fixable. The time to fix them is now - not during an emergency.

If you'd like help thinking through your document disaster readiness, we're happy to have that conversation.

-

MaxRecall Technologies

Business Process Automation Experts
maxrecall.com | 770-998-1400