

# The Business Impact Analysis Starter Worksheet

Six questions your leadership team can answer this week, before you spend another dollar on backup.

## WHY THIS EXISTS

### Backup is the last step, not the first.

Anyone can copy your data. Keeping your organization running through a failed server, a ransomware attack, or a building you cannot get into starts earlier than that: knowing what must not stop, deciding how you stay open, and only then building recovery to match. Most providers sell the third step first and call it protection. This worksheet is the first step.

It is not a technology exercise. It is a leadership conversation. Nothing on these pages requires you to know how a server works. It requires you to know your business, which you already do.

#### How to use it

Who: the owner or CEO, whoever runs operations, and whoever runs finance. Three people is ideal. One is fine to start.

Time: about an hour. Do not aim for perfect. Aim for honest first answers you can refine later.

Order: work the six questions in sequence. Each one builds on the last.

Then: the final page tells you what your answers mean and what to do with them, whoever your IT provider is.

**The two numbers.** Every question here feeds two decisions for each part of your business: how long you could afford to be down, and how much work you could afford to lose. Once you can say those two numbers out loud, recovery stops being a guess and becomes a decision, sized to your business and your budget. The industry calls them RTO and RPO. You can call them what they are: your tolerances.

# What must not stop?

Every business has a handful of functions that, if they stopped, would stop the business. A practice cannot see patients without scheduling and records. A manufacturer cannot ship if the shop floor and the ERP stop talking. A contractor cannot invoice. A lender cannot fund. List yours. Think in business functions first, then name the systems each one lives on.

*What this produces: your list of critical functions and the systems behind them.*

| Critical business function                  | Systems it runs on                                              | What stops if it stops                                   | Who owns it                   |
|---------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------|-------------------------------|
| <i>Example: Seeing and billing patients</i> | <i>Practice management system, email and identity, internet</i> | <i>Appointments, care, and revenue stop the same day</i> | <i>Practice administrator</i> |
|                                             |                                                                 |                                                          |                               |
|                                             |                                                                 |                                                          |                               |
|                                             |                                                                 |                                                          |                               |
|                                             |                                                                 |                                                          |                               |
|                                             |                                                                 |                                                          |                               |
|                                             |                                                                 |                                                          |                               |

**A useful test.** If you are unsure whether something belongs here, ask: would we notice within a day? If yes, it belongs. Most organizations land between four and eight functions. If you have twenty, you are listing systems, not functions.

# How long could you go without each one?

For each function from Question 1, imagine it went dark at 8 a.m. tomorrow. When does it start to hurt? When does the damage become serious: lost revenue you cannot recover, patients or customers who leave, a missed regulatory or payroll deadline? Your tolerance is the point just before serious.

What this produces: your tolerable downtime for each function. Industry term: Recovery Time Objective (RTO).

| Critical business function        | When it starts to hurt          | When it becomes serious                     | Your tolerance (circle one)            |
|-----------------------------------|---------------------------------|---------------------------------------------|----------------------------------------|
| Example: Order entry and shipping | Within 2 hours, orders queue up | By day 2, customers reroute to a competitor | Minutes / Hours / 1 day / Several days |
|                                   |                                 |                                             |                                        |
|                                   |                                 |                                             |                                        |
|                                   |                                 |                                             |                                        |
|                                   |                                 |                                             |                                        |
|                                   |                                 |                                             |                                        |
|                                   |                                 |                                             |                                        |

**Watch for this.** The instinct is to say "minutes" for everything. Minutes cost more than hours, and hours cost more than a day. Being honest here is what keeps you from paying enterprise prices for tolerances you never needed, or from discovering the opposite during an outage.

# How much work could you lose and recreate?

Downtime is one loss. Lost work is another. If a system had to be restored from last night, everything entered since then is gone. Could your team recreate a morning of work from paper, email, and memory? A full day? A week? For each function, decide how far back is acceptable.

What this produces: your acceptable data loss for each function. Industry term: Recovery Point Objective (RPO). It sets how often each system must be backed up.

| Critical business function | How fast the data changes        | Could you recreate a day of it?                  | Your tolerance (circle one)       |
|----------------------------|----------------------------------|--------------------------------------------------|-----------------------------------|
| Example: Loan processing   | Constantly during business hours | Partly. Some documents exist only in the system. | 1 hour / 4 hours / 1 day / 1 week |
|                            |                                  |                                                  |                                   |
|                            |                                  |                                                  |                                   |
|                            |                                  |                                                  |                                   |
|                            |                                  |                                                  |                                   |
|                            |                                  |                                                  |                                   |
|                            |                                  |                                                  |                                   |
|                            |                                  |                                                  |                                   |

**Why it matters.** A once-a-night backup means a bad afternoon can erase a full day of work. If that would be damaging, the answer is more frequent backups for that system specifically, not for everything. This question tells your provider where frequency actually matters.

# What does each one depend on that you do not control?

Most outages are not a server dying. They are a dependency failing: the internet connection, the phone system, the identity provider everyone signs in with, a vendor's cloud, the building, the one person who knows how something works. List the dependencies behind your critical functions and whether you have any alternative today.

What this produces: your dependency map, and the first draft of your workarounds.

| Dependency                   | Which functions need it              | Alternative if it fails?                  | Who to contact                        |
|------------------------------|--------------------------------------|-------------------------------------------|---------------------------------------|
| Example: Internet connection | Every cloud system, phones, payments | Cellular hotspots for the front desk only | Provider support line, account number |
|                              |                                      |                                           |                                       |
|                              |                                      |                                           |                                       |
|                              |                                      |                                           |                                       |
|                              |                                      |                                           |                                       |
|                              |                                      |                                           |                                       |
|                              |                                      |                                           |                                       |

**Common ones people miss:** email and sign-in (if identity is down, nothing else works), the phone system, payment processing, the building itself, a key vendor's portal, and a single employee whose knowledge is not written down anywhere.

## Who decides, and who needs to hear from you in the first hour?

When something happens, two things go wrong before any technology does: nobody is sure who is in charge, and nobody knows who to tell. Decide both now, while it is calm. Assume email and phones may be part of the problem.

*What this produces: the decision roles and communication list for your continuity plan.*

### Decision roles

| Role                                                     | Name                | Backup person          | How to reach them if systems are down          |
|----------------------------------------------------------|---------------------|------------------------|------------------------------------------------|
| <i>Example: Declares the incident and makes the call</i> | <i>Owner or CEO</i> | <i>Operations lead</i> | <i>Personal mobile, kept on a printed card</i> |
|                                                          |                     |                        |                                                |
|                                                          |                     |                        |                                                |
|                                                          |                     |                        |                                                |

### Who needs to hear from you

| Audience              | Who tells them         | How (if email is down)    | Within            |
|-----------------------|------------------------|---------------------------|-------------------|
| <i>Example: Staff</i> | <i>Operations lead</i> | <i>Text message group</i> | <i>30 minutes</i> |
|                       |                        |                           |                   |
|                       |                        |                           |                   |
|                       |                        |                           |                   |
|                       |                        |                           |                   |

Audiences to consider: staff, customers or patients, key vendors, your insurer, legal counsel, regulators (if you are held to one), and your IT partner.

## What are you already required to have?

For many organizations, continuity planning is not optional. Regulators, insurers, and customers may already require pieces of it, and they will ask for evidence. Check what applies to you and note where the evidence lives today. "I think our IT company handles it" is a gap, not an answer.

*What this produces: your compliance and contractual obligations, so the plan satisfies them by design instead of in a scramble.*

| Requirement                                                              | Applies? | What it asks for                                                                                                                                                  | Where is the evidence today? |
|--------------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| <b>HIPAA</b> (healthcare providers and their business associates)        | Yes / No | A contingency plan: data backup plan, disaster recovery plan, emergency mode operation plan, testing, and an analysis of which applications and data are critical |                              |
| <b>CMMC / NIST</b> (defense contractors and subcontractors)              | Yes / No | Protection of backups and recovery capability as part of the assessed controls                                                                                    |                              |
| <b>Cyber insurance</b> application or renewal                            | Yes / No | Whether backups are isolated from your network, whether restores have been tested, and how recently                                                               |                              |
| <b>Customer or partner contracts</b> with uptime or recovery commitments | Yes / No | Specific recovery times or notification windows you have promised                                                                                                 |                              |
| <b>Financial or industry regulators</b>                                  | Yes / No | Business continuity documentation and periodic testing                                                                                                            |                              |
| <b>Other</b>                                                             | Yes / No |                                                                                                                                                                   |                              |

**Note.** This is a prompt list, not legal or compliance advice. Requirements change and vary by contract. The point is to know which questions you will be asked, and to make sure the answers exist somewhere other than an assumption.

## WHAT YOUR ANSWERS MEAN

### Where does your organization sit today?

Read the four descriptions below and mark the one that is honestly closest. Most businesses are further down this list than they think, and that is the point of asking.

|   |                                                                                                                                                                                                                                                                                     |     |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| 1 | <b>Unknown</b><br>No one can say with confidence what is backed up, how often, or whether it works. Nobody has asked what must not stop.                                                                                                                                            | [ ] |
| 2 | <b>Backed up, untested</b><br>Backups run, but no one has ever restored from them, and there is no written plan for how the business operates in the meantime. This is false confidence, and it is the most common place to be.                                                     | [ ] |
| 3 | <b>Recoverable data</b><br>You can restore files and systems, but bringing the business back to operational still takes days, and the recovery order gets decided during the outage.                                                                                                | [ ] |
| 4 | <b>True continuity</b><br>Leadership knows what must not stop and for how long. A written plan says who decides, how people keep working, and what comes back first. Critical systems can be running again in minutes, and the recovery has been tested on a schedule, not assumed. | [ ] |

### What to do with this

Whoever your IT provider is, this worksheet gives you the questions they should have asked. Bring it to your next conversation with them and ask three things:

| Ask your provider                                                     | A good answer sounds like                          | A gap sounds like                             |
|-----------------------------------------------------------------------|----------------------------------------------------|-----------------------------------------------|
| Who owns our continuity plan?                                         | A named person, a written plan, a review date      | "We handle your backups."                     |
| When did you last restore from our backups, and can I see the result? | A date, a documented test, and what was learned    | "The jobs report success every night."        |
| What comes back first, and who decided that?                          | A recovery order set by our leadership, in writing | "We'd get everything back as fast as we can." |

**If you would like a second set of eyes.** For our managed clients, this analysis and the continuity plan that follows it are part of the strategic relationship, led by our founder, not sold as a separate engagement. If you want to walk through your answers with someone who has done this many times, the conversation is free and there is no obligation. [steppingforward.tech/chat-with-matt](https://steppingforward.tech/chat-with-matt)

Matt Harvey, Founder and CEO, Stepping Forward Technology. Serving Colorado Springs and the Mountain West since 2006.

This worksheet is yours to keep, copy, and share. It names no products and requires none.