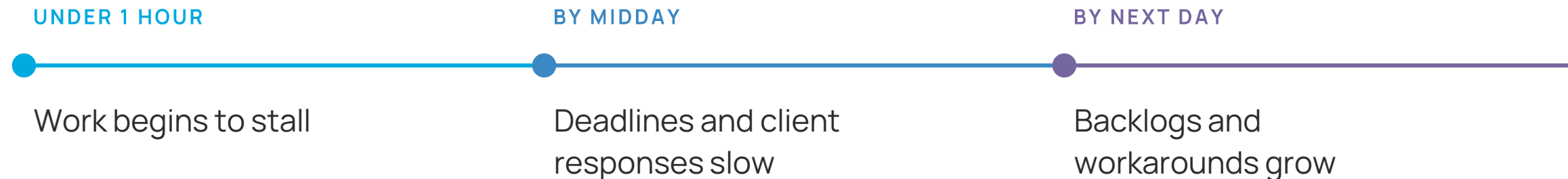


Business Continuity for CPA Firms

Keeping client commitments moving when systems do not

Your files are unavailable. How long before client work stops?

If you're not sure, that uncertainty is the first continuity gap. Continuity begins with knowing which client commitments stop first.



Scenario: At 8:15AM, the outage reaches the client

This illustrative CPA-firm scenario shows how the continuity plan protects the work around the technology, not only the technology.

01

THE TRIGGER

A core accounting application goes offline. Staff can't reach working files or complete scheduled work.

02

THE OPERATING IMPACT

The outage is technical, but the consequences are operational. Deadlines don't move. Client questions continue. Remote staff need direction.

03

WHAT THE PLAN MUST ANSWER

Who declares an incident? Which work is critical? How does the team continue? When do clients hear from us?

The real risk is the dependency chain

Continuity fails where one untested dependency becomes a single point of failure.

People

Who decides, and who can act?

Connectivity

Can staff authenticate and connect?

Apps & Data

Can critical workflows reach what they need?

Comms

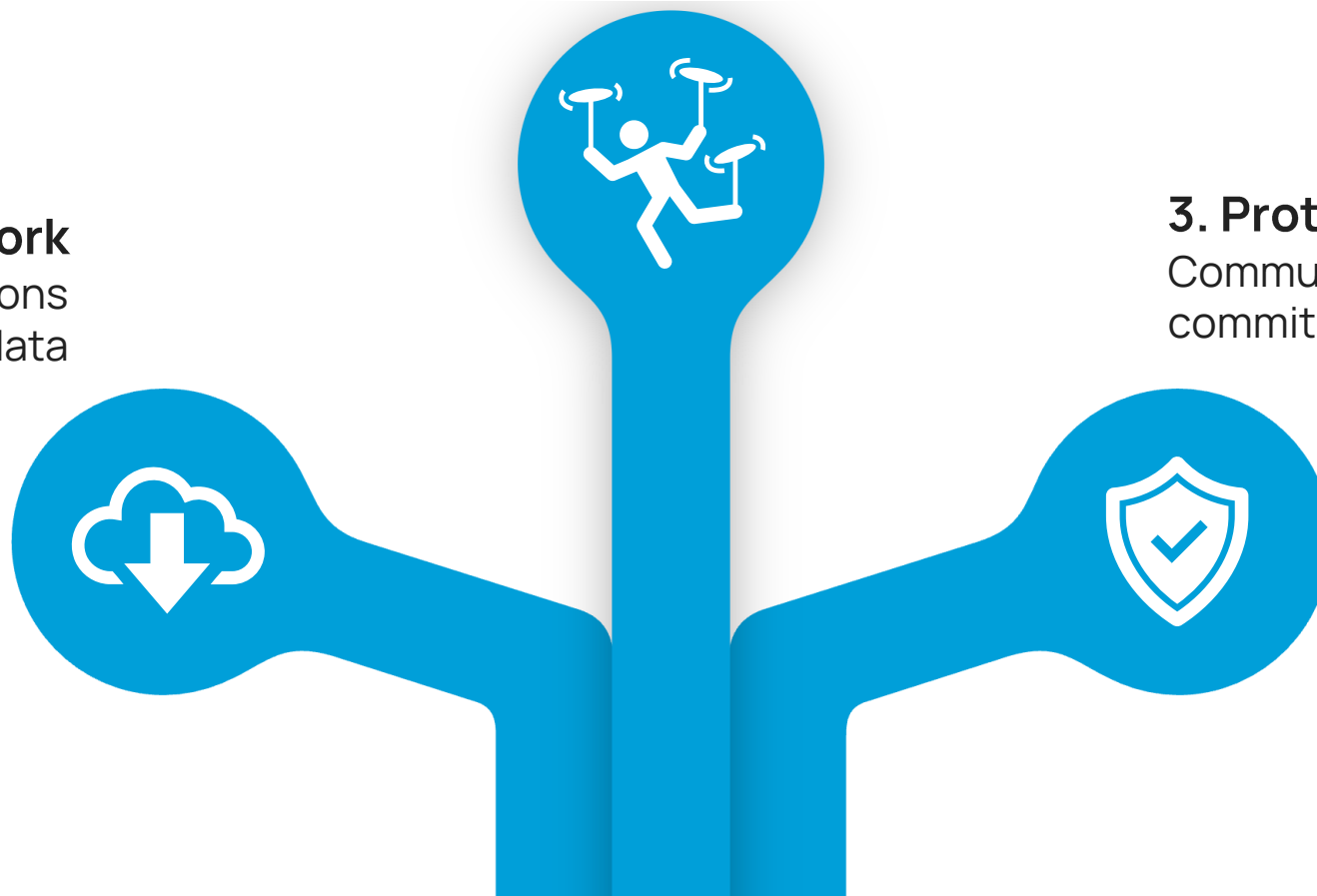
Can vendors, partners, and clients be reached another way?

Continuity protects 3 major business outcomes

2. Keep People Working
Preserve the critical workflows

1. Recover The Work
Restore the right applications
and data

3. Protect Client Trust
Communicate clearly and keep
commitments visible



Don't just back up, **prove** you can recover

A backup you've never restored is an **assumption**, not a capability.

DEFINE THE WORK THAT MATTERS MOST:

- 1 Set acceptable data loss and recovery time per workflow.
- 2 Protect backup copies from the same event.
- 3 Monitor exceptions and ownership.
- 4 Restore a representative workload and record the result.

ASK YOURSELVES:

ACCEPTABLE DATA LOSS

How much work can we afford to recreate?

ACCEPTABLE DOWNTIME

How long can this workflow remain unavailable?

Build the workaround before you need it

Legacy knowledge is a hidden single point of failure: alternates have to be named, not assumed. Minimum viable operations answer a different question: can the firm keep its most important work moving?

VERIFY BEFORE AN OUTAGE:



Remote access

Secure access works away from the office.



Application map

Critical applications and integrations are mapped.



Role backups

Key roles have alternate people and procedures.



Client channels

Phones, email, portals, and approvals have workarounds.

Silence turns an outage into a trust event

Clients don't need every technical detail. They need **clarity** about what affects them.

DECIDE IN ADVANCE:

OWNER

Who approves and sends the message?



ORDER

Which clients and channels come first?



TRIGGER

What triggers the next update?

A plan you haven't tested is still a hypothesis

Use a cadence appropriate to your risk, client commitments, and obligations.

CADENCE	TIMES PER YEAR	WHAT GETS TESTED
MONTHLY	 12×	Review backup and monitoring exceptions.
QUARTERLY	 4×	Restore a representative workload and test remote access.
SEMIANNUALLY	 2×	Run a leadership tabletop exercise.
ANNUALLY	 1×	Exercise the full plan and update responsibilities.

Continuity ownership is shared, not handed off

The firm keeps accountability. The provider reduces technical burden and makes execution repeatable.

YOU OWN

Business priorities

Decision roles

Staff procedures

Client communication

SHARED

Recovery objectives

Escalation path

Tests and evidence

Procedure and runbook updates

YOUR PROVIDER (OR SUMMIT) OWNS

Platform availability & monitoring

Backup and recovery

Secure application access

Technical response

The result: Fewer technical failure points for your team to manage

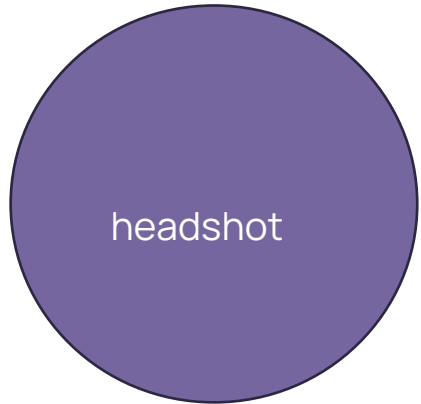
Ask for **evidence**, not reassurance

Summit environment demo

SUMMIT CAN SUPPORT:

- Hosted applications and secure access
- Managed backup and recovery
- Managed environment and monitoring
- Technical response and coordination
- Alternate work locations

Summit client testimonial



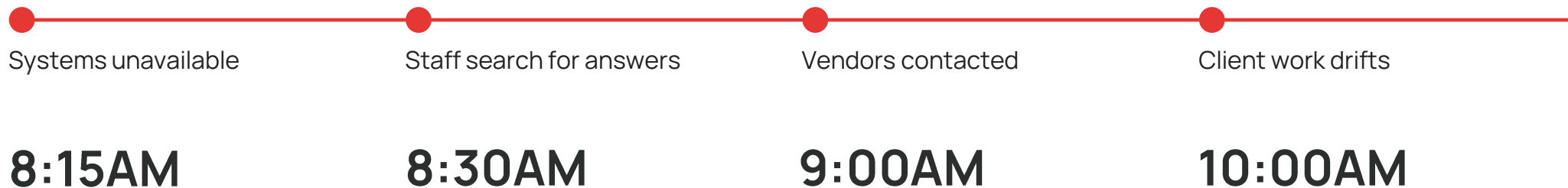
Jeni Ramsey, CPA, CGMA

Henry Peters
Tyler, TX

The plan is written before 8:15AM, or during it

Prepared decisions and tested capabilities change the first critical hour.

UNPREPARED TIMELINE



PREPARED TIMELINE



WHAT CHANGED

● Roles assigned

● Access paths tested

● Recovery practiced

● Messages prepared

Build the first version in 30 days

Don't turn continuity into a yearlong project.



5 questions to take back to your firm

If one answer's uncertain, you've found a continuity priority.

1

Which client commitments stop first?

2

How much work can we afford to recreate?

3

How quickly must each critical workflow return?

4

Who has authority to decide and communicate?

5

When did we last prove the plan works?

Q&A

What would stop your firm first?