CRYSTAL IT — GOLD COAST

The Business Owner's Field Guide to Backup, DR & Business Continuity

A practical, jargon-free reference for understanding how backup, disaster recovery, and business continuity actually work — and what the right strategy looks like for your business.

CIT

We wrote this guide because we kept having the same conversation. A business owner would call us after an incident — ransomware, a dead server, a failed drive — and say, "*But we had backups.*" They did. But backups alone were never going to be enough. This guide explains why, and what a complete strategy actually looks like.

Crystal IT — Gold Coast IT Support Since 2001

In This Guide

CHAPTER 01

Why This Matters More Than You Think

In our experience, most business owners take data protection seriously in principle. They know backups matter. They assume someone is handling it. And in many cases, someone is — to a point.

The gap is not in awareness. It is in understanding **what a backup actually covers** versus what a business needs to survive a serious incident. And it is a gap that stays hidden until the worst possible moment.

What we consistently see across Gold Coast businesses is this: a backup exists, but nobody has tested whether it can actually restore a full working system. Recovery targets have never been discussed, let alone documented. And the plan for what happens when something catastrophic occurs is, frankly, "*We'll figure it out.*"

That is not a criticism. It is a reflection of how busy business owners are. IT resilience rarely feels urgent — until it is the only thing that matters.

> ***"The businesses that recover well are not the ones with the most expensive technology. They are the ones who planned before the incident, not during it."***

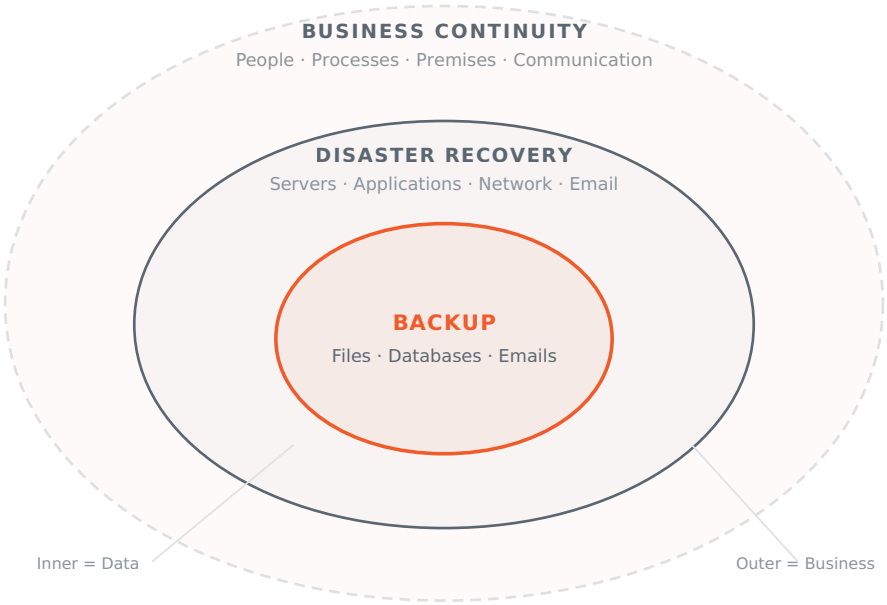
The current threat landscape has made this planning more important, not less. Ransomware attacks now routinely target backup systems before encrypting production data. The strategy is deliberate: destroy the recovery path first, then demand payment. Businesses without a layered, tested approach are the ones most likely to pay a ransom — or close permanently.

This is not about fear. It is about making informed decisions while you still have the luxury of time.

CHAPTER 02

Three Layers, Three Different Problems

Backup, Disaster Recovery, and Business Continuity are not three names for the same thing. They are three distinct layers of protection, and each one solves a different problem. Every layer builds on the one inside it.



Backup — "Does our data still exist?"

Backup copies your data — files, databases, emails — so they can be retrieved if the originals are lost, corrupted, or encrypted. It answers one question only: *do we still have the information?*

What backup does **not** do is rebuild your server, reconfigure your network, reinstall your applications, or reconnect your team. It preserves the raw materials. It does not rebuild the house.

Disaster Recovery — "Can we get our systems running again?"

DR is the plan and technology to restore your entire IT environment — servers, applications, network, email — after a major failure. It defines *how* your systems come back online and *how quickly*.

If backup is the photocopied documents in a fireproof safe, DR is the ability to move into a fully equipped replacement office and start working from those documents within a defined timeframe.

Business Continuity — "Can our business keep operating?"

BC is the complete strategy that ensures your business continues to function during and after a disruption. It encompasses DR but extends to people, processes, communication, client commitments, premises, and supply chains.

In our experience, this is the layer most businesses have not planned for. The technology may be recoverable, but if nobody knows who to call, where to work from, or how to communicate with clients during an outage, the business stalls regardless.

> "***Backup asks: Do we have the data? DR asks: Can we restore the systems? BC asks: Can the business survive? You need all three.***"

CHAPTER 03

The Numbers That Define Your Strategy

Three metrics form the foundation of every backup and disaster recovery plan. They determine what technology is needed, what it will cost, and whether the plan will actually work under pressure.

RPO

Recovery Point Objective

How much data can you afford to lose?

RPO looks **backwards** from the moment of failure to the last good backup. The gap is lost data — transactions, records, documents created between that backup and the incident. A shorter RPO means more frequent backups and less data at risk.

IN PRACTICE

An accounting firm's backup runs at midnight. A server fails at 3:00 PM the next day. Every invoice, journal entry, and client file created in those 15 hours is gone. With an RPO of 1 hour, the maximum loss would be 60 minutes of work — a very different outcome.

24 hrs	1 hr	Near 0
Nightly backup. Lower cost, more exposure.	Hourly snapshots. Minimal data loss.	Real-time replication. Mission-critical.

RTO

Recovery Time Objective

How quickly do you need to be back up and running?

RTO looks **forwards** from the failure. It defines the maximum acceptable downtime before the business impact becomes unacceptable — lost revenue, missed deadlines, damaged client relationships. A shorter RTO requires more sophisticated recovery infrastructure.

IN PRACTICE

A construction company's project management server dies at 8:00 AM Monday. Estimators cannot quote, project managers cannot schedule, and invoices cannot be issued. Can the business absorb two days of downtime while a new server is sourced and rebuilt? If not, the RTO needs to be measured in hours, and the infrastructure must match.

24-72 hrs	4-8 hrs	<1 hr
Traditional restore to new hardware.	Standby hardware or cloud recovery.	Live failover. Highest investment.

MTTR

Mean Time to Recovery

How long does recovery actually take in the real world?

RTO is the target. MTTR is the truth. It is the average actual time to detect a failure, diagnose the cause, restore systems, and verify that everything works. If your MTTR exceeds your RTO, your recovery plan has a gap — and you will only discover it under pressure.

IN PRACTICE

A real estate agency sets a 4-hour RTO for its property management system. During an actual restore test, it takes 11 hours. The backup was slower than expected, the replacement hardware was not fully compatible, and nobody had documented the network configuration. The 7-hour gap between target and reality would have been devastating in a live incident.

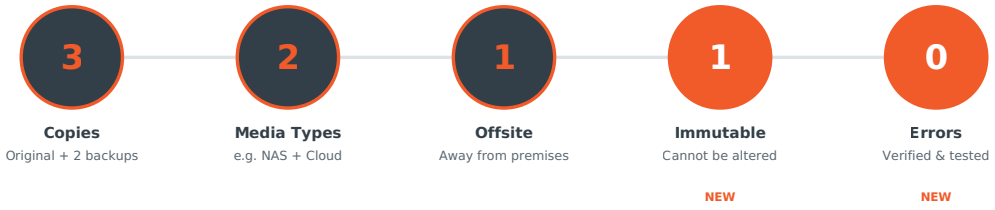
The point: if you have never tested a full restore, you do not know your MTTR. And if you do not know your MTTR, your RTO is an assumption, not a plan.

CHAPTER 04

The 3-2-1-1-0 Framework

For years, the 3-2-1 rule was the standard: three copies of data, on two different media types, with one copy offsite. It remains sound advice, but it was designed for a world where the main threats were hardware failure and natural disaster.

Today, attackers specifically target backup infrastructure. Their objective is to eliminate your ability to recover without paying a ransom. The updated **3-2-1-1-0** framework adds two layers that directly address this.



Why the extra "1-0" changes everything

Immutability ensures that at least one backup copy cannot be modified, encrypted, or deleted — even by an attacker who has gained administrative access to your systems. Without it, a single breach can wipe out every backup you have, including cloud copies accessible with compromised credentials.

Verification means regularly confirming that backups can be used to restore a working system — not just that the backup job completed without errors, but that the resulting data is intact, bootable, and functional. Without it, you may discover your backups are corrupt or incomplete at the moment you need them most.

> "***The businesses that recover from ransomware are, without exception, the ones with an immutable backup that was verified before the attack. Everything else is recovery by luck.***"

CHAPTER 05

From Numbers to Technology

There is no one-size-fits-all solution. The right combination of hardware, software, and cloud services flows directly from your RPO and RTO targets — which themselves come from understanding how critical each system is to your day-to-day operation.

Prioritising your systems

Not every system warrants the same level of protection. The practical approach is to tier them by business impact.

PRIORITY	SYSTEM TYPE	RPO	RTO	EXAMPLES
CRITICAL	Core operations	15 min – 1 hr	1 – 4 hrs	ERP, POS, accounting, patient records
IMPORTANT	Supporting functions	1 – 4 hrs	4 – 12 hrs	Email, CRM, scheduling, file shares
STANDARD	Internal tools	4 – 24 hrs	24 – 72 hrs	Archived projects, training materials

How targets map to technology

Once targets are defined, the technology decisions become straightforward. Here is how the layers typically align.

On-premises hardware — NAS devices for fast local backup and restore, standby server hardware for rapid failover, image-based backup for full system recovery. Best for achieving short RTO targets where local restore speed outperforms cloud download times.

Cloud services — Offsite and immutable backup repositories, cloud-to-cloud backup for Microsoft 365 and Google Workspace, cloud-based disaster recovery (DRaaS) for spinning up systems in a remote environment. These deliver the offsite and immutable layers of the 3-2-1-1-0 framework.

Software and automation — Image-based backup for complete system recovery, automated scheduling and monitoring, integrity verification to achieve the "zero errors" target, and orchestration tools that reduce MTTR through automated failover.

The tighter the targets, the more investment is required. The goal is not to make everything critical — it is to **protect the right things at the right level** and accept manageable risk where the cost of premium protection is not justified.

CHAPTER 06

Closing the Gaps — Where We Come In

Reading a guide is useful. Acting on it is what actually protects your business.

What we have found, consistently, is that the gap between where a business *thinks* it is and where it *actually* is only becomes clear when someone sits down and maps it out properly. That is exactly what we do.

We help businesses move from **assumptions to documented plans** — assessing the current environment, identifying the gaps, defining realistic recovery targets, and designing a layered strategy that delivers the outcomes the business actually needs.

What a typical engagement looks like

Step 1 — Assessment. We review your current backup, recovery, and continuity posture. What exists, what works, what does not, and where the gaps are. This is a factual, no-surprises review.

Step 2 — Run Book. We draft a documented incident response run book tailored to your business. It defines who does what, in what order, when an incident occurs — so recovery is a process, not a scramble.

Step 3 — Strategy. Based on the assessment and your business requirements, we design a layered backup, DR, and continuity strategy that addresses the identified gaps. This includes recommended RPO and RTO targets, technology selections, and an implementation plan.

Step 4 — Protected. The strategy is implemented, tested, documented, and verified. You have a working plan, proven technology, and the confidence that if something goes wrong, your business can recover.

> ***"The best time to plan your recovery is before you need it. The second best time is today."***

Start With a Conversation

We will review where your business stands, identify what is working and what is not, and give you a clear picture of your options. No obligation, no pressure.

Call 1800 99 2001 **Request a Free Review**

Crystal IT — Gold Coast IT support since 2001 · Freecall 1800 99 2001 · crystalit.com.au

www.crystalit.com.au | Freecall 1800 99 2001 | Gold Coast, Queensland

This guide is provided for general information purposes. Recovery targets and recommendations should be tailored to your specific business requirements.