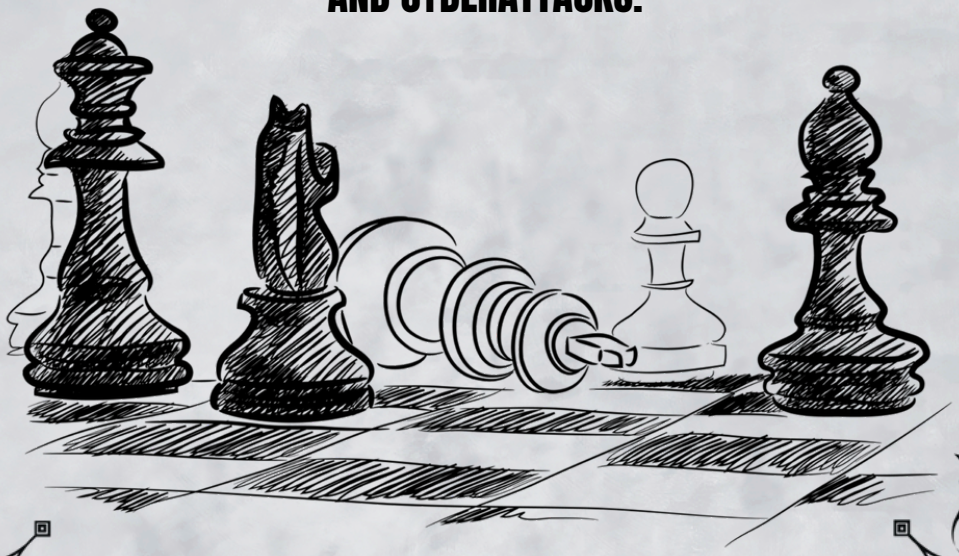
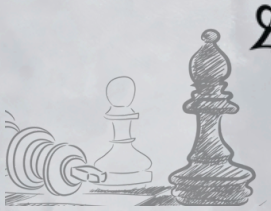
BUILDING YOUR BUSINESS CONTINUITY PLAN

HOW TO PROTECT YOUR BUSINESS FROM DOWNTIME, DISASTERS, AND CYBERATTACKS.



written by **Gregorio Chaves**

WHY CONTINUITY MATTERS



Most business owners know they need antivirus, backups, maybe even cyber insurance. But when asked about a Business Continuity Plan (BCP) you'll usually get a blank stare. Then...

The dreaded response:

"We'll just deal with it ***if it happens."***

The real problem is:

"If it happens" is ***"when it happens."***

So what happens?

- A single server crash.
- A ransomware email.
- A cloud outage at Microsoft 365.
- Even a burst pipe in your office.

Each one can stop your operations cold. And downtime isn't just an IT problem, it's a business killer. Studies show that **"when it happens"** SMBs lose thousands of dollars per hour of downtime, not to mention the reputation hit if clients can't reach you. Once the dust settle's there still is no plan to follow for **"when it happens"** again.

Think of BCP as your playbook for survival. It's not just about restoring files; it's about keeping your business moving when the unexpected happens. Such as **"when it happens",** you are ready and downtime is short lived vs days or weeks of recovery efforts.

👉 That's the difference between a normal backup and a continuity plan:

- Backups = insurance. You can recover eventually.
- Continuity plan = action. You know exactly how fast you'll be back, who's in charge, and how you'll keep clients in the loop.

At GCMSP, we've seen firms that thought **"backups were enough"** lose entire weeks of revenue because they didn't know their **Recovery Time Objectives (RTOs)** or how to reroute staff during an outage. On the flip side, clients with tested BCPs? They treat a ransomware attack like a fire drill, stressful? Yes, but survivable.

This guide will break down exactly what a BCP is, what it should aim for, and how you can build one tailored to your industry. By the end, you'll have the blueprint for resilience, not just security.

WHAT A BCP REALLY IS

If you ask 10 business owners what a Business Continuity Plan (BCP) is, you'll get 10 different answers:

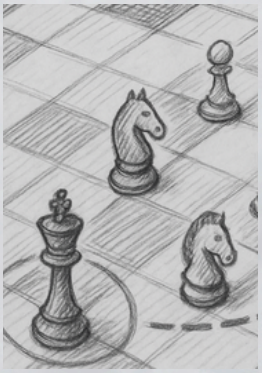
- "It's just backups."
- "It's our insurance policy."
- "It's something only big companies need."

Here's the truth: a BCP is your playbook for survival.
It's the written plan for how your business keeps running when disruptions happen, whether that's a cyberattack, hardware failure, or even something as simple as a power outage.

BCP vs. Disaster Recovery (DR)
People often confuse these. Here's the difference:

- Disaster Recovery (DR): How IT restores systems and data after an incident. (Think: restoring files from backup, rebuilding a server, re-imaging a PC.)
- Business Continuity (BCP): How the entire business continues to function during and after disruption. (Think: how staff serve clients, how payroll gets run, how deadlines are met.)

👉 **DR is a subset of BCP. You <u>need</u> both.**



BCP vs. Cybersecurity

Cybersecurity prevents bad things from happening.
BCP assumes bad things will happen and answers: *"Now what?"*

- Cybersecurity: locks on the doors.
- BCP: a fire drill, escape plan, and sometimes even a backup office ready to go.

They're different disciplines but deeply connected.

The Real Aim of a BCP

A strong continuity plan isn't about paperwork. It's about:

1. Protecting operations – keeping services running so clients aren't left waiting.
2. Protecting cash flow – every hour of downtime bleeds money.
3. Protecting trust – how you respond to crisis shapes how clients, regulators, and staff see you.
4. Protecting compliance – many frameworks (HIPAA, PCI, IRS, NIST) expect proof you can operate through disruption.

A Simple Analogy

Business continuity is like playing chess at a high level. Winning isn't about the last move, it's about planning several moves ahead.

- Backups are like remembering where the pieces were. When an unexpected play happens, you can reset and re-strategize on the fly. But that alone doesn't mean you'll win the game.
- BCP is your playbook. The openings you've practiced, the contingencies you've prepared, and the counter-moves you've already thought through when your opponent surprises you.

In business, the players who think ahead survive the unexpected. The ones who only react often end up in checkmate.

✅ By the end of this eBook, you'll see that BCP isn't just for Fortune 500s.
It's for every SMB that depends on technology, people, and reputation,
which means it's for you.

THE PILLARS OF A STRONG BCP

In chess, champions don't just react to the board in front of them, they study openings, anticipate threats, and know how to recover when a piece falls. A strong Business Continuity Plan works the same way. It's built on a few core pillars that give you structure when the unexpected strikes.

Pillar 1: Maximum Tolerable Downtime (MTD)

- What is The longest your business can afford to be down before damage becomes critical?
  - Like a time control on the clock in chess game. If you run out of time, the game ends no matter how strong your position is.

Why it matters? Every SMB has a limit. For some, it's hours; for others, days. Knowing your MTD sets the pace for every other part of your plan.

Pillar 2: Recovery Time Objective (RTO)

- What is the target for how quickly systems and processes must be restored after disruption?
  - Your next move under pressure. You can't freeze at the board, you need a prepared response to get back into play fast.

Why it matters? An RTO of 8 hours vs. 48 hours changes the technology, staffing, and budget required.

Pillar 3: Recovery Point Objective (RPO)

- How much data loss is acceptable? measured in time. (Example: last backup was 4 hours ago, so you could lose up to 4 hours of work.)
  - It's the material you're willing to sacrifice. Sometimes you give up a pawn to protect your queen, but you need to know in advance what's expendable.

Why it matters? If your RPO tolerance is minutes, you'll need advanced replication. If it's a day, simpler backups may suffice. Cost and efforts are impacted based on your RPO.

Pillar 4: Roles & Responsibilities

- Clear assignments for who does what during a disruption.
  - Every piece has a role, pawns defend, bishops strike diagonally, rooks hold the line. Chaos comes when pieces move without purpose.

Why it matters? If no one knows who's calling clients, running failovers, or approving vendor access, downtime doubles.

Pillar 5: Communication Plan

- The process for keeping staff, clients, and partners informed when things go wrong.
  - Coordinated play. Grandmasters don't just move pieces randomly, they align them to work together toward the same goal.

Why it matters? Silence during an outage breeds panic. Clear communication keeps trust intact, even when systems falter.

✅Together, these pillars form the foundation of resilience. Just like in chess, the winner isn't the player with the fanciest moves, but the one who sticks to fundamentals and adapts under pressure.

WWW.GCMSP.COM

MAPPING YOUR BUSINESS RISKS

In chess, every move carries risk. Push a pawn too far, and you might expose your king. Continue to move with no strategy, and your opponent takes control of the board. Business works the same way: every operation has risks that need to be spotted, measured, and managed before they turn into checkmate.

A Business Continuity Plan starts with a risk map, your way of identifying the threats most likely to hit and how damaging they could be.

Cyber Threats
Examples: ransomware, phishing, insider misuse.
- Surprise attacks — the gambits and traps your opponent sets to catch you off guard.

Why it matters? These risks can cripple SMBs quickly because they spread fast and often hit where you least expect it.

Physical Threats
Examples: fire, flood, power outage, hardware failure.
- Board conditions the clock running low, the lights flickering, or a mis-timed hand slip. They don't come from your opponent, but they can still cost you the game.

Why it matters? Even the strongest cyber defense can't stop a failed server fan or storm knocking out power.

Human Risks
key staff absence, errors, vendor dependency, insider sabotage.
- Misplays the wrong move at the wrong time. Even a grandmaster can blunder, and one mistake can shift the entire match.

Why it matters? Most continuity failures trace back to people, not machines. A plan has to account for staff turnover, mistakes, or a partner not delivering.

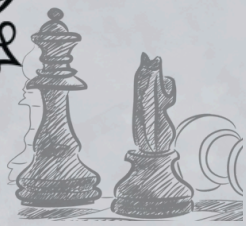
Risk Ranking Exercise

Every SMB should rank risks across two simple scales:

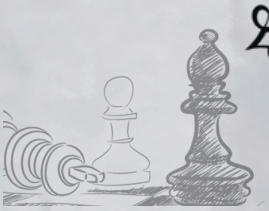
1. **Likelihood** (How often could this happen?)
   - High = daily/weekly exposure (like phishing emails)
   - Medium = occasional (like hardware failure)
   - Low = rare but catastrophic (like a natural disaster)
2. **Impact** (What's the damage if it happens?)
   - High = stops operations cold
   - Medium = slows things down, adds costs
   - Low = minor inconvenience

Before making a move, players weigh the risk vs. reward, is capturing that piece worth the potential counterattack? In business, risk ranking helps you decide where to build your strongest defenses first.

✅ By mapping risks, you can see the whole board clearly. And once you know where the threats are, your BCP becomes less about guessing and more about planning the right moves to stay ahead of disruption.



STEP-BY-STEP GUIDE TO BUILD YOUR BCP



Champions don't wing it. They've practiced openings, studied mid-game strategies, and even rehearsed what to do when they lose a major piece. A Business Continuity Plan works the same way, it's not theory, it's preparation you can execute under pressure.

Here's your move-by-move guide to building a plan:

Step 1: Identify Critical Business Functions

- List the processes your company must keep running — payroll, client communication, manufacturing lines, healthcare records.

  -Your king. Protecting it is non-negotiable; everything else revolves around keeping it safe.

Step 2: Assign Owners for Each Function

- Give clear responsibility to individuals or teams. No "maybe it's Bob's job."

  -Every piece has a role — pawns defend, knights surprise, rooks control the board. Strength comes from knowing who does what.

Step 3: Define RTO and RPO Targets

- Set the max downtime (RTO) and max data loss (RPO) for each function.

  -Time controls. You can't take forever to make a move, and you need to know what sacrifices are acceptable to keep momentum.

Step 4: Document Dependencies

- Map out what each function relies on: apps, vendors, internet, key staff.

  -Piece coordination. A knight out of position weakens the whole board. Business functions don't operate in isolation either.

Step 5: Create Action Playbooks for Top Risks

- Write short, clear instructions for the top risks you mapped in Chapter 3. Example: "If ransomware hits accounting, switch to cloud backup X, notify clients with template Y."

  -Prepared defenses. You don't invent responses over the board; you know the counter-moves before the attack comes.

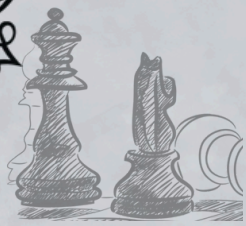
Step 6: Test Your Plan

- Run tabletop exercises, simulate outages, and practice failovers.

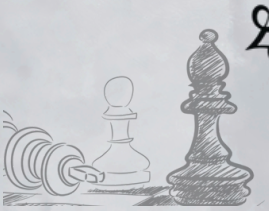
  -Practice games. Grandmasters don't just study openings; they play them under pressure until responses are second nature.

✅ By following these steps, you transform your BCP from a document on the shelf into a living strategy. In chess and in business, the difference between amateurs and pros isn't talent, it's preparation.

WWW.GCMSP.COM



INDUSTRY EXAMPLES



Every chess player has a style. Some play aggressively, some patiently, some defensively. Businesses are the same. Your continuity plan must reflect not just your industry's rules, but its tempo, risks, and stakes.

Here's how continuity looks across key sectors:

Legal: Precision Play
Missing a court deadline or leaking client files destroys trust instantly.

- BCP Focus: Systems and case data must be accessible quickly, even during an outage.
  - Like a tactical player who relies on accuracy. Every move must be deliberate, with no room for careless mistakes.

CPA / Accounting: Speed is king
Tax season and reporting deadlines create massive workload spikes. Downtime of even hours can cost clients and revenue.

- BCP Focus: Rapid recovery, cloud redundancy, and backup internet to handle filing crunches.
  - Blitz games. Every second counts, and the ability to respond under time pressure separates winners from losers.

Healthcare: Defense is the best offense
Patient safety, HIPAA fines, and reputation. Even small disruptions can trigger big consequences.

- BCP Focus: Prioritize access to patient records, tested recovery for EHR systems, and a clear plan for communication with patients.
  - A defensive strategist. Protect the king (patients and data) at all costs: steady, reliable, and layered defenses win.

Manufacturing: Endurance Match
Shop floor downtime = halted production lines and lost contracts. Intellectual property (IP) theft also puts years of R&D at risk.

- BCP Focus: Segment networks, test backups for ERP/production systems, and prepare alternate workflows for supply chain disruptions.
  - A long, grinding endgame. Success isn't flashy, it's about stamina, keeping resources safe, and avoiding costly blunders over time.

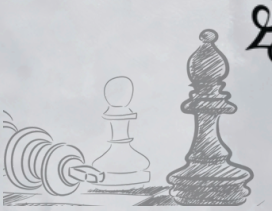
Retail / Nonprofit: Adaptability Play
For retail, every hour offline means lost sales and unhappy customers. For nonprofits, outages can mean missing fundraising deadlines or disrupting critical community programs.

- Backup point-of-sale (POS) systems, cloud-hosted donor databases, and alternative communication channels for staff and clients.
  - A flexible, opportunistic player. Success comes from adapting quickly, shifting strategies mid-game when resources or priorities change.

✅ The lesson? Every industry plays a different game. Your BCP must be tuned to your sector's tempo, risks, and priorities, otherwise you're playing blind.

And if your business doesn't fit neatly into these industries? No problem. Your RTO (how fast you need to recover) and RPO (how much data you can afford to lose) will dictate the right continuity strategy for you.

WHAT A BCP SHOULD AIM FOR



Victory isn't about moving the most pieces: it's about protecting your king, controlling the board, and outlasting your opponent. A Business Continuity Plan has the same goal. It's not just about having backups, it's about ensuring your business wins the long game.

Here's what every BCP should aim for:

1. Minimize Downtime
Every hour offline bleeds revenue, trust, and productivity.

- Time control. If you stall too long, the clock runs out, no matter how good your position looks.

2. Preserve Client Trust
Customers and partners will forgive a disruption if you keep them informed, but silence or chaos costs loyalty.

- Positioning. Even if you lose material, strong positioning keeps you in the fight. Communication keeps your reputation intact the same way.

3. Reduce Financial Impact
Downtime is expensive. From lost sales to overtime pay, continuity planning saves money by shortening recovery.

- Material balance. You can sacrifice a pawn — maybe even a rook — but the goal is to avoid losing the entire game. Smart sacrifices protect your long-term advantage.

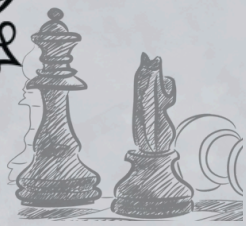
4. Meet Compliance & Insurance Requirements
Regulators and insurers increasingly demand proof of continuity. A weak BCP can mean denied claims or costly penalties.

- Playing by the rules is key. No matter how brilliant your tactics, if you break the rules, you lose. And in business, losing could translate into going out of business.

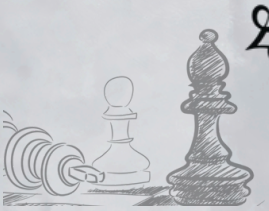
5. Build Confidence for Staff & Leadership
Panic kills recovery. A tested BCP gives your team clarity on who does what, so they act decisively when disruption hits.

- Coordination. In championship play, all pieces work together, not randomly. A confident team moves in harmony.

✅ The win condition: A strong BCP doesn't just restore systems it restores business momentum. In chess and in business, those who plan ahead don't just survive the unexpected… they come back stronger.



COMMON PITFALLS TO AVOID



Even great chess players blunder. One careless move, one overlooked piece, and the match can collapse. Business continuity is no different. Many SMBs make avoidable mistakes that leave them exposed when disruption strikes.

Here are the most common pitfalls:

1. Thinking It's Just an IT Problem
Believing continuity is only about servers and backups.
Why it hurts? Operations, communication, payroll, and client trust all need protection too.
- Focusing only on your win condition while ignoring all other the pieces around it. The whole board matters.

2. Never Testing the Plan
Writing a plan once and letting it collect dust.
Why it hurts? An untested plan will fail when pressure hits, often at the worst possible moment.
- Memorizing openings but never practicing endgames. When you reach that position, you don't know what to do.

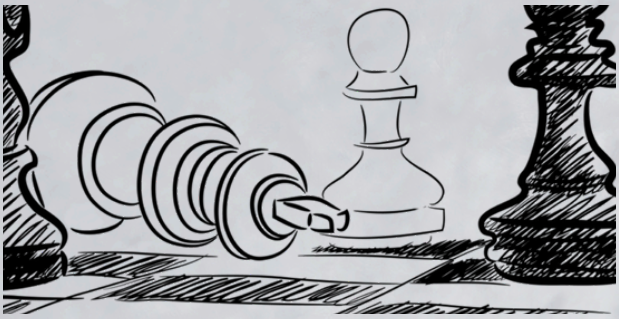
3. Overcomplicating the Document
Creating a 50-page binder no one reads or understands.
Why it hurts? Staff won't follow it in real life. Simplicity wins under stress.
- Trying to calculate 20 moves ahead when one solid move will do. Complexity creates paralysis. A BCP can be large and comprehensive, but breaking it down by teams, branches, or roles makes it usable. Your office/admin users won't follow the same strategy as your operations team, each needs a plan tailored to their function, but aligned under one playbook.

4. Forgetting Vendors, Remote Workers, and Cloud Apps
Only planning for in-house systems.
Why it hurts? Cloud outages, vendor downtime, and remote staff disruptions can be just as damaging.
- Ignoring the edges of the board. A knight on the rim or a pawn left unprotected can turn the tide.

5. Assuming Insurance Will Cover Everything
Relying on cyber insurance as a safety net.
Why it hurts? Carriers deny claims if you can't prove compliance, show you have security controls, or show you had a tested plan.
- Playing recklessly because you think you'll get a rematch. In business, one loss can end the game.

✅ The takeaway: Avoiding blunders is as important as making brilliant moves. A smart BCP doesn't have to be perfect, it just needs to be practiced, realistic, and free from the mistakes that catch most businesses off guard.

CONCLUSION
AVOIDING CHECKMATE



Victory rarely comes from a single brilliant move. It comes from steady preparation, anticipating threats, and avoiding blunders. Business continuity works the same way.

A strong BCP isn't just paperwork — it's peace of mind. It means:

- **Your downtime is measured in hours, not weeks.**
- **Your clients stay informed and loyal.**
- **Your team knows exactly what to do when the unexpected strikes.**
- **Your business survives disruption — and keeps moving forward.**

Without a plan, you're gambling every day that disruption won't happen. But in today's world, from cyberattacks to power failures — it's not if, it's when. And when that moment comes, the difference between survival and collapse comes down to whether you thought three moves ahead.

✅ The win condition? Don't play blind. Build a strategy that fits your business, test it, and refine it. The companies that plan ahead don't just survive the unexpected — they turn it into a competitive advantage.

Your Next Move

At GCMSP, we help SMBs like yours design, test, and refine BCP strategies tailored to your industry, size, and risk tolerance. Whether you're a law firm facing strict deadlines, a CPA firm bracing for tax season, a healthcare provider protecting patients, a manufacturer keeping production lines moving, or simply an SMB that knows it needs a plan, we've built strategies that keep operations safe, resilient, and ready for whatever comes next.

👉 Ready to see how your business would hold up under pressure?
Book a Resilience Readiness Review with GCMSP. We'll walk through your risks, RTOs, and RPOs — and give you a clear roadmap to avoid checkmate.

WWW.GCMSP.COM