


What to Include in Your Business Continuity Plan (BCP)

A **Business Continuity Plan (BCP)** ensures your company can **maintain operations** during disruptions—whether from cyberattacks, natural disasters, or system failures. Without one, businesses risk **downtime, lost revenue, and reputational damage**.


At **Micro Computer Consulting Inc.**, a trusted **MSP service provider in Toronto**, we help businesses create **comprehensive BCPs** tailored to their needs. Below is a step-by-step guide on **what to include** in your plan.

 **Need expert help? Call us at 905-206-1003 for a free BCP consultation!**

1. Business Impact Analysis (BIA)

Identify **critical operations** and their **maximum allowable downtime (MTD)**.

- **Key processes** (e.g., payroll, customer support, inventory management).
- **Financial & operational risks** if systems go down.
- **Recovery Time Objective (RTO)** – How quickly must each function recover?
- **Recovery Point Objective (RPO)** – How much data can you afford to lose?

 *Example:* A retail business may prioritize **e-commerce servers** (RTO: 2 hours) over internal HR systems (RTO: 24 hours).

2. Risk Assessment & Threat Scenarios

List potential **disruptions** and their likelihood:

- **Cybersecurity incidents** (ransomware, data breaches).
- **Natural disasters** (floods, power outages).
- **Human error** (accidental deletions, misconfigurations).
- **Supply chain failures** (vendor outages).

 **Pro Tip:** Rank threats by **probability vs. impact** to prioritize preparedness.

3. Emergency Response Plan

Define **immediate actions** when disaster strikes:

- **Incident escalation** (who declares an emergency?).
- **Crisis communication** (employees, customers, media).
- **Emergency contacts** (IT support, backup vendors, insurance).

 *Sample Alert Protocol:*

1. **IT team** isolates affected systems.
2. **Management** notifies stakeholders.
3. **Backup restoration** begins within RTO.

4. Data Backup & Recovery Strategy


Ensure **fast, secure data restoration** with:

3-2-1 Backup Rule

- **3 copies** of data (primary + 2 backups).
- **2 different media** (cloud + offline storage).
- **1 offsite backup** (protected from physical disasters).

 **Automated, encrypted backups** (tested monthly).

 **Ransomware-proof backups** (immutable/air-gapped).

 **Don't gamble with data—call 905-206-1003 for bulletproof backups!**

5. Alternate Work Arrangements

Plan for **remote operations** if offices are inaccessible:

- **Cloud-based tools** (Microsoft 365, VoIP phones, VPN access).
- **BYOD policies** (secure employee devices).
- **Redundant internet** (cellular hotspots, dual ISPs).

 *Example:* A law firm switches to **Teams/SharePoint** during a power outage.

6. IT Disaster Recovery (DR) Plan

A subset of BCP focused on **restoring IT systems**:

- **System prioritization** (email > CRM > internal apps).
- **Failover servers** (cloud or secondary locations).
- **Patch management** to prevent exploits.

 **Our MSP services include DR planning—call 905-206-1003!**

7. Vendor & Supply Chain Continuity

- **Identify critical vendors** (e.g., cloud hosts, payment processors).
- **Review SLAs** for their own BCPs.
- **Maintain backup suppliers.**

8. Employee Training & Testing

- **Annual drills** (simulated cyberattacks, evacuation tests).
- **BCP access** (store copies offline & digitally).
- **Role-specific checklists** (who does what during recovery?).

 *Sample Test:* Restore a backup file to verify speed & integrity.

9. Post-Recovery Review

After an incident:

1. **Analyze response effectiveness.**
2. **Update the BCP** with lessons learned.
3. **Retrain staff** on gaps.

How Micro Computer Consulting Inc. Can Help

We assist Toronto businesses with:

- ✓ **BCP Development** – Tailored to your risks & needs.
 - ✓ **Automated Backups** – Secure, compliant, & tested.
 - ✓ **Disaster Recovery Services** – Minimize downtime.
 - ✓ **Employee Training** – Ensure smooth execution.
-  **Don't wait for disaster—call 905-206-1003 to build your BCP today!**

Final Checklist for Your BCP

Component	Status
Business Impact Analysis (BIA)	<input type="checkbox"/>
Risk Assessment	<input type="checkbox"/>
Data Backup Strategy	<input type="checkbox"/>
Emergency Contacts	<input type="checkbox"/>
Alternate Work Plans	<input type="checkbox"/>
Vendor Continuity	<input type="checkbox"/>

Employee Training	<input type="checkbox"/>
-------------------	--------------------------

 **A robust BCP isn't optional—it's essential for survival.** Let us help you prepare.