BUSINESS CONTINUITY PLANNING

In an increasingly uncertain world, business continuity planning cannot be limited solely to technological considerations. It must be based on a comprehensive, structured, and proactive approach that integrates all of the organization's critical functions.

- Operations
- Supply chains
- Human resources
- Finance
- Legal
- Information technology

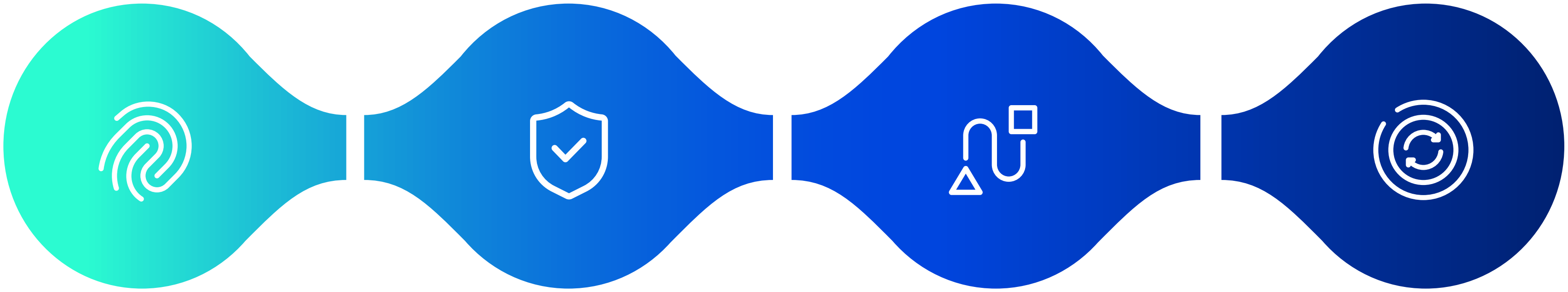
IT INTELLIGENCE.
HUMAN
INTELLIGENCE.

Let's talk

Toll free 1-888-251-1622 **ITI Québec** 418-871-1622 **ITI Montréal** 514-940-1662 **ITI Toronto, Kingston & Ottawa** 1-866-549-6558

→ iti.ca

THE 4 PILLARS OF ORGANIZATIONAL RESILIENCE



STEP 1

PREVENTION

Train employees to respond effectively before, during, and after an attack.

+ MFA / Access management
+ Updates
+ Securing systems and communications
+ Backups / recovery solutions
+ Access management
+ Phishing tests
+ Internal and external penetration tests

STEP 2

DETECTION

Identify the event, minimize impacts, and ensure rapid and appropriate intervention.

+ Intrusion Detection Systems: IDS and IPS (Intrusion Prevention Systems)
+ EDR (endpoint detection and response) for computers and phones
+ MDR (managed detection response) for all IT infrastructures, the cloud, and networks
+ Behavioral analysis: Detection of abnormal activities
+ Monitoring of system availability and outages

STEP 3

RESPONSE

React quickly, efficiently, and in a coordinated manner.

+ Execution of the incident response plan that defines what to do, who is involved, and when to act
+ Incident response team that knows the critical tools, the procedure to follow, and the documentation protocols
+ Crisis communication plan that informs employees without causing panic and manages relationships with clients, media, and partners

STEP 4

RECOVERY

Recover rapidly to minimize operational, financial, and reputational impacts.

+ Recovery plan: evolving document, restoration of critical systems
+ Prioritization: mapping of vital assets (payments, production, HR)
+ Communication: internal and external transparency after an incident
+ Post-mortem analysis: identify flaws, improve procedures

WHERE TO BEGIN?

1 — CONDUCT A BUSINESS IMPACT ANALYSIS (BIA)

Identify the organization's critical activities and the essential human and technological resources needed for their functioning. Assess the financial, operational, and reputational impacts that interruptions could cause.

2 — IMPLEMENT STRATEGIES

Determine the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) based on the BIA. Put in place the appropriate tools, such as backups and disaster recovery solutions, to ensure effective protection.

3 — DEVELOP AN INCIDENT RESPONSE PLAN (IRP)

Develop procedures to detect, respond, and recover quickly. The consequences and impacts of inaction must also be assessed: loss of revenue, damage to reputation, contractual or regulatory penalties, etc.

4 — DEVELOP A DISASTER RECOVERY PLAN (DRP)

Define precise strategies aimed at restoring systems and data following a disaster, taking into account the criticality level of activities.

5 — ORGANIZE A BUSINESS CONTINUITY PLAN (BCP)

Create a comprehensive plan to maintain essential operations during and after a major disruption.

6 — TEST, MEASURE AND ADJUST

Simulation exercises and post-mortem feedback are essential to verify the effectiveness of a business continuity plan and for training teams to respond in real-life situations.