Business Continuity Planning Guide for Small and Medium-sized Organizations

A GUIDE ON HOW TO MINIMIZE RISKS AND MAXIMIZE ORGANIZATIONAL RESILIENCE PERFORMANCE

STRATOGRID
ADVISORY

INTRODUCTION

We all live in an unpredictable world.

We are faced with many risks that can disrupt our livelihood and can jeopardize our existence. Regardless of their nature, weather-related events that cause havoc in our communities, pandemics that can wipe us out, or cyber-related incidents that can potentially shut-down our technology, these events require us to be more resilient.

Why did we write this guide? It is our finding that many organizations, small and large alike, are not adequately equipped to handle events that can disrupt their operations and protect their most valuable resource, their people.

We recognize that many business continuity planning terms and industry-leading methodologies can be foreign to your organization. It can be overwhelming if your organization has never implemented a robust business continuity program.

Once implemented, a Business Continuity Management (BCM) Program will support your organization's value statement and its mission.

This high-level guide intends to shed some light on the business continuity planning process you can apply at your small or medium-sized organization. We hope that this guide will help demystify the business continuity planning process and give you a few practical tips and guidelines on how to implement it in your organization.

About Us

We are StratoGrid Advisory, a Business Continuity Management Advisory firm located in the Ottawa/Gatineau region, and servicing clients across Canada. We were founded in 2015 to ensure that organizations of all types and sizes implement and improve their organizational resiliency.

We specialize in Business Continuity Planning and IT Disaster Recovery Planning. We also offer our signature Business Continuity Management as a Service (BCMaaS), designed for smaller organizations without dedicated business continuity resources.

About the Authors

This guide is written by Alex Jankovic, StratoGrid Advisory president and principal consultant and **Jakub Pilkowski**, a Business Continuity Management consultant.

Alex is an experienced Certified Management Consultant (CMC) and Certified Business Continuity Professional (CBCP), as well as an IT Professional with broad expertise in business continuity and IT operations. During his career he has implemented several robust Business Continuity Management Programs and provided technical leadership on many large IT implementations and IT transformation engagements.

Alex can be reached at ajankovic@stratogrid.com

Jakub is a Business Continuity Management Consultant and chief creative assistant. He has experience in finance, economics and marketing. He has assisted a variety of businesses with business continuity planning initiatives.

Jakub can be reached at jpilkowski@stratogrid.com

About the Editor

This guide has been edited by Wendy Verkerk B.A.,B.Ed.; she can be reached at - wendy@yellowcanoe.ca

StratoGrid Advisory

251 Laurier Avenue West
Suite 900, Ottawa, K1P 5J6
Ontario, Canada

TABLE OF CONTENTS

Introduction

Chapter 1 - Introduction to Business Continuity Planning (BCP)

Chapter 2 - Business Continuity Management (BCM) Program Implementation

Chapter 3 - Risk Assessment

Chapter 4 - Business Impact Analysis

Chapter 5 - Business Continuity Strategy

Chapter 6 - Business Continuity Plan

Chapter 7 - IT Disaster Recovery Plan

Chapter 8 - Testing, Training & Awareness

Chapter 9 - BCM Program Maintenance

Chapter 10 - Resilient Organization

CHAPTER 1 - INTRODUCTION TO BCP

Business Continuity should be one of the top priorities for all organization leaders, and response plans should be implemented in organizations of all sizes.

Regardless of the industry (non-profit organizations, professional services companies, manufacturing, public sector, etc.), organizations should develop response plans to deal with unexpected events related to:

- Natural disasters (hurricanes, earthquakes or freezing rain)
- Technological disruptions (loss of data centers, data breaches or other IT security-related incidents)
- Talent related disruptions (pandemic planning, emergency management and physical security-related events)

The truth is that many organizations are not ready to deal with unexpected events. The implementation of a Business Continuity Management (BCM) Program can be a complicated and lengthy process, which directly depends on the organization's size and complexity.

There is a common misconception among many small and medium-sized organizations about what the Business Continuity Planning (BCP) process entails.

BCP requires collaboration across the entire organization and the participation of all business units and departments. It requires time investment from all stakeholders (including executive management time), staff training and continuous maintenance and testing. It requires a budget and long-term commitment (hence why it is a BCM Program). As such, it should not be taken lightly.

What some organizations fail to realize is what Business Continuity is not. Business Continuity is not a data backup. The Managed Services Providers (MSPs) industry has managed to hijack the Business Continuity term, and it became all about data backup. A data backup is only one component of IT Disaster Recovery Planning, which we address in Chapter 7.

Many organizations struggle with implementation once they realize the potential investment of stakeholder time, money, and ongoing requirements to maintain such a vital and essential program.

Industry Governance

Currently, there are a few organizations that govern the overall Business Continuity industry. The Disaster Recovery Institute International (DRII) and the Business Continuity Institute (BCI) are the two major governing bodies that are responsible for defining and developing business continuity practices as well as certifying business continuity professionals.

DRII is prevalent in North America, while BCI is more dominant in other parts of the world. In addition, there are other standards such as the International Organization for Standardization - ISO 22301:2019 Societal Security – Business Continuity Management Systems, or the National Institute of Standards and Technology - NIST 800-34, which provide similar implementation guidelines.

In Canada, the public sector is governed by the Treasury Board Security Management directive, which outlines BCM practices in federal government agencies and departments.

Provinces and territories have their own regulations that govern some parts of the Business Continuity Program, for example, Emergency Management procedures. Specific industries (e.g. Financial) have their own rules, which could differ from the standards mentioned above.

Countries around the world have similar government or regulatory organizations which are governing Business Continuity guidelines and regulations.

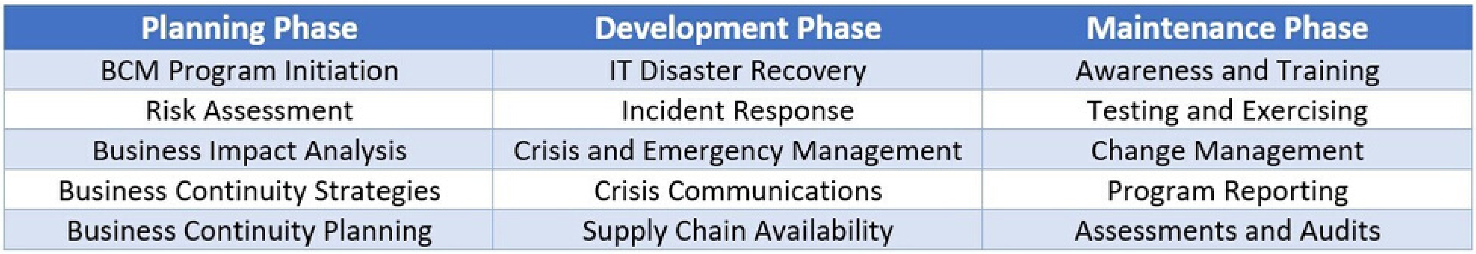
Most smaller organizations are free to choose the business continuity standard which will meet their organizational, regulatory or vendor requirements.

What is Business Continuity Management?

A leading business continuity industry standard, ISO 22031:2019, defines BCM as a "*holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.*".

This statement is quite a mouthful, but it boils down to the identification of organizational threats, management of their impacts, and building response strategies to protect critical resources.

The BCM program contains three distinct implementation phases; its activities are outlined in the table below.



Planning Phase	Development Phase	Maintenance Phase
BCM Program Initiation	IT Disaster Recovery	Awareness and Training
Risk Assessment	Incident Response	Testing and Exercising
Business Impact Analysis	Crisis and Emergency Management	Change Management
Business Continuity Strategies	Crisis Communications	Program Reporting
Business Continuity Planning	Supply Chain Availability	Assessments and Audits

There are many different activities and practices required to implement a successful and effective BCM Program in an organization. The critical point a business needs to understand is that the program implementation and its maturity will require some time and effort across the organization.

We all recognize that running a small or medium-sized organization is not easy and not without challenges. The organization's senior leadership team (SLT) is continuously pressured by quarterly revenue numbers, new products or services, competition and future growth concerns.

There is not much time to deal with "non-essential" business problems. As such, the implementation of a BCM Program is typically not high on the priority list. The management continually fails to recognize that the organization is not equipped to weather the next big emergency or crisis.

This is why Business Continuity Management (BCM) is a program and not a project. Business continuity planning is an activity which an organization should execute and continue to mature on an ongoing basis. The long-term future of your organization might depend on it.

Where to start – BCM Program Implementation Drivers

An organization's BCM Program implementation should start with research and understanding which business requirements are driving its implementation. Although it is an excellent idea to implement a BCM Program in all organizations, it could be required if an organization needs to meet some of the following scenarios:

- Regulation and compliance requirements – the organization is required to develop and implement a robust BCM Program to meet industry requirements
- Client or customer demands – depending on the type of services an organization provides to its clients, it may be mandated to implement business continuity and IT disaster recovery plans
- Business insurance needs – some business interruption policies are requiring organizations to implement business continuity programs. An added benefit to a more resilient organization will be lower insurance rates

These are just a few examples. The main reason to implement a BCM Program is that it will ensure that an organization embraces resiliency as part of its core values. This process exists to support the organization's mission statement, and not just to appease senior leadership, board members, or to meet industry regulatory requirements.

BCM Program Team

The implementation of the BCM Program will touch all parts of an organization. Therefore a BCM team should be selected across all organizational functions: finance, operations, communications, legal and information technology as well as any other key departments.

Once the team is selected, a member of the BCM Team should be chosen to be the program leader. The BCM Program leader will drive its implementation and will be responsible and accountable for all program activities once implemented. An alternate leader should also be selected to ensure program leadership resiliency.

Additionally, several members leading a BCM Program implementation may be chosen to form a Crisis Management Team (CMT), which will be responsible for managing disruptive business events and leading the organizational recovery efforts. Typical members of a CMT are outlined later in this book.

A quick tip: When selecting a BCM Program team, choose members who fully understand the inner workings of organizational functions they represent such as Directors or Managers.

BCM Program Policy

The program policy is a document that outlines all high-level aspects of the BCM Program implementation in an organization. This document should contain information as per the guideline below:

- Program scope and purpose
- Governance structure
- How often documents should be updated (Documents such as the Business Impact Analysis, Business Continuity Plan or IT Disaster Recovery Plan)
- Exercise, testing and program maintenance schedule
- Business continuity stakeholders training regime
- Reporting schedule, and other related information.

The BCM Program policy should be presented to the organizational leadership for review and approval. This approach will introduce some formality around the process, ensure senior leadership buy-in, and secure budget to maintain the program.

CHAPTER 3 - RISK ASSESSMENT

The idea of assessing risk in various situations should be familiar to everyone. Insurance companies assess risks to determine the insurance premiums they will charge. Investment firms assess risks to determine where and how to invest their client's money.

Ordinary people assess risks daily to guide their actions. Unsurprisingly, a risk assessment is one of the most important components of the Business Continuity Planning process.

Correctly determining the risks facing any organization's operations is essential for creating relevant business continuity plans, IT disaster recovery plans, emergency response and any other incident or crisis-related plans.

Risk Assessment can also enhance an organization's strategic decision-making abilities. It will increase an organization's awareness of threats and vulnerabilities, which will help management make informed decisions.

Additionally, the Business Impact Analysis (BIA) process outlined in Chapter 4 will leverage findings of the organizational Risk Assessment activity, which could be executed as a part of the BIA engagement.

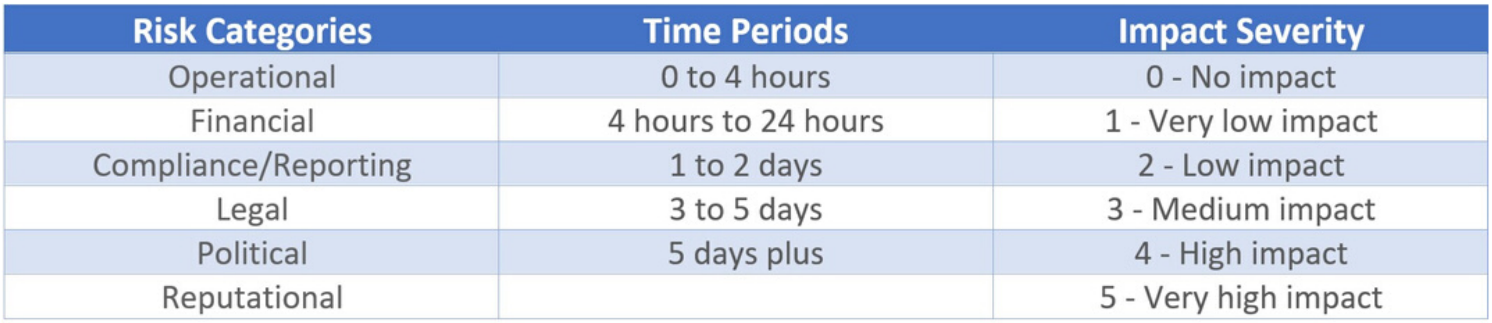
Risk Methodology

The Risk Assessment can be completed by using a traditional Operational Risk Management (ORM) methodology (for larger organizations), or an All-Hazards Risk Assessment (AHRA) approach.

The AHRA is defined as "*An approach for prevention, mitigation, preparedness, response, continuity, and recovery that addresses a full range of threats and hazards, including natural, human-caused, and technology-caused*" - NFPA 1600 Standard.

For smaller and medium-sized operations, and in the context of business continuity planning efforts, we recommend executing an AHRA approach. It will define the business functions and process risks and their impacts on business operations if disrupted.

Following the ISO 22301:2019 standard approach (impacts over time), some of the example risk categories, time periods, and impact severities an organization could assess are as follows:



Risk Categories	Time Periods	Impact Severity
Operational	0 to 4 hours	0 - No impact
Financial	4 hours to 24 hours	1 - Very low impact
Compliance/Reporting	1 to 2 days	2 - Low impact
Legal	3 to 5 days	3 - Medium impact
Political	5 days plus	4 - High impact
Reputational		5 - Very high impact

A risk matrix should be developed and used to assess and calculate the severity of impacts on each business process from each of the pre-identified risk categories and periods.

The risk matrix will allow the BCM Program team to assign a weight to each impact type. It will reflect risk significance and estimated probability relative to the other outlined impact types.

This risk matrix will be used during the Business Impact Analysis activity to calculate criticality and recovery priority of various business functions and processes.

A key component of the BCM Program is the execution of a Business Impact Analysis (BIA). A BIA execution will drive the rest of the BCM Program implementation.

Business Impact Analysis - BIA

BIA is a cornerstone of the Business Continuity Management (BCM) Program. It is an activity that will identify the organization's mission-critical business functions, processes or services, and the resources required to recover those activities in a timely manner. A properly executed BIA will reduce overall operational and financial impacts, reduce potential losses, and enhance the organization's business operations.

How does the industry define a BIA?

The Disaster Recovery Institute International (DRII) defines it as an activity to "*Identify and prioritize the entity's functions and processes to ascertain which ones will have the greatest impact should they not be available.*"

The Business Continuity Institute (BCI) definition of a BIA is a "*Process of analyzing the business activities and the effects that a business disruption might have upon them.*"

A simplified explanation: a BIA is a process that identifies the organization's critical functions and processes and the resources required to restore business operations.

Regardless of which industry association and best practice, traditional or adaptive BCM approach, or standard an organization decides to follow, this chapter will outline the importance of a BIA to Business Continuity Planning efforts and introduce inputs and outputs which go into a typical BIA engagement.

BIA Executed "the Right Way"

The BIA is an organization-wide activity. It is a project within the BCM Program. The BIA engagement will require a partnership with business stakeholders across all business units and departments. It will include every business function and will amplify the importance of an organization's Information Technology (IT) department.

One of the main challenges impeding a successful BIA implementation is that the engagement must be sized and fine-tuned for each organization. If not executed efficiently, the organization's stakeholders could quickly lose interest, and the BIA results could not meet BCM Program requirements.

Although BIA execution has to follow industry-leading standards and methodologies, it has to be completed in a way that will leverage the organization's size, culture, business style and operational resilience requirements.

BIA Engagement Inputs

To successfully start a BIA engagement, an engagement team will need to gather essential organizational information such as:

- **Business functions, process or service information** – at larger organizations, this is usually completed by the Enterprise Architecture (EA) group.
- **List of IT applications** - internally and externally hosted IT and business applications.
- **Contact information (Organizational chart)** - A responsibility of the Talent Management (HR) department (internal contacts), IT department (outsourced applications contacts) and vendor management department.

The above information will be used to map out the BIA engagement, identify key business stakeholders and better understand the business' complexity and its operations.

BIA Engagement Execution

The BIA starts with mapping out and leveraging the organizational inputs outlined above, which are used to develop a BIA execution plan and engagement toolset, which will include spreadsheets and training materials.

Once the BIA engagement plan and toolset are developed, they will have to be validated and approved by the Senior Leadership Team (SLT), which will continually be required to provide direction and guidance during the BIA engagement.

A significant part of the BIA engagement execution is stakeholder training. The BIA training will ensure that the engagement approach, terminology and expectations are fully understood across the organization. It will provide the "quality control" of captured data and, most of the time, will remove the stakeholders' "guesswork." The training can typically be completed with in-person meetings (smaller organizations) or over video-conferencing technology (larger or distributed organizations).

BIA Engagement Outputs

The BIA engagement, once completed, will produce a set of findings that will be used to develop recovery strategies, Business Continuity Plans and IT Disaster Recovery Plans. The developed BIA tools (in-house developed or leading BCM software platforms) could be used to streamline the process and capture the following information:

- **inter-dependency** of functions and processes (internally and externally)
- **recovery priority** of business functions, processes and IT applications
- availability of **Standard Operating Procedures** (SOPs) and manual workaround procedures for business processes
- **compliance and regulatory** fines and reporting requirements
- **alternate site** and **technology requirements** (ability to work remotely)
- business process **essential records** (electronic or paper files)
- **external vendors,** suppliers and Service Level Agreements (SLAs).

On the IT side, the BIA will define Recovery Time Objectives (RTO – how long can you be without the service) and Recovery Point Objectives (RPO – how much data are you willing to lose) as well as business function application dependencies. These findings will be used to develop recovery strategies and to ensure the IT Disaster Recovery Plan aligns with business requirements.

BIA - the letter "A" stands for Analysis

The critical step of the BIA engagement is the analysis of captured data and the development of a Business Impact Analysis report, to outline key findings and key recommendations to the senior organizational leadership.

Some of the typical BIA report results are as follows:

- outlining **Business Continuity Strategy** requirements and the alignment with the **business requirements**
- identifying **key personnel** and providing opportunities for critical functions cross-training
- ensuring that **Standard Operating Procedures (SOPs) and manual workaround procedures** are documented
- aligning the **IT Disaster Recovery Plan** to the BIA requirements
- ensuring that **vital electronic records** are backed up to enable the recovery of business functions and processes.

Vendor Risk Management

When developing organizational continuity plans, third-party providers (e.g. managed service providers, cloud-based providers, external service providers) and suppliers must be included in the planning process. The internal recovery plans of vendors and service providers must be be taken into consideration.

The Service Level Agreements (SLAs) provided by these vendors must align with the organization's business continuity requirements. If the SLAs are not meeting business recovery requirements, they will need to be reviewed and possibly re-negotiated with the vendors.

BIA findings might surprise you

Most of the time, a BIA will uncover some unintended facts, such as a business' inability to answer some critical questions, or IT findings, which will surprise everyone.

For example: where are IT Applications hosted; lack of organizational understanding of third-party service contracts and Service Level Agreements; the fact that shadow IT exists; and that IT is not in charge of all business applications.

The bottom line is, a BIA can be complicated to execute, however it is a must-have process to execute in any organization. If not executed properly, BCM Program stakeholders can quickly lose interest, and the BIA findings will not meet long-term business objectives and goals.

While implementing a BCM Program, and as a side benefit, an organization will learn more about their business. Many organizations uncover business areas and processes which require improvements to ensure the long-term effectiveness of their business operations.

Once completed, the Risk Assessment and Business Impact Analysis will provide a solid foundation for the development of an organization's business continuity strategy.

Organization-wide Planning

The development of a business continuity strategy will require high level of support from the internal or outsourced IT organization. IT will need to research, price and present technology options that will meet or exceed an organization's resiliency requirements outlined in the BIA. Examples of IT options are: secondary data centres, migration to cloud-based services, or outsourcing part of IT operations. A BIA and Business Continuity strategy will be key inputs for the development of a robust IT Disaster Recovery plan.

In addition to the technology delivery strategies, examples of business continuity strategies an organization will need to address are:

- Workaround procedures – some processes could be completed by executing manual workaround procedures.
- Work area requirements – the ability to deliver services from an alternative location, or remotely, when business facilities are not available. Decision points are to build, lease or procure an additional site.
- Split team operations – the possibility of splitting functional teams at alternate buildings to reduce outage impacts to operations (e.g. manufacturing facilities).
- Vital records management – development of a data and paper records protection strategy.
- Reciprocal agreements – agreements with mission-aligned organizations to provide space or technology capacity on demand.
- Third-party providers – contracting third-party providers to provide additional capacity and capability when required (e.g. cyber IT firms, cloud based IT infrastructure).
- Wait it out – do-nothing approach; this is not a suggested strategy, but it could be the best choice in certain circumstances.

Options Cost-benefit Analysis

A critical part of the business continuity strategy process is a recovery options cost-benefit analysis, as strategies must meet budgetary program requirements. Selected strategies will have to balance the realm of possibilities and practicalities and fit the overall organizational business continuity requirements. The business continuity strategy should therefore be balanced, as its approach will drive the rest of the BCM program.

When developing a business continuity strategy, an organization must ensure that selected recovery options and approaches meet its industry regulatory and compliance requirements.

A quick tip: Business Continuity strategy development will need to be completed collectively with the business and IT organizations. Expect some negotiations within the business to ensure that business continuity requirements fit the selected continuity and recovery strategies.

A Business Continuity Plan (BCP) is a document that details how an individual organization will continue to perform its essential functions during a wide range of events that could impact normal operations.

This document should capture the information gathered in previous phases (Risk Assessment, BIA and business continuity strategy) and present it in a logical way, which will assist an organization in recovering during and after a disruption.

Before developing a BCP, an organization will have to select BCM Program resources, which will lead its operational recovery during unexpected events. This team will consist of business and IT decision-makers and will form a Crisis Management Team (CMT). An example of a CMT team is as follows:

- **Chair and vice-chair** (a vice-chair will provide redundancy and continuity)
- **Business Continuity Manager** (a person responsible for the overall BCM Program)
- **Business operations managers** (talent management - HR, finance, legal, etc.)
- **Communications representatives** (internal and external communications)
- **IT Organization** (internal and external if outsourced)
- **Facilities and physical** security representative
- Other representatives **as required**

A Business Continuity Plan Document

A BCP should be a go-to guide during disruptive events, and it must include all the information a BCM Program team will require to assess and recover organizational functions and processes successfully. A typical BCP should contain the following information:

- **Roles and responsibilities** – this section should outline who are the organizational resources responsible for BCM Program implementation and selected CMT members.
- **Decision-making process** – document who will lead recovery during and after an incident or a crisis (e.g. an IT organization will lead IT-related events).
- **Call trees** – a list of whom and when to call.
- **Critical event criteria** – establish criteria which could trigger an organization's recovery efforts such as negative corporate news, technology events, or employee-related events.

- Meeting locations – outline where and how a CMT will meet to lead the organizational recovery (e.g. teleconferencing information, office space). This has to be completed in conjunction with an Emergency Management Program (an activity separate from business continuity planning efforts).
- Incident assessment process – outline how an organization will assess, as an example, damage to the facilities, an IT outage or any other scenarios.
- Detailed response and recovery plan – outline response strategies required when facilities are affected, staff reduction occurs (influenza or pandemic plan), and full or partial loss of business functions or services occur.
- Activation and deactivation procedures – an operational guide on how to activate (what circumstances) and how to de-activate BCP.
- Return to normal procedures – outlines what has to be done once the incident or a crisis is resolved. Examples are workload management, communications, etc..
- Contact information – a list of all internal or external contacts such as external vendors, legal counsel, and temporary space providers.
- Business functions recovery procedures – a detailed guide on how to recover individual functions and processes, and their recovery priority.

Communication and Notification

A critical element of managing disruptions is an ability to effectively communicate, both internally and externally, with staff and with customers/clients.

A communication plan must provide a playbook for how the organization will communicate its BCP (this can be a separate document, or it could be included in the BCP). It should consist of how-to guides for all the organization's communication platforms, such as email, Twitter, website, phone messages, and collaboration tools.
It should clearly outline who can provide messages during a disruption, and who all inquiries (e.g. media) should be directed to.

The ability to provide a consistent message in a crisis is key for managing organizational reputation, and it will minimize impacts after the disruptive events.

Emergency Notification Platform

An organization should consider how it will maintain communication with internal or external resources during disruptive events. Weather-related events (earthquakes, tornados, freezing rain) or more serious, physical security-related events (workplace violence) require continuous communication to ensure the well-being of staff, clients and third-party vendors once on site.

These communications and notifications can be delivered through a mobility telephony provider short message service (SMS), or other third-party notification software platforms. An organization should evaluate BCM Program requirements and select an appropriate approach.

A quick tip: Don't forget to plan how to notify third-party vendors, clients or consultants when on premise.

Business Continuity Documentation

Secure electronic and physical storage of Business Continuity Plans and procedures are essential when disaster strikes. The availability and access to documentation that will guide the organization will make a considerable difference between timely or delayed recovery efforts.

Our recommendation is to evaluate different documentation storage options and their respective availability capabilities. A cloud-based solution might provide better availability than locally stored data solutions, the access of which could be impacted by IT-related incidents.

Third-party crisis notification and management tools could also be deployed, which, as a bonus, can store all organizational business continuity and recovery documentation.

A quick tip: When developing organizational business continuity plans, ensure coordination with the facilities management organization (landlord) and external agencies (emergency services). As an example, emergency services response will trump your organization's recovery plans in some life or death situations. This has to be coordinated in advance and well before an emergency.

When asked about their organization's IT Disaster Recovery (ITDR) plans, some will smile and say, "Yes, we have a backup, and it is fully outsourced."

IT systems and applications are an integral part of all organizations' operations and can pose unique challenges and needs in terms of disaster recovery. An IT disruption can completely halt operations, and recovery often requires specific skills, detailed planning and testing.

ITDR Planning depends on Business Impact Analysis (BIA) and Risk Assessments

The goal of ITDR planning is to prioritize the recovery of various IT systems and applications and to ensure that recovery capabilities meet operational business requirements.

The first steps in successful ITDR planning is understanding business recovery requirements, which IT systems and applications an organization uses, and determining which specific functions or services they support. Some functions may have manual workarounds, but many tasks cannot be performed without the available IT systems or applications.

For example, there may be a way to manually process payments if the need arises, but there is no way to respond to customer emails without access to the Internet.
However, being aware of these dependencies is only part of the planning process. The matter is further complicated by the presence of service/function inter-dependencies as very few processes happen in a vacuum.

Organizational functions depend not only on the IT systems that support them but also on other functions and services (as outlined in Chapter 4 - internal and external to the organization). To accurately prioritize the recovery of IT systems, organizations cannot ignore their indirect importance to all functions.

Recovery Time and Recovery Point Objectives

Once an organization has mapped out all dependencies and inter-dependencies (Business Impact Analysis process), they can then evaluate their Recovery Time and Point Objectives and their recovery capabilities.

In simple terms, Recovery Time Objective (RTO) means how long an organization can be without a specific IT service or application. A Recovery Point Objective (RPO) will outline how much data an organization is willing to lose before having a material impact on its operations.

This step is where the idea of having a backup often gives organizations a false sense of security. Many do not realize that the mere presence of data backups does not guarantee that services will be able to come back online in the required time and in the required order.

As an example, an organization may have requirements to restore all emails up to the last 6 hours before an incident, within a time period of 4 hours, to restore the service following the incident. Unfortunately, email server data backups may only have emails from up to 1 day before the incident, and it may take 12 hours following the incident to have the data restored.

This gap between recovery requirements and capabilities can create problems while also being completely avoidable.

Proper ITDR planning will allow an organization to address any such gaps in order to become truly resilient. Having an accurate idea of recovery requirements and capabilities will also allow an organization to perform a cost-benefit analysis to determine which solutions are right for it.

IT Disaster Recovery

A typical IT Disaster Recovery Plan will contain the following information:

- IT plan goals and objectives
- data backup and resiliency information (how often data must be backed-up to meet organizational and regulatory requirements)
- assumptions and scenarios (what IT disaster scenarios the plan will address)
- IT staff roles and responsibilities
- IT infrastructure and applications recovery strategy such as a secondary data centre and/or a cloud-based recovery
- assessment, activation and deactivation instructions
- maintenance and plan testing instructions
- password keeping information
- communication strategy
- IT team and external vendor contacts
- other relevant information

<u>A quick tip</u>: An IT Disaster Recovery plan does not have to contain all IT information in it. It could reference other internal and more detailed IT infrastructure, services and recovery documents. The availability of these documents will need to be taken into consideration, which could minimize the impacts and increase recovery capabilities.

You may find this statement in a lot of our documents, presentations and speaking engagements: "An Untested Plan is ONLY a Strategy." Let that sink in for a moment.

The previous planning phases are finally completed. Your organization went over countless hours of mapping out business requirements and developing plans and procedures. Now it is the time to celebrate, store the binders in cabinets, and forget about them. Next challenge, please.

Joking aside, this is what happens in most organizations once they complete their business continuity plans. Plans are not distributed to the staff. The organization's resources are never trained on how to execute these plans. They are never tested or exercised. Nobody knows where they are stored. The executives are too busy to even look at them.

It is a recipe for disaster.

Test, Exercise and Continuously Improve

Will the staff follow the planned response procedures precisely as they are outlined in the plans? Or, will they just follow their instincts and do whatever they think is right at the time? How well will various stakeholders work together, including the coordination with external agencies?

The testing and exercising of the plans and procedures are vital for successful mission-critical function recovery during disruptive business events. An organization's resources will need to know what to do, whom to call, where to go, how to communicate and how to perform critical tasks, to ensure that an organization recovers its functions and processes in the planned timeframe.

This can only be achieved with a comprehensive business continuity testing program, which will evaluate and exercise all the organization's recovery plans. These exercises, once executed, will produce actionable improvements that an organization can use to improve and mature its BCM program components.

Some of the testing and exercise delivery options are as follows:

- Walk-through exercise - review of documented recovery procedures to check overall plan viability.
- Tabletop exercises - exercises in which participants review and discuss the actions they would take without actually performing the actions. Representatives of a single team, or multiple teams, may participate in the exercise, typically under the guidance of exercise facilitators.
- Functional exercises - functional exercises examine and/or validate the coordination, command and control between various business functional teams such as finance, operations and talent management.
- Full-scale functional - evaluation of the effectiveness or ability of all components of a recovery strategy by relocating services to the recovery site(s).
- IT Disaster Recovery tests – full-scale (a site cutover) test.

A quick tip: Establish an annual or semi-annual organizational testing and exercising regime, and test all business continuity plans within the organization.

Business Continuity Training and Awareness

We know that people love new challenges and that many can't stay long in their positions and organizations. Some organizations have quite a significant internal (people moving between positions) or external (people coming in or leaving the organization) turnover that can cause considerable problems with their business continuity planning efforts.

Integration of the BCM Program and the organization's Talent Management department (HR) initiatives will ensure that an organization's most valuable resource, its people, will know what to do and how to act when disaster strikes. Business continuity training must be delivered as a part of leadership or new employee training initiatives. It will introduce individual business resilience expectations and accountability across the organization.

Robust training and awareness programs will ensure that staff are ready to execute recovery plans and minimize operational impacts.

A quick tip: An organization can create visual guides (videos) and documentation (brochures and manuals), to be distributed as part of staff on-boarding initiatives.

CHAPTER 9 - BCM PROGRAM MAINTENANCE

A BCM Program should never end. The maintenance of the BCM Program components must be completed at least once or twice a year, aiming to capture all changes within the organization.

Some more significant BCM Program initiatives, such as Risk Assessment or Business Impact Analysis, could be completed on a biennial schedule. Some of the examples which will drive BCM program maintenance requirements are as follows:

- New or transformed business lines
- Added or removed business functions or processes
- Staff and resource changes
- IT applications changes
- Vendors or third-party changes.

If not maintained properly, the BCM Program will become less relevant over time and the organization will be more vulnerable to business disruptions.

The changes outlined above will have to be documented on a regular basis (as defined in the BCM policy), and staff will need to be continuously trained to maintain the overall effectiveness of your plans.

Consultants can be an excellent tool for BCM Program implementation, although they may not be available for long-term maintenance and training activities. To address this challenge, some BCM advisory and consulting firms offer a service to capture and manage all program changes (such as our BCMaaS).

A BCMaaS can be a cost-effective approach once the advisors and consultants complete the planning and implementation process and move on to the next client.

BCM Program Assessments and Audits

Business Continuity standards, guidelines and industry regulations change from time to time. They are continuously maturing and evolving, which could render some of the organizational BCM Program components out of compliance.
As a general rule, it is a best practice to assess and audit the BCM program regularly (every two to three years). An audit will identify the gaps and present the recommendations on how to update and align the organization's BCM program with the latest requirements.

The effectiveness of the BCM Program will depend on the organization's ability to embrace resiliency as part of its core values. Once implemented, business resilience will be engrained in the organization's way of life.

BCM Program implementation and its maintenance is a process. It should be delivered in phases, so an organization can implement it and mature it over time. There will be challenges along the way, but they can be addressed with executive and stakeholder support.

Accountability

Many organizations have implemented formal management accountability frameworks that define sound management practices and performance expectations. Unfortunately, at some organizations, accountability is a loose term.

Resilient organizations, regardless of their size, are embracing business continuity accountability at all levels. Senior leadership must lead by example, and business continuity accountability should be a part of their performance process.

Additionally, mid-level management and employees must be responsible for their business functions and processes. This is imperative to ensure that the organization is ready to respond when an unexpected event disrupts their operations.

Business Continuity and Business Integration

Business continuity must be at the forefront of any organization's business planning initiatives. It should be introduced early on in the new business function, process or new service planning discussions. Business Continuity Managers should be included at the senior leadership table.

Not integrating Business Continuity and IT Disaster Recovery at the outset of business discussions, processes or service design will potentially introduce re-work, demoralize the team, and lower customer satisfaction. It will be more challenging to introduce resilience once the product or service is already “in production". Many successful organizations realize that operational resilience builds over time, and it is introduced into their daily processes and procedures.

In Conclusion

BCM Program implementation can be a challenge for small and medium-sized organizations with limited resources. Smaller organizations are typically understaffed; adding another role to somebody who is already stressed by their workload will not lead to the desired outcomes.

BCM practitioners see a few organizational problems while implementing BCM Programs at smaller organizations. At the high-level, they can be categorized into two areas:

Business challenges

- lack of **documented** organizational charts and business **functions/processes** maps
- the business procures many **cloud-based services** (Software as a Service – SaaS), but rarely understand the vendor Service Level Agreements (SLA's), service resiliency or data residency/recovery **capabilities**
- lack of documented **Standard Operating Procedures** (SOP's) to execute business functions and processes.

IT Organization challenges

- **applications and software** used across the organization are not documented
- **shadow IT**, a situation when applications are installed without business and IT knowledge, which can cause organizational data leaks and data fragmentation
- IT Disaster recovery planning, and sometimes the IT organization as a whole, is **disconnected** from the rest of the business continuity planning activities.

The above points are just a few of the examples, but they summarize the key challenges which most organizations have to address in order to successfully implement the BCM Program.

We have discovered that a BCM Program is critical to an organization's success. Its implementation is vital for any organization that cares about its people, its clients and the overall long-term viability of its operations.

Is <u>your organization</u> one of those?