



**WE'RE OPEN FOR BUSINESS:
A PRACTICAL GUIDE FOR MSME BUSINESS CONTINUITY**



Global Affairs
Canada
Affaires mondiales
Canada



Organization of
American States



UWI

Disaster Risk Reduction Centre
**Enhancing Knowledge
and Application of
Comprehensive
Disaster Management**
(EKACDM) Initiative

Developing your Business Continuity Plan

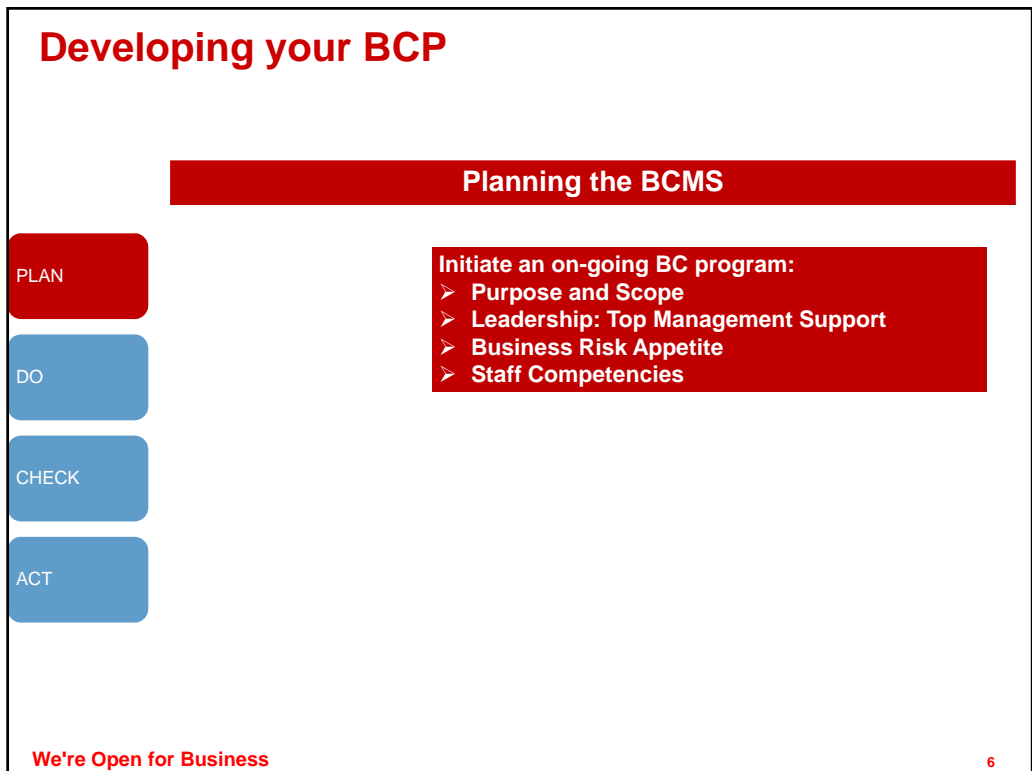
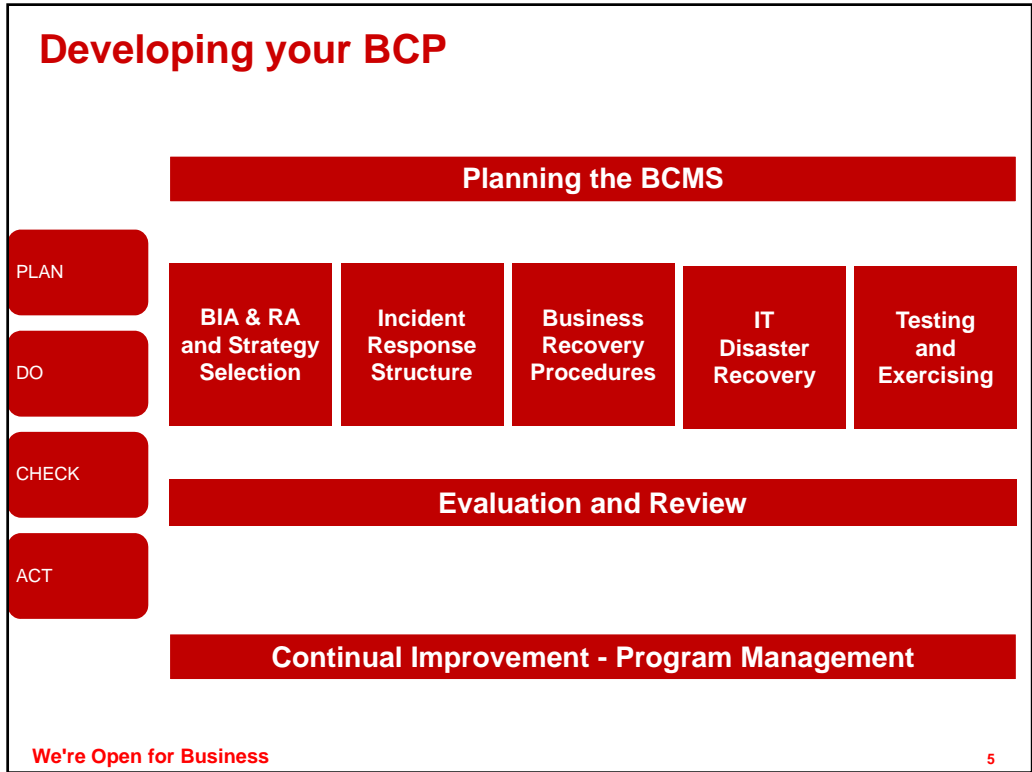


What does the flashing red light
mean?

3

Developing your BCP

- In 2012, a new international standard for business continuity management, **ISO 22301 - Societal security - Business continuity Management Systems** – was released by the International Standards Organization.
- This BCM standard is intended to be applicable to all organizations, regardless of **type, size or nature** of the organization.
- It promotes a gender-neutral approach to BCM, in that its focus is on the **impact analysis of business disruptions** on key business activities, such as the loss of key staff, resources or technology, and the identification of strategies to enhance the resiliency of an organization.



Developing your BCP

- Every BCP has four main objectives:
 - protect your **PEOPLE** – your staff, your customers, and other visitors to your business premises
 - protect your **PROPERTY** – your business premises, your equipment, your assets
 - protect your **PROFITS** – your finances, your operations, your relationships with your staff, your clients and your suppliers
 - protect your **PROSPERITY** – your business reputation, your relationships with key stakeholders, such as your bank, your investors, your insurance company – your long-term business survival
- Every business needs to clearly define its own purpose in developing a BC program; this will help determine its priorities when identifying **KEY BUSINESS ACTIVITIES** and when creating strategies to protect its key products or services.

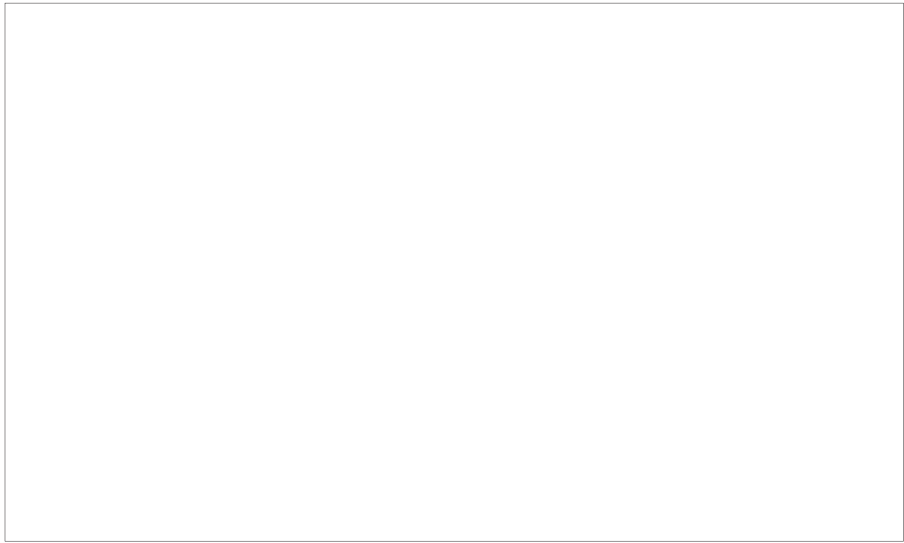
Developing your BCP

SCOPE

- Rarely does a Business Continuity Plan protect all aspects of a business. Typically, a BCP is intended to ensure that your **KEY BUSINESS ACTIVITIES** will not suffer **UNACCEPTABLE** losses.
 - What aspects of your business are the most important – to you, to your employees, to your major clients, etc.?
 - Will your BCP cover all aspects of your business, or will it focus on certain locations, or certain products, or certain activities?
 - The scope of your BCP will play a significant role when looking at your Business Impact Analysis and Risk Assessment.
- Creating a BCP that will keep your business running under every contingency is the main purpose of a BC Plan; creating a good-looking document that will just sit on a bookshelf is not.

Determine the Scope of your BCP

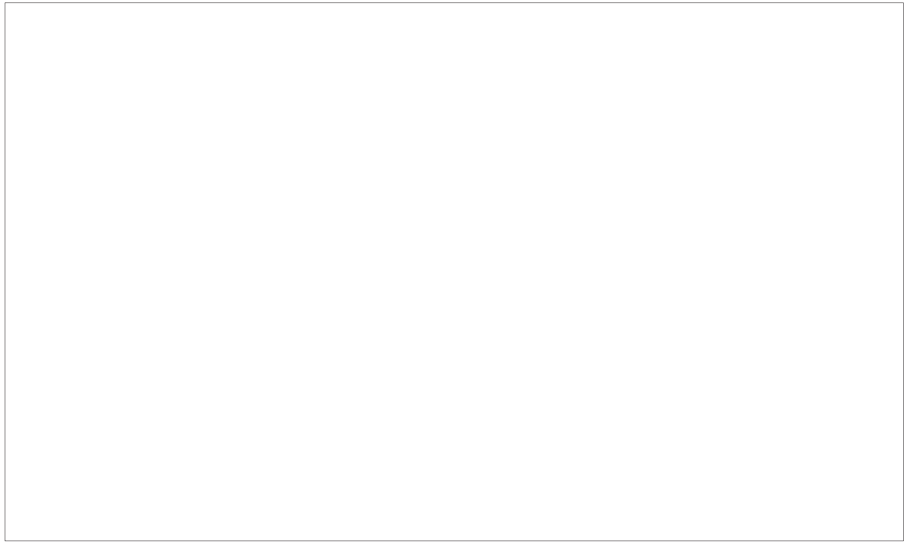
What is your business? Why are you in business?



We're Open for Business 9

Determine the Scope of your BCP

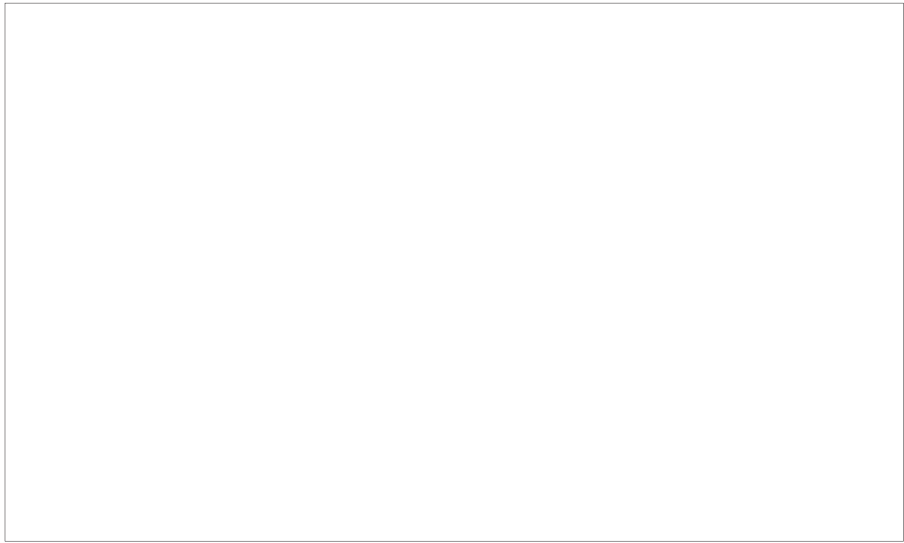
What products or services do you provide?



We're Open for Business 10

Determine the Scope of your BCP

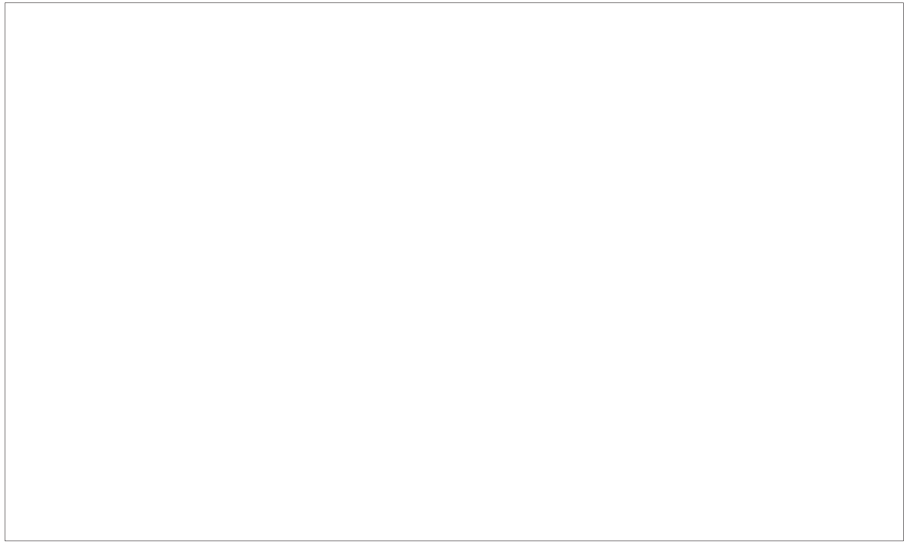
How do you provide your products/services?



We're Open for Business 11

Determine the Scope of your BCP

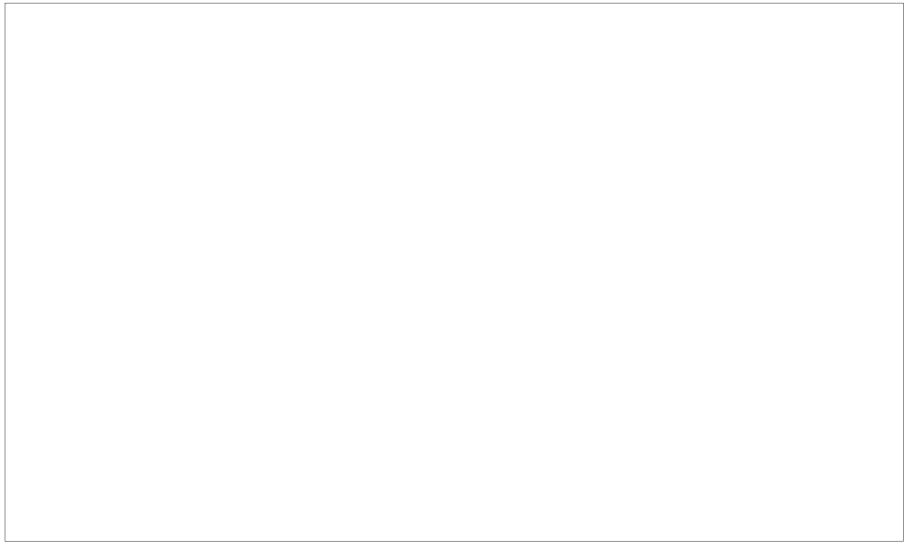
Who are your employees? What are their major duties?



We're Open for Business 12

Determine the Scope of your BCP

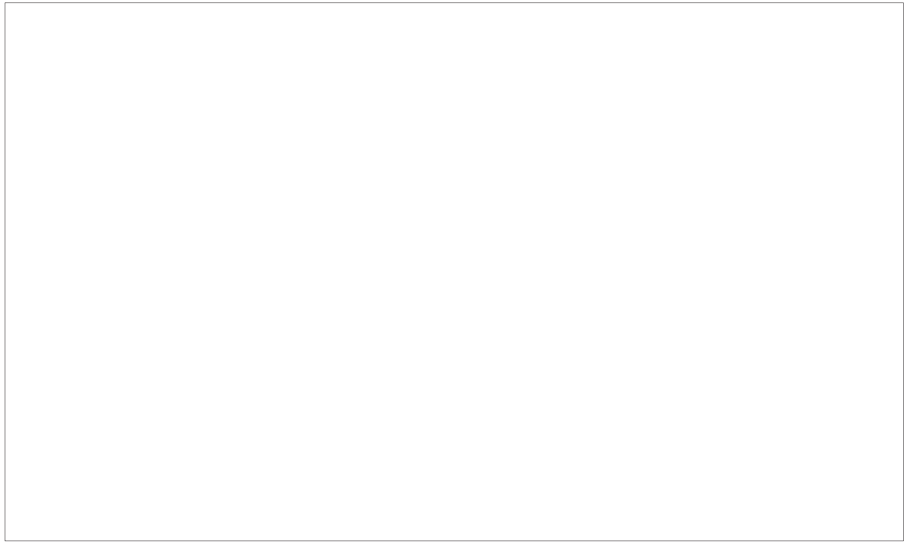
Who are your major suppliers?



We're Open for Business 13

Determine the Scope of your BCP

Who are your major customers?



We're Open for Business 14

Business Risk

- Every business has to take some risks and avoid others.
- Risk appetite can be defined as ‘the amount and type of risk that a business is willing to take in order to meet its strategic objectives’.
- A business will have different risk appetites depending on their sector, culture and objectives. A range of appetites exist for different risks and these may change over time.

Business Risk

Risk Outcomes



Positive risks can result in good things happening: *sometimes called “opportunities”*

Negative risks involve understanding potential problems that might occur: *can be defined as “threats”*

By treating the negative consequences of an incident, business continuity management can **create opportunities** for benefit and gain.

A business that responds positively to a disruptive event can position itself to **recover quickly** and improve its long term business performance

Determine your Risk Appetite

What parts of your business do you need to protect? Why?



We're Open for Business 17

Determine your Risk Appetite

What would you do if these parts of your business were not available?



We're Open for Business 18

Developing your BCP

Planning the BCMS

PLAN

DO

CHECK

ACT

**BIA & RA
and Strategy
Selection**

BUSINESS IMPACT ANALYSIS & RISK ASSESSMENT
Identify and analyze time-sensitivity of business interruption, such as:

- Loss of revenue
- Loss of market share
- Loss of reputation
- Loss of productivity
- Regulatory non-compliance, etc.

STRATEGY SELECTION
Select and implement appropriate strategies for:

- Reducing risk
- Reducing impact
- Resuming key business activities

We're Open for Business
19

Developing your BCP

BUSINESS IMPACT ANALYSIS

- The purpose of a BIA is to help you determine which products or services should be recovered as your first priority when a critical incident disrupts your business. These are called your **“key business activities”**.
- For a small business, this is often very obvious: what is your top selling product? Who are your most important clients?
- For a larger business, such as a hotel, what are your priorities should half your staff not show up for work? New reservations, Front Desk, Gift Shop, Food and Beverage, Housekeeping, Facilities Management, Security?

We're Open for Business
20

BIA Data Collection

1. The first step is to define the **types of impact** that are important for your business, and to establish criteria for ranking the impacts based on their level of **severity**

Five Impact Categories:

- 1. Financial
- 2. Reputational
- 3. Legal and Regulatory
- 4. Contractual
- 5. Business Objectives

Example severity levels:

- **Low** impact: undesirable, but tolerable
- **Medium** impact: very undesirable, but unlikely to have a long term effect on the business
- **High** impact: highly undesirable, and likely to have some long term effect on the business

List of Business Impacts

Business Impacts	Low Impact	Medium Impact	High Impact
Financial			
Reputational			
Legal and Regulatory			
Contractual			
Business Objectives			

BIA Data Collection

2. The second step is to **identify** all the Business Activities performed by your business

Keep in mind the following considerations:

- A **Business Activity** is “a process or set of procedures undertaken by an organization that produces or supports one or more products and services” (e.g. Accounts Receivable is an activity, Invoice Reconciliation is a procedure)
- **All activities must be identified**, not just the acknowledged ‘important’ ones – in case of interdependencies
- Any **automated activities** must also be included
- If an activity is performed in more than one location, it must be listed for **each location**

Sample List of Business Activities

Business Unit	Business Activity
Finance	<ul style="list-style-type: none"> . Accounts Payable . Accounts Receivable . Financial Statements . Asset Management
Procurement	<ul style="list-style-type: none"> . Asset Acquisition . Asset Disposition . Purchasing
Marketing	<ul style="list-style-type: none"> . Marketing
Human Resources	<ul style="list-style-type: none"> . Employment function . Payroll
Administration	<ul style="list-style-type: none"> . Management Support
Information Technology	<ul style="list-style-type: none"> . Maintenance of IT infrastructure . Maintenance of telecommunication infrastructure

Identifying Key Business Activities

Key Business Activities

- **Key business activities have the greatest impact on your company's operations and potential for recovery.**
- **Key business activities are those activities that your company cannot do without. These should not be a surprise to almost anyone working in your business.**



Identifying Prioritized Activities

Important Business Activities

- **Important business activities will not stop the business from functioning in the near-term but their effects are usually felt in the long-term, if they are missing or disabled.**
- **If they are not there, these kinds of business activities cause some disruption to the business over time.**



Key Business Resources

- As part of the BIA, you will also need to identify the resource requirements needed for each key business activity, such as copies of operating procedures, key staff, records, systems, and equipment.

- Examples:
 - Key Business Activity: **HR will issue pay cheques to employees.**
 - Key Resources:
 - **blank cheques**
 - **staff** who know how to gather pay data and print cheques.

Key Business Resources

- **What are Key Business Resources?**
 - **Facilities or Work Sites**
 - **Communications Systems**
 - **Key Staff**
 - **Vital Records and Databases**
 - **Vital Technology and Equipment**
 - **Key Vendors**

- **i.e.: people, equipment, technology**

Traditional Risk Assessment

- Traditional Risk Assessments identify and analyze the “101 Things That Could Go Wrong” – hazards that could negatively affect an organization’s ability to deliver key products or services:
 - 1) Fire
 - 2) Flood
 - 3) Storm
 - 4) Hurricane
 - 5) Earthquake
 - 6) Tornado
 - 7) Asteroid
 - 8) Polar Vortex
 -
 - 100) Zombie Attack
 - 101) Alien Invasion

Invariably, it is the “102nd” thing that causes the problem – the one that wasn’t planned or prepared for!

Threats to Key Business Activities

- A business continuity event can be anything that has the potential to disrupt normal service delivery
- Essentially, all such events will be caused by either a **loss of a resource** (e.g. buildings, equipment, etc.), **loss of people**, a **loss of IT systems**, or possibly two or three simultaneously
- **The cause of the problem is usually immaterial:**
 - it doesn’t matter whether a building is inaccessible because it has burned down or is completely flooded;
 - it doesn’t matter whether a staff shortage is due to snow or a strike or a pandemic
 - whatever the case, the organization has to respond to a **loss of resource**

Threats to Key Business Activities

- In the BIA, we identified the resources each key business activity is dependent upon for normal operation
- Key resources may include:
 - Trained staff
 - Office facilities
 - Plant facilities
 - Workstations
 - Computer systems
 - Electronic data
 - Hard copy data
 - Voice communication systems
 - External network connectivity
 - Specialized equipment
 - Materials and supplies
 - Key suppliers, etc.
- In the Risk Assessment, we need to determine the extent to which normal operations would be disrupted by the loss of any of those key resources

We're Open for Business

37

Threats to Key Business Activities

Threat Assessment

Key Activity:

THREATS	SEVERITY				COVERAGE					EXPOSURE
	n/a	L	M	H	>20%	>40%	>60%	>80%	>100%	
1. Loss of work space										
2. Loss of manufacturing work space										
3. Loss of repair work space										
4. Loss of workstations										
5. Loss of inventory										
6. Loss of external suppliers										
7. Loss of power supply										
8. Loss of water supply										
9. Loss of key staff										
10. Loss of data files										
11. Loss of hard copy files										
12. Loss of cell phone service										
13. Loss of internet										
14. Loss of e-mail service										
15. Loss of website										
16. Loss of computer										

We're Open for Business

38

Identifying Strategies



Overlooking a serious risk can be dangerous

39

Considering the Options: the Basics

- The BIA will undoubtedly have identified numerous exposures that can be rectified with **relatively little time or expense** (e.g. cross-train staff where only one trained staff available).
- These are your 'quick hits'.



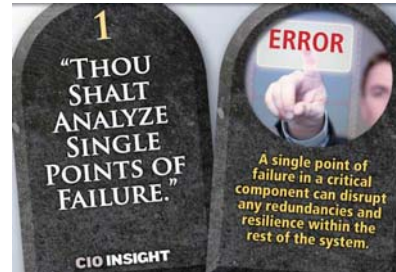
- Apart from the fact that these 'quick hits' are easy to do: acting on them will demonstrate **immediate value** from your efforts

We're Open for Business

40

Threats to Key Business Activities

- It is exceptionally important to identify any potential **'single points of failure'** within the resources supporting the various business activities
- Loss of a **'SPOF'** can lead to the failure of a key business activity
- **'Single points of failure'** may include:
 - Key staff with specialized knowledge
 - Equipment parts which cannot readily be replaced
 - Non-redundant communication links
 - Critical data which is not backed up
 - Telephone systems
 - Specialized equipment
 - **'Sole source'** suppliers, etc.



Considering the Options: the Basics

- **Minimize the Potential Impact of a Hazard**
 - Once you have identified the key risks your business faces, you need to take steps to protect your Key Business Activities should the risk materialize
- **Premises**
 - Think what you would do in a situation if your premises could not be used. For example, you might suggest an arrangement with another local business to share premises temporarily if an incident affected either of you.
 - You may consider using a business continuity supplier who can make alternative premises available at short notice (but this can be expensive).

Considering the Options: the Basics

- **Equipment/machinery**
 - If you use key pieces of equipment, you may want to cover them with maintenance plans guaranteeing a fast emergency call-out.
- **IT and Communications**
 - Installing anti-virus software, backing up data and ensuring the right maintenance agreements are in place can all help protect your IT systems.
 - You might also consider contracting with an IT company to regularly back up your data offsite on a secure server.
 - Printing out copies of your customer database might be a good way of ensuring you can still contact customers if your IT system fails.
 - Provide IT support systems to facilitate home working should the need arise.

Considering the Options: the Basics

- **People**
 - Cross-training staff is effective and inexpensive
 - Try to ensure you are not dependent on a few staff for key skills by getting them to train other people.
 - Consider whether you could get temporary cover from a recruitment agency if illness left you without several key members of staff. Take health and safety seriously to reduce the risk of staff injuries.
- **Supply Chain**
 - Consider stock piling critical supplies and materials.
 - Create a list of alternative suppliers should your main supplier be unable to deliver the goods and materials you require.

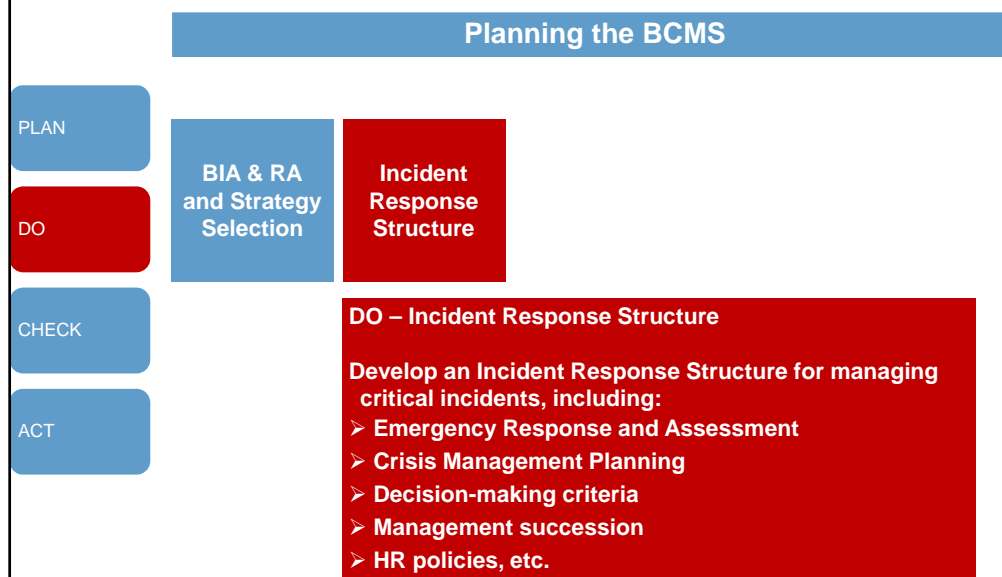
BC Strategies - Insurance

Insurance type	Policy Number	Policy coverage/exclusions	Insurance company and contact information	Last review date	Payments due

We're Open for Business

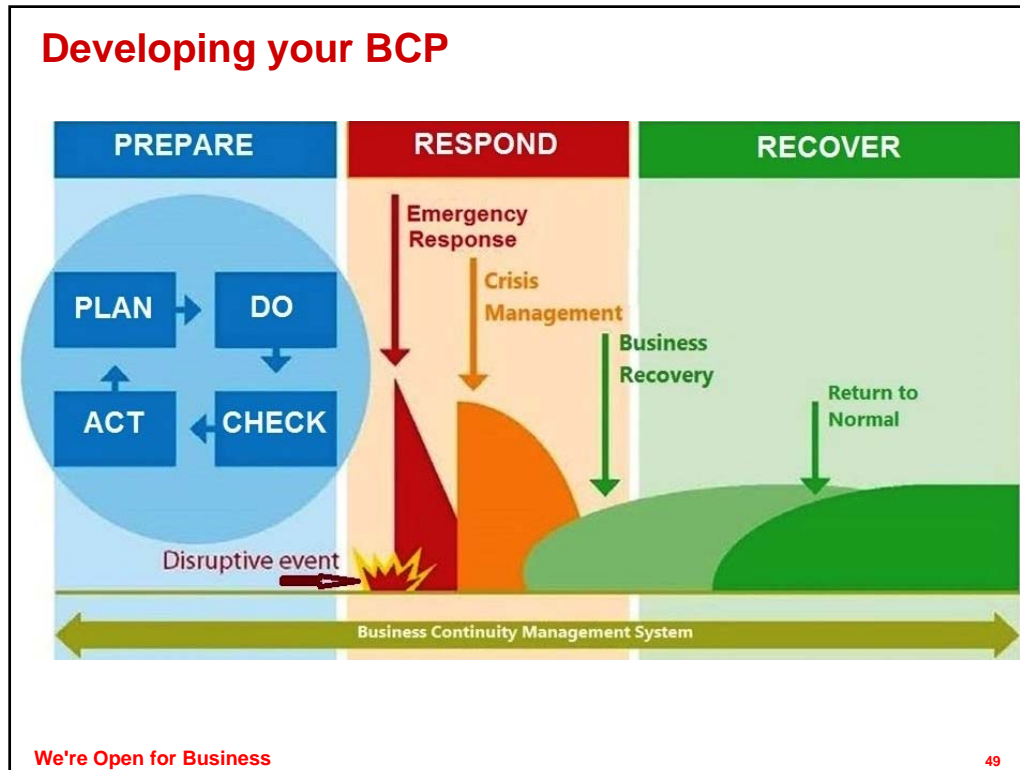
47

Developing your BCP



We're Open for Business

48



Emergency Response

Evacuation and Rescue

- Most companies already have an evacuation plan. If you do not have one, it should basic evacuation procedures and assembly sites.
- You need to make sure all employees understand the evacuation plan and are able to safely evacuate as planned. This is done by running evacuation drills.
- Some companies also give all employees a small laminated card containing key information such as what actions to take, where to assemble and emergency contact information.

We're Open for Business

50

Emergency Response

Sample Evacuation Plan:

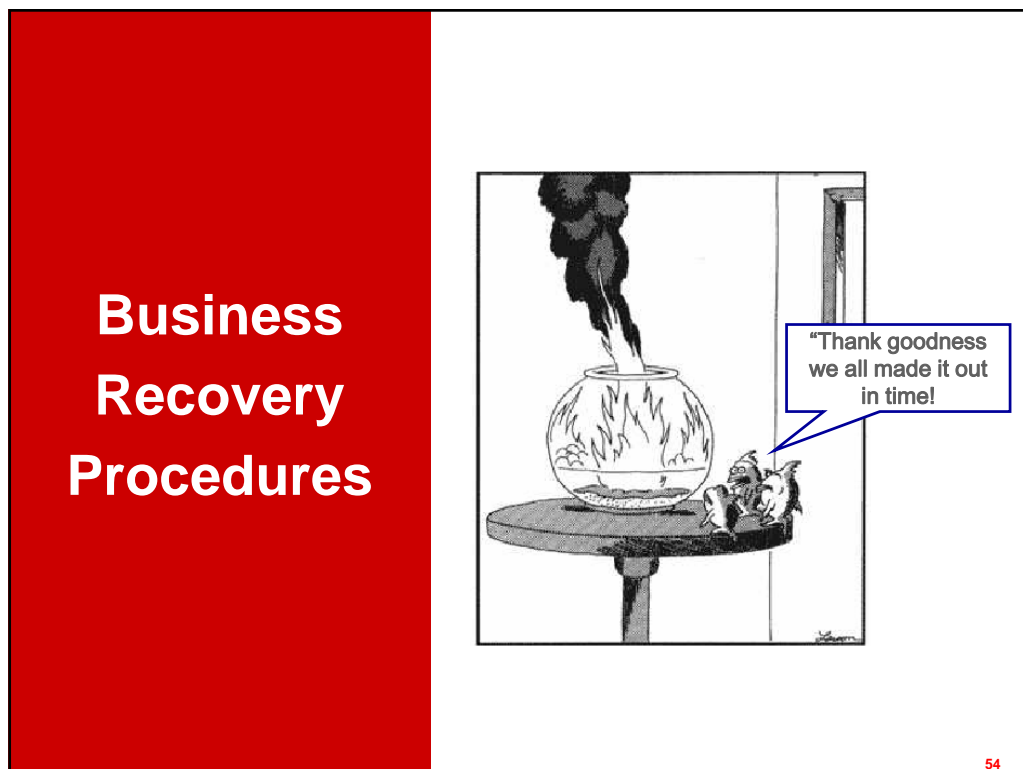
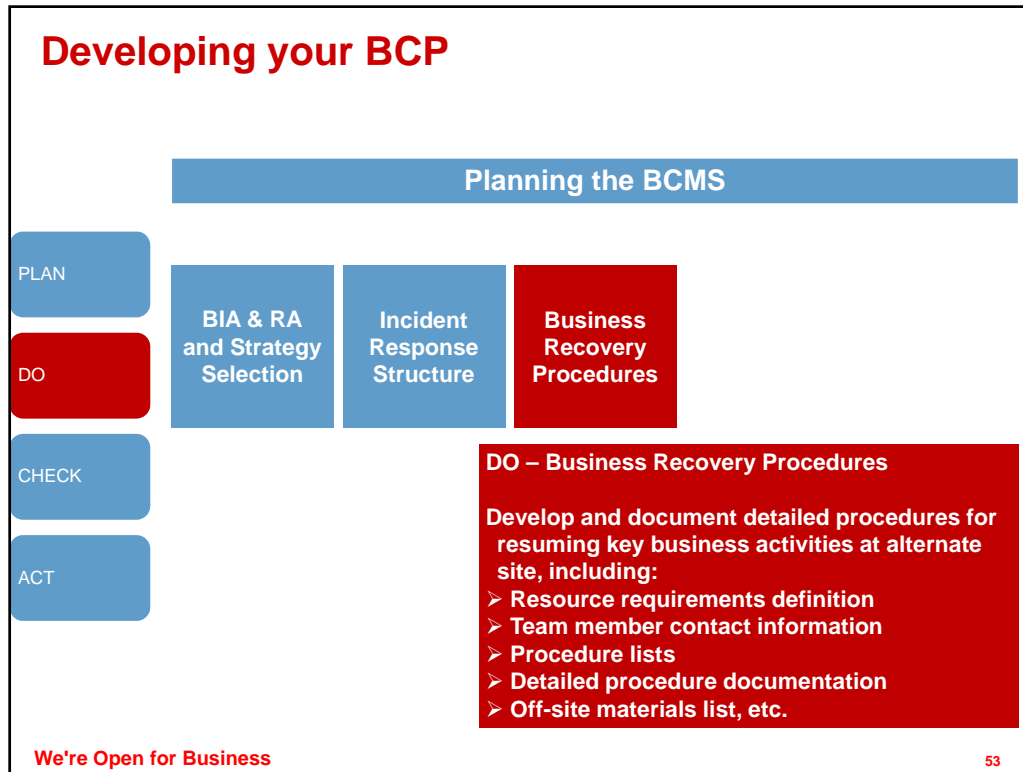
1. Stop all other activities (phone calls, meetings, etc.)
2. Remain calm and follow directions from appropriate staff.
3. Do not return to your workspace for personal possessions; evacuate from where you are.
4. Walk, do not run, to nearest safe exit. use stairwell, not elevators.
5. Direct all visitors to the nearest safe stairwell.
6. Know the alternate evacuation routes.
7. Check door handles for heat: if a door is hot, use an alternate route.
8. Close all doors behind you and proceed to the assembly point.
9. Remain at the assembly point and do not re-enter the building until instructed by emergency personnel.

Emergency Response

Draw a map showing your building, the surrounding streets, building Exit Points and the Assembly Points.

Assembly Point:

Backup Assembly Point:



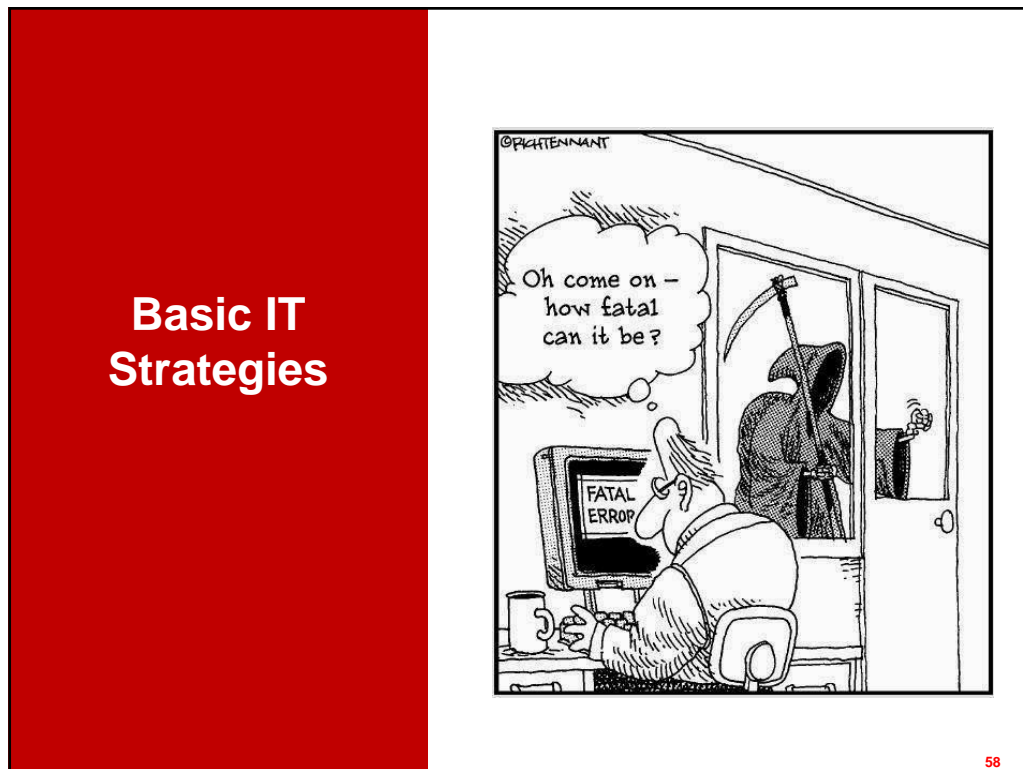
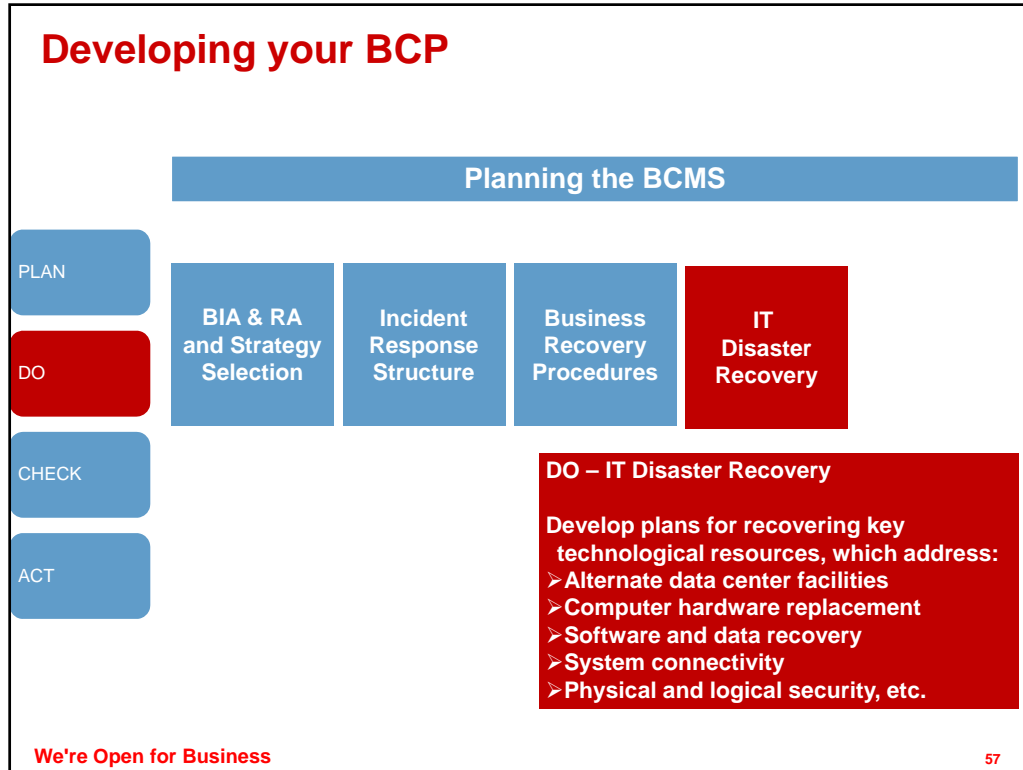
Business Recovery Plan

The Business Recovery Plan is the detailed part of the BCP and covers specific temporary activities to allow the business to remain viable to its clients.

- It requires a detailed, documented series of **BRP procedures/checklists** that may need to be performed by designated BCMS Teams
- It also includes **detailed instructions** how the organization will resume its key business activities within a predetermined timeframe

Business Recovery Plan

Recovery Options	Strategy	Key Business Activities to Resume	Key Resources	External Contacts
Option 1: Resume at the damaged/affected site				
	(e.g.) Restore damaged buildings and equipment and resume KBA			
Option 2: Resume at an alternate site				
	(e.g.) Start up an alternate factory/office/shop			
	(e.g.) Activate back-up IT centre			
Option 3: Resume using alternate methods				
	(e.g.) Start up using older methods, using spare (old) equipment			
Option 4:				



Basic IT Strategies

- Nearly 70% of data loss is the result of human error; 60% of companies that lose their data shut down within 6 months of the loss
- 140,000 hard drives crash in the U.S. weekly
- Start by making an **inventory** of your computer hardware and software
- Then, develop a **schedule** for performing Virus Scans, Regular Maintenance, and Backups on a regular basis

Basic IT Strategies

Regular Computer Maintenance

- Computers do not like heat and vibration - keep computers in a dry, clean area with little traffic
- Attach a UPS (uninterrupted power supply) to desktop computers

Run Scandisk, Defrag and Anti-virus software

- Run Scandisk every 2 to 3 weeks
- Defrag! Data recovery success is more likely when damaged files are clustered
- Update your anti-virus program regularly - enable auto update features

Basic IT Strategies

- **Complete a data restore**
 - **Run a restore to return backed-up files to their original locations. Do this on a regular basis to ensure the system is actually working.**
- **Maintain offsite copies of your backups**
 - **In the case that your office files are destroyed by fire, lightning damage, flooding or theft, make sure you have multiple copies of your files elsewhere.**
- **Keep virus protection and Firewall on and up-to-date**
 - **Without the right protection, viruses can be put back onto your computer after backup and your files can be deleted through an unprotected port.**

Basic IT Strategies

Your Key Technology (Hardware/Software) Inventory

KEY TECHNOLOGY (Hardware/Software)	Serial # or Password	Product/Licence Key	Installation Disk Location

Thank You

- On behalf of our Workshop Sponsors, I wish to thank you for participating in this workshop and we trust that the information we have presented to you will be put to good use.
- Feel free to address any follow-up questions to:



Michael Bittle, MA, CCM, BCRP
Managing Director
Institute for Business Continuity Training
1623 Military Road, # 377
Niagara Falls, NY 14304-1745

Tel: 844-408-4358
Fax: 716-313-1750
Email: mebittle@ibct.com
Web: www.IBCT.com