

# HUB

Risk & Insurance | Employee Benefits | Retirement & Private Wealth

## Risk Management for Post-Secondary Student Associations: What Has Changed?

June 1, 2022

AMICCUS-C

Antigonish, NS

© 2022 HUB International Limited.





# Isaac Monson, CPP

---

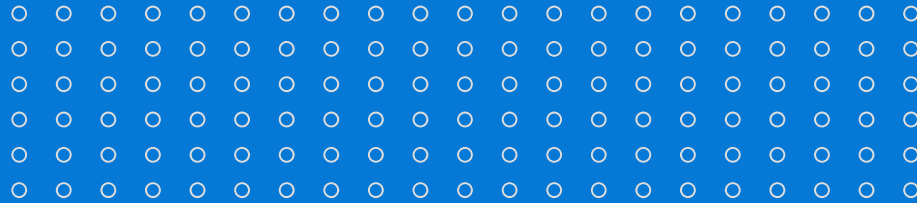
AVP | Sr. Risk Consultant

# Agenda

- 1** | Overview - Organizational Readiness & Resilience
- 2** | Business Continuity Management
- 3** | Q&A



# 1



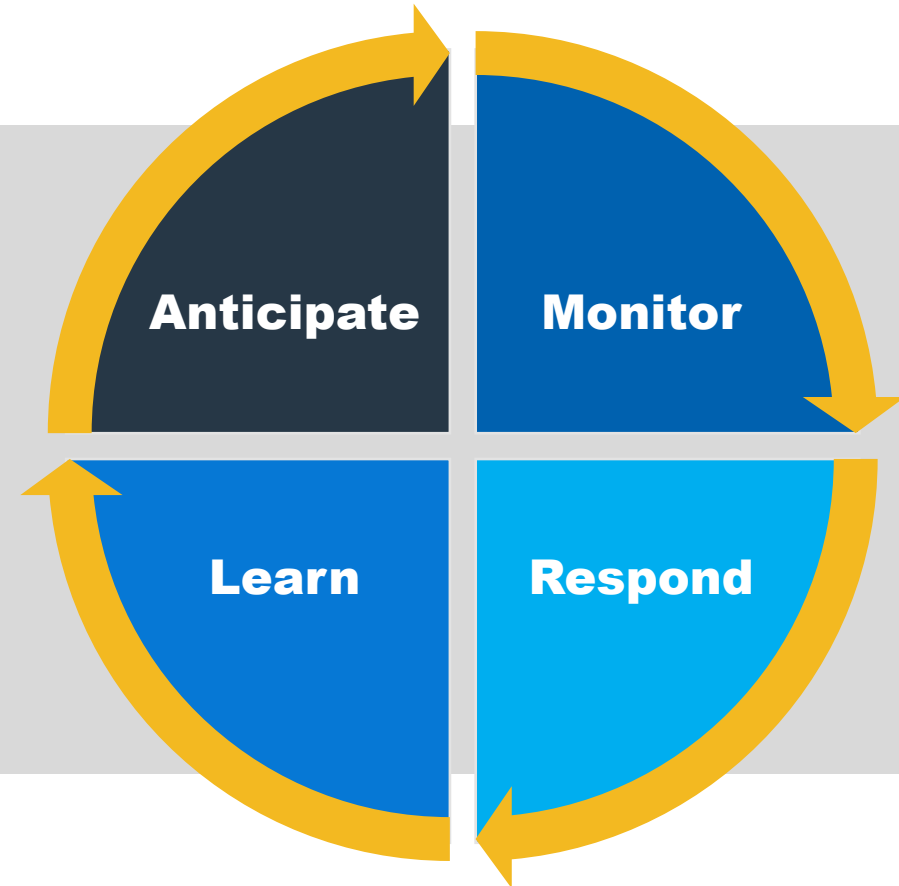
## Overview - Readiness & Resilience

---



# What is Organizational Resilience?

**“the ability of an organization to anticipate, prepare for, respond, and adapt to incremental change and sudden disruptions in order to survive and prosper”\***

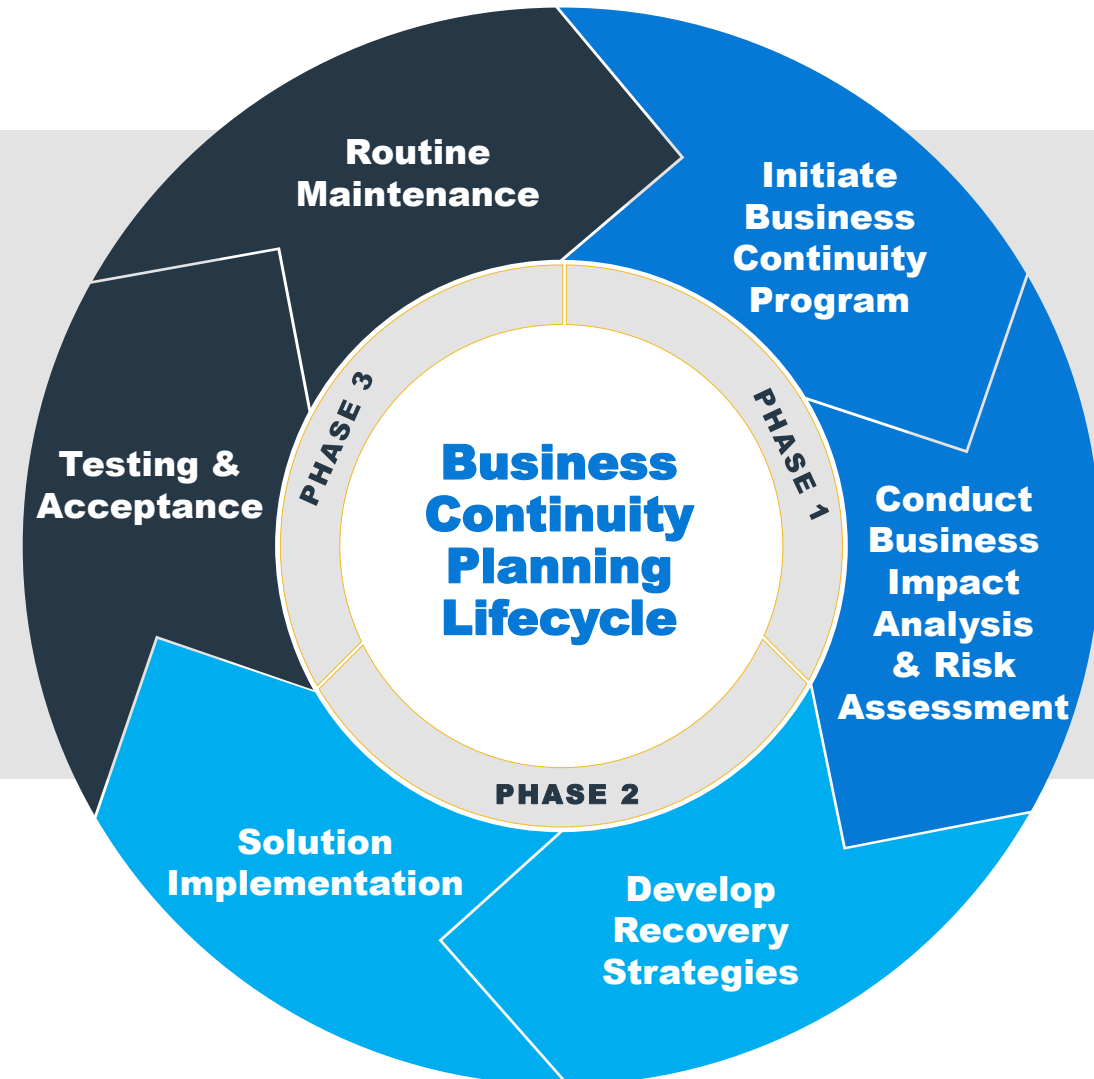


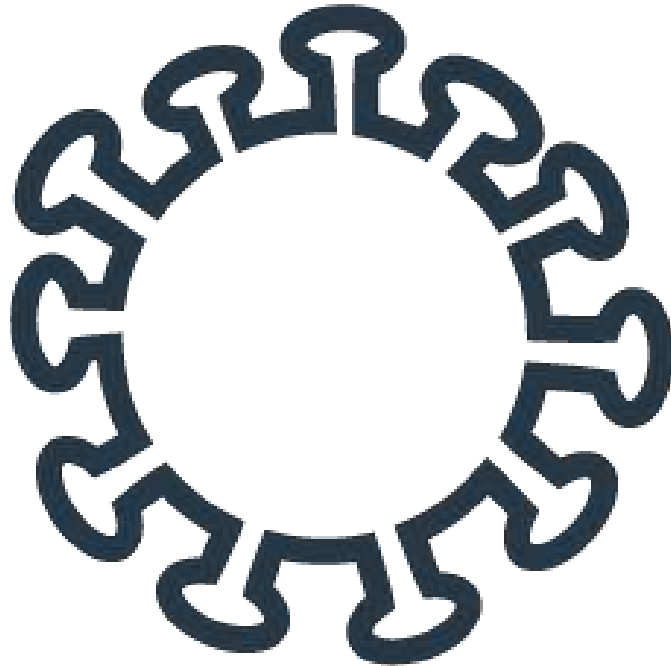
*\*BS 65000:2014 Guidance on Organizational Resilience (British Standard)*

# Business Continuity Management: What is it?

## ISO 22301 BCP Lifecycle

- A process intended to ensure **critical business activities are performed no matter what else is happening.**





## Protecting People

- Terminations, layoffs, workplace conflict, civil-unrest, protest, etc.
- Travel risk, staff/student mental health & wellness

## Protecting Property

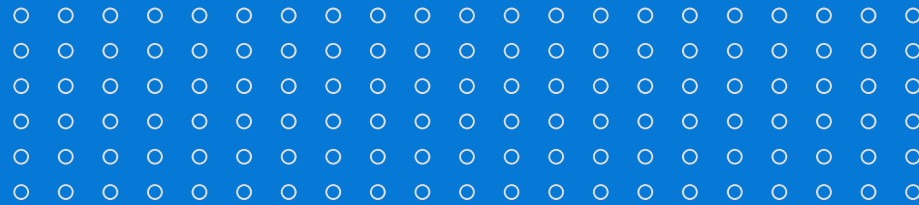
- Closing of physical locations, limited staff presence at sites – More vulnerable
- Increased exposure for internal & external criminal activity (*theft, shrink, embezzlement, vandalism, etc.*)

## Protecting Operations

- Managing compounding disruptive events – Examples:

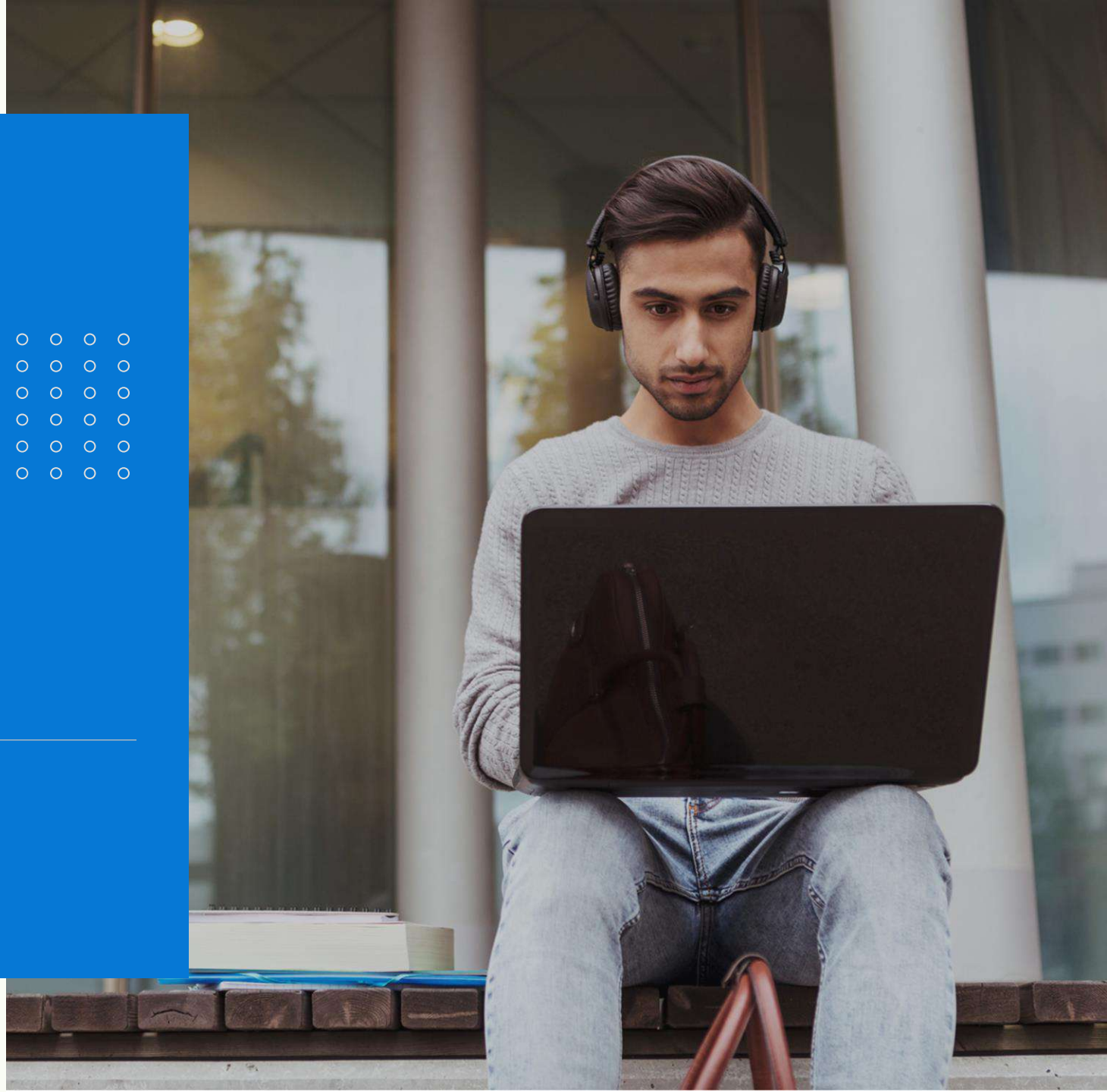
**Natural Disasters x Covid-19 x Civil Unrest x Supply Chain Disruptions**

# 2



## Business Continuity Management

---





VANCOUVER ISLAND

## UVic bus in fatal crash rolled after it moved for Jeep on logging road: RCMP

Terri Theodore  
The Canadian Press

Published Tuesday, December 17, 2019 4:35PM PST  
Last Updated Tuesday, December 17, 2019 5:44PM PST



A police crash reconstruction says a bus loaded with University of Victoria students moved over for an oncoming vehicle as a logging road narrowed before the rollover that killed two students. A tow-truck crew removes a bus from an embankment next to a logging road near Bamfield, B.C., Saturday, Sept. 14, 2019. (THE CANADIAN PRESS/Chad Hipolito)

SHARE: [Tweet](#) [Reddit](#) [Share](#)

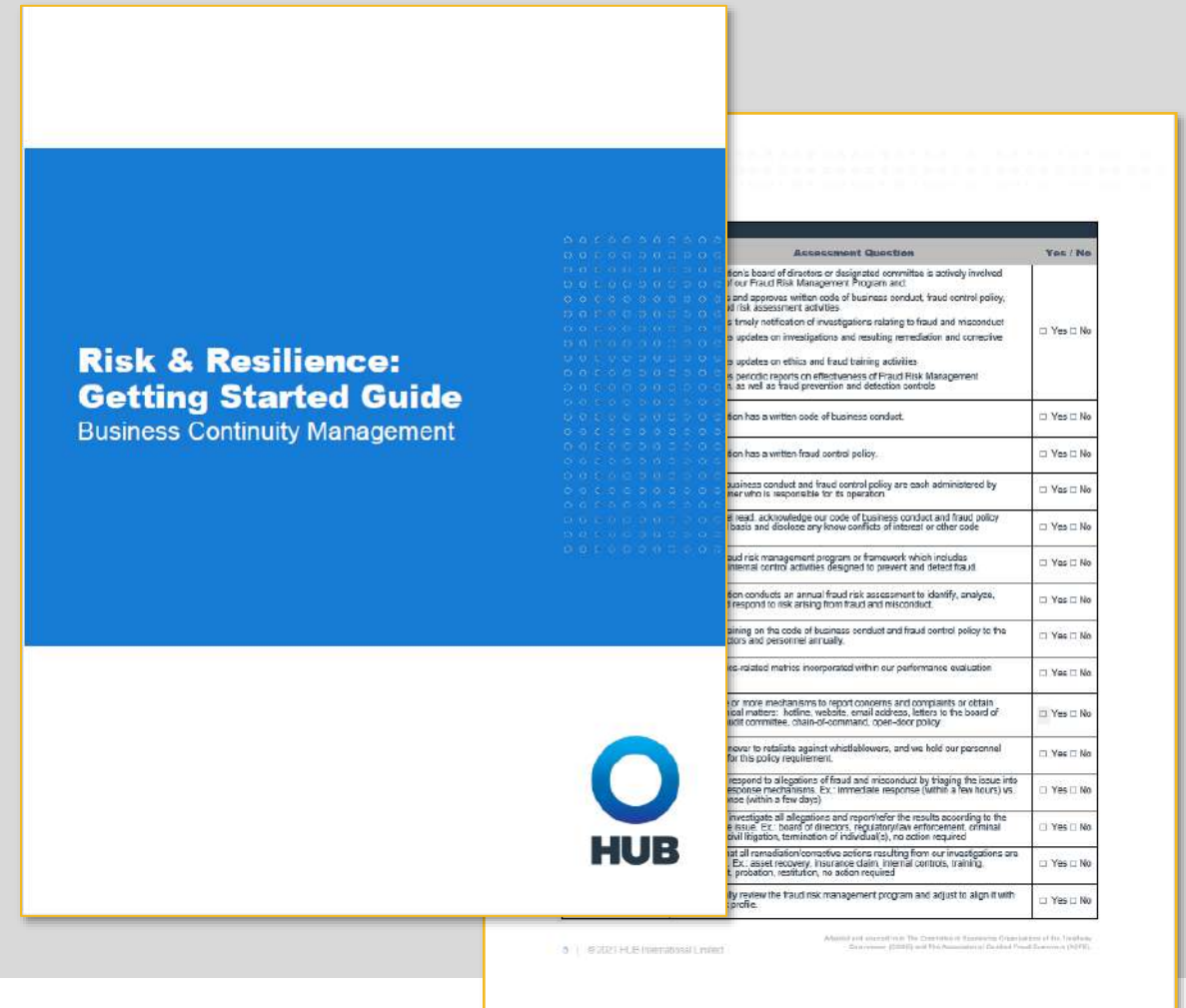
TORONTO | News

## Two golf students from Ontario critically injured in Texas crash that killed nine people



## Getting Started Guides Cover:

- **Assembling & Orienting Project Teams**
- **Assessing your Current State - Self-Assessment Tools & Checklists**
- **Links to Industry Resources, Standards & Guidelines**



**Risk & Resilience: Getting Started Guide**  
Business Continuity Management

Assessment Question	Yes / No
Company's board of directors or designated committee is actively involved in Fraud Risk Management Program and approves written code of business conduct, fraud control policy, and risk assessment activities.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company provides timely notification of investigators relating to fraud and misconduct to relevant departments and updates on investigations and resulting remediation and corrective actions.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company updates on ethics and fraud training activities and provides periodic reports on effectiveness of Fraud Risk Management Program as well as fraud prevention and detection controls.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company has a written code of business conduct.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company has a written fraud control policy.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company's business conduct and fraud control policy are both administered by the same person who is responsible for its operation.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company's leadership acknowledges our code of business conduct and fraud policy basis and discloses any known conflicts of interest or other code of conduct issues.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company has a fraud risk management program or framework which includes internal control activities designed to prevent and detect fraud.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company conducts an annual fraud risk assessment to identify, analyze, and respond to risk arising from fraud and misconduct.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company communicates the code of business conduct and fraud control policy to the board and personnel annually.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company's fraud-related metrics incorporated within our performance evaluation.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company has a process or more mechanisms to report concerns and complaints or obtain confidential matters: hotline, website, email address, letters to the board of directors, committee, chain-of-command, open-door policy.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company has a process to retaliate against whistleblowers, and we hold our personnel accountable for this policy requirement.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company responds to allegations of fraud and misconduct by taking the issue into business seriousness, i.e. immediate response (within a few hours) versus delayed (within a few days).	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company investigates all allegations and reports the results according to the results: i.e. board of directors, regulatory/enforcement, criminal investigation, termination of individual(s), no action required.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company takes all remediation/corrective actions resulting from our investigations are: i.e. asset recovery, insurance claim, internal controls, training, A, probation, restitution, no action required.	<input type="checkbox"/> Yes <input type="checkbox"/> No
Company periodically reviews the fraud risk management program and adjust to align it with the business profile.	<input type="checkbox"/> Yes <input type="checkbox"/> No

© 2022 HUB International Limited

# Business Continuity Management: What is it?



## BCM Integrates the disciplines of:



*Source: DRI International*

# Response & Recovery Plans Differentiated



## Emergency Response Plans

### IT Disaster Recovery Plans

#### Minutes to Hours

- Initial control of emergency situations
- Safeguarding human life
- Stabilizing, securing, preventing further harm to property
- Assessing damage

## Crisis Management Plans

### Cyber Incident Response Plans

#### Hours to Days

- Strategic pre-existing plans for a Crisis Management Team (CMT)
- Crisis communications – internal & external
- Outward facing liaison - stakeholders, media, etc.
- Co-ordination of service recovery efforts

## Business Continuity Plans

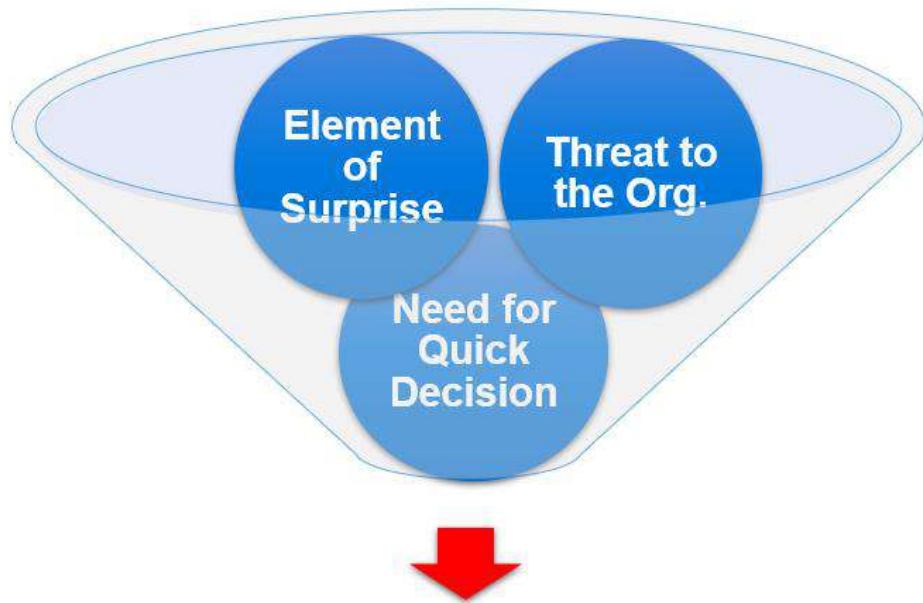
### IT Operations Recovery Plans

#### Days to Weeks

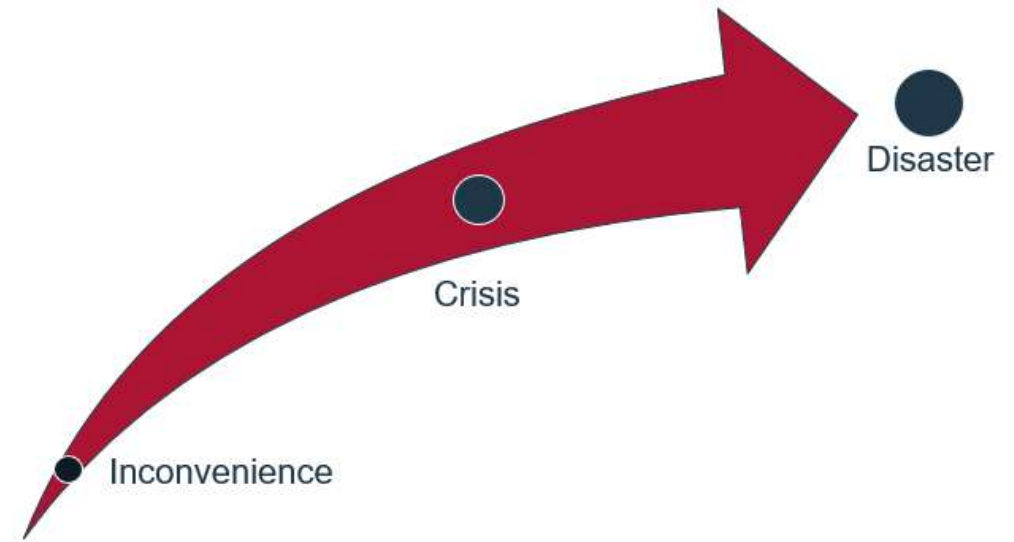
- Recovery of technology services
- Returning IT to “business as normal”
- Phased recovery of business-critical processes



# Elements of a Crisis / Critical Incident & Our Response



Critical Incident & Crisis



Prudent Over-Reaction & Rapid De-Escalation

# Comprehensive All-Hazards Planning

## **Identify the risks.**

Understand hazards, vulnerability, and the worst-case scenarios

## **Develop comprehensive and risk-appropriate plans.**

An all-hazards approach to planning is most efficient

**Emergency  
Response**

**Crisis  
Management**

**IT Operations  
Recovery**

**Business  
Continuity**

# All-Hazards Planning Considerations



Natural Hazards	Human Hazards	Technology Hazards
<p><u>Geological Hazards</u> Earthquakes, Landslides, Subsidence, or Sinkholes</p> <p><u>Meteorological Hazards</u> Flood, Flash Flood, Tidal Surge, Severe Drought, Snow, Ice, Hail, Tornado, etc.</p> <p><u>Biological Hazards</u> Pandemic, Infectious / Communicable Disease, Blood-Borne Pathogens, etc.</p>	<p><u>Unintentional</u> Hazardous Material Spill or Release, Explosion/Fire, Transportation Incidents, Building or Structure Collapse, etc.</p> <p><u>Intentional</u> Terrorism, Robbery, Workplace Violence, Kidnap, Extortion, Hostage Incident, Demonstrations, Civil Disturbance, Riots, etc.</p>	<p><u>Infrastructure</u> Utility interruption or failures Telecomm, Electrical Power, Water, Gas, HVAC, Sewage Systems, Other Critical Infrastructure, etc.</p>

# Prioritizing Hazards & Readiness Planning



		\$5M	\$1M	\$750K	\$500K	\$100K
<b>SEVERITY</b>		<b>Catastrophic</b>	<b>Major</b>	<b>Serious</b>	<b>Minor</b>	<b>Insignificant</b>
<b>1 y e a r</b>	<b>Almost Certain</b>	<b>Intolerable</b>	<b>Intolerable</b>	<b>Intolerable</b>	<b>High</b>	<b>Medium</b>
	<b>Frequent</b>	<b>Intolerable</b>	<b>Intolerable</b>	<b>High</b>	<b>Medium</b>	<b>Medium</b>
	<b>Occasional</b>	<b>Intolerable</b>	<b>High</b>	<b>Medium</b>	<b>Medium</b>	<b>Acceptable</b>
	<b>Unlikely</b>	<b>High</b>	<b>Medium</b>	<b>Medium</b>	<b>Acceptable</b>	<b>Acceptable</b>
	<b>Extremely Unlikely</b>	<b>Medium</b>	<b>Medium</b>	<b>Acceptable</b>	<b>Acceptable</b>	<b>Acceptable</b>



# Comprehensive All-Hazards Planning



**Emergency  
Response**

**Crisis  
Management**

**IT Operations  
Recovery**

**Business  
Continuity**

---

**Communicate and implement the plan across the organization.**

Roles, responsibilities, and alternates should be assigned and trained

---

**Test, evaluate, and continuously improve your plans.**

During a crisis is not the time to discover a plan's shortcomings

---

# Response Planning by Disruption Scenario



**Loss of a Facility**



**Loss of Staff**



**Loss of a Vendor or Supplier**



**Loss of Technology**


# Emergency Action Planning

## Emergency Response

### Minutes to Hours

- Initial control of emergency situations
- Protecting human life
- Stabilizing, securing, preventing further harm to property
- Assessing scope and scale of damage

Your Company Name Here – Facility Emergency Action Plan Version 1.0/Date



**YOUR LOGO**  
Emergency Action Plan  
Address Here

Date: \_\_\_\_\_

by any means or in any form, in  
and employees authorized

Date
_____
_____
_____
_____

Hardcopy Distributed

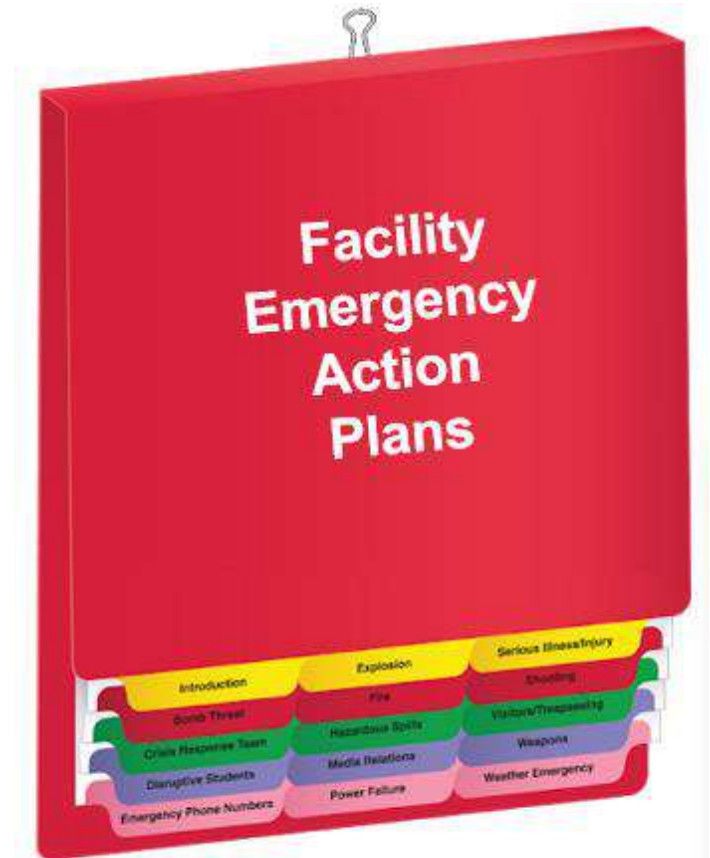
_____
_____
_____

Site Emergency Coordinator: \_\_\_\_\_  
Title: \_\_\_\_\_  
Phone: \_\_\_\_\_  
Email: \_\_\_\_\_

1 | CONFIDENTIAL

2 | CONFIDENTIAL

In conditions and practices observed by  
such conditions and practices, which may  
state on that the client or any such  
person, standards or recommendations. All  
include the sole responsibility of, and  
events of future results not an assurance  
of from both open and closed sources.



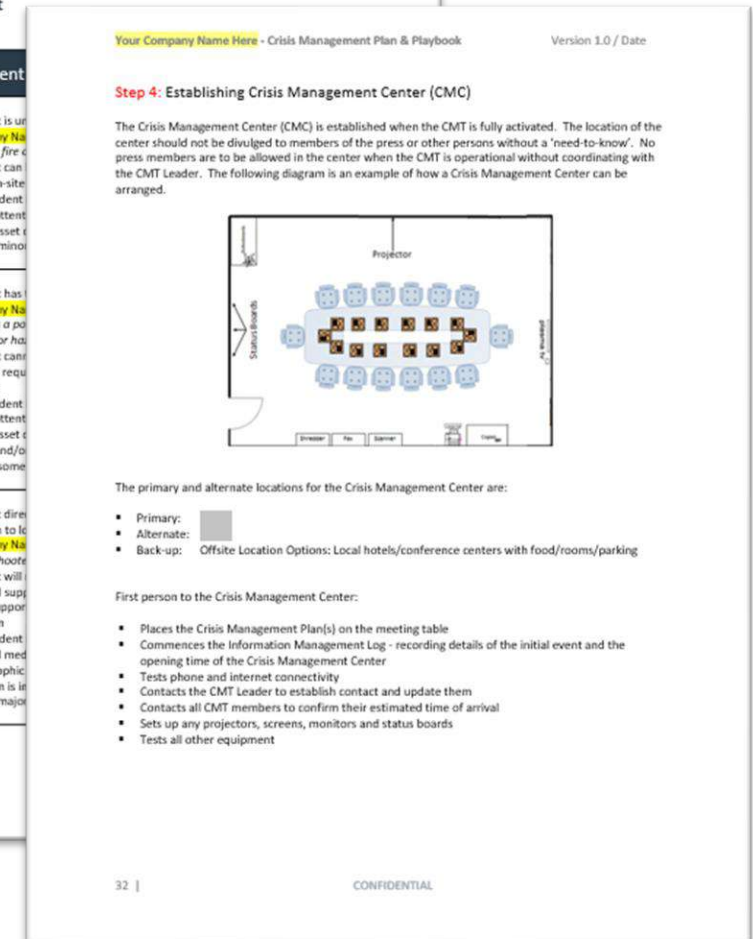
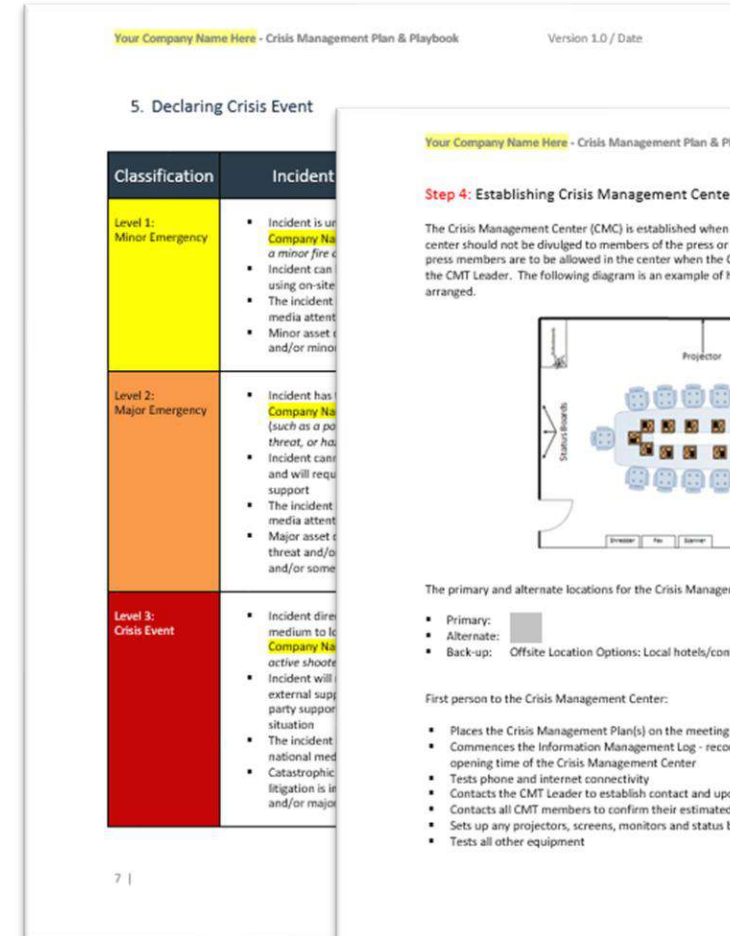
# Crisis Management Planning



## Crisis Management

### Hours to Days

- Strategic pre-existing plans for a Crisis Management Team
- Crisis communications for internal & external
- Outward facing liaison - stakeholders, media, etc.
- Co-ordination of service recovery efforts



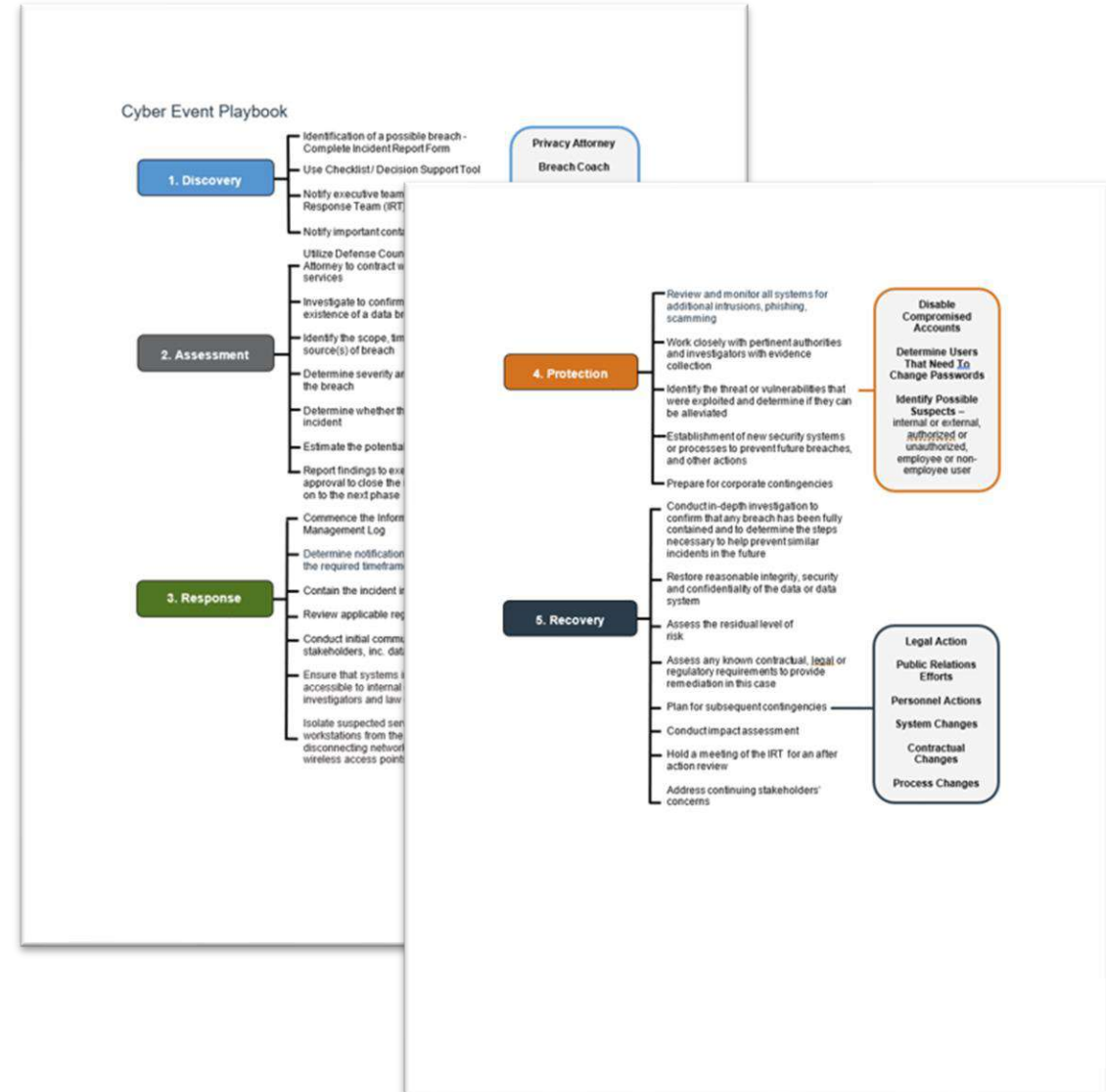


# Information Technology Recovery Planning

## IT Operations Recovery

### Days to Weeks

- Phased recovery of technology services
- Returning IT to “business as normal”
- IT Disaster Recovery
- Incident Response Plans
- IT Operations Recovery



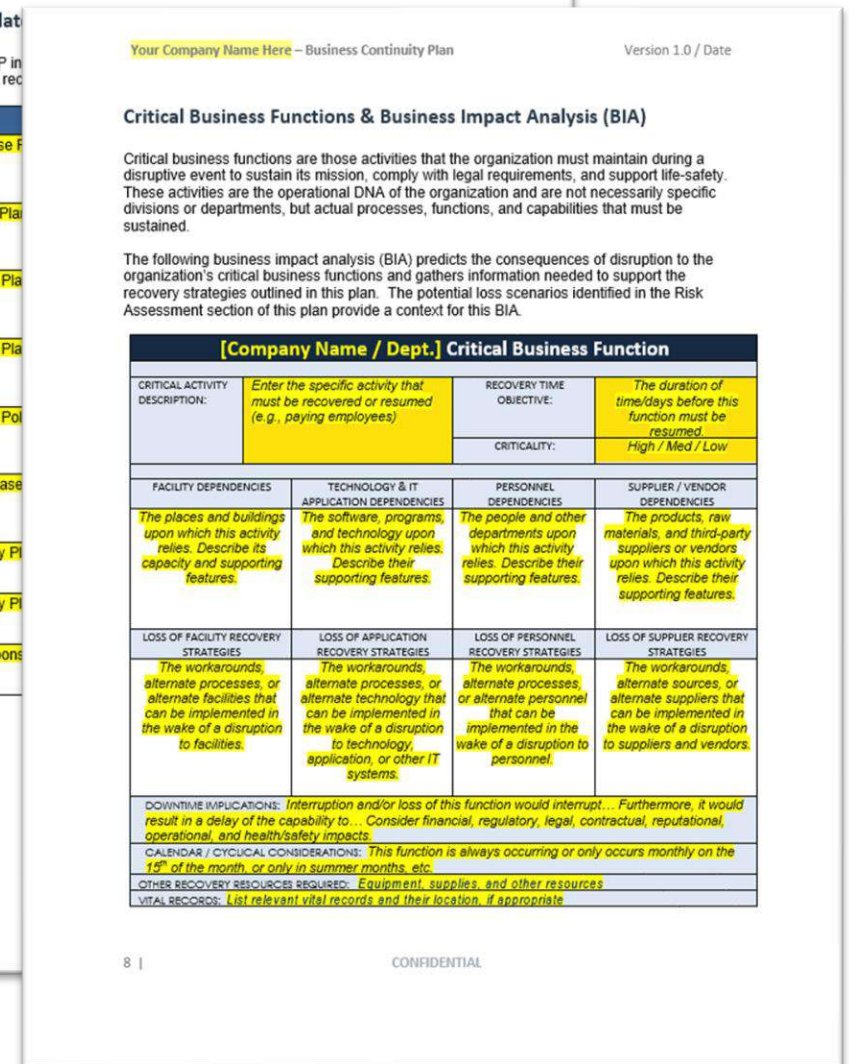
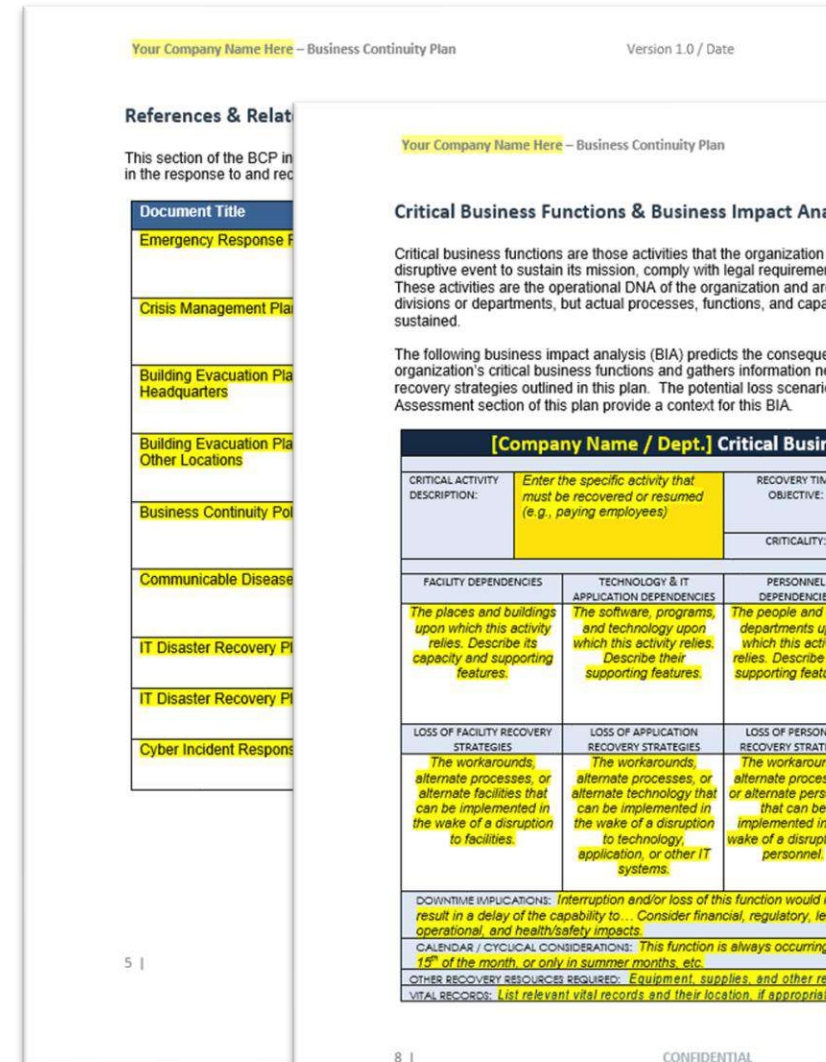
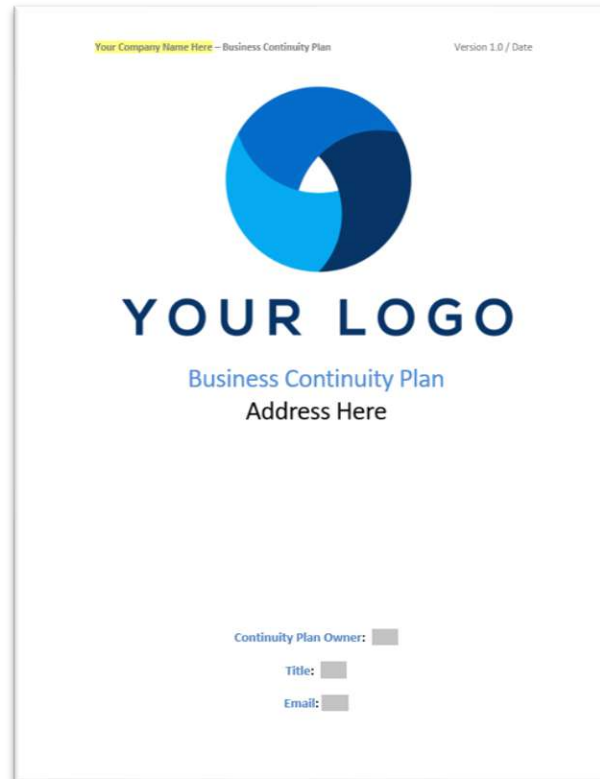
# Business Continuity Planning



## Business Continuity

### Days to Weeks

- Restoring business critical processes
- Continuing to deliver on critical activities amidst the disruption
- Phased recovery to “business as normal”



# Business Impact Analysis (BIA)

## BIA identifies, categorizes, and prioritizes:

- Critical functions / processes & vital records
- Required resources, personnel, & equipment

Maximum Tolerable Outage	<b>(MTO)</b>
Recovery Time Objectives	<b>(RTO)</b>
Recovery Point Objectives	<b>(RPO)</b>

Criticality		Application		Facility	
Business Impact	Tier	RTO	RPO	RTO	RPO
<b>Mission Critical</b>	1	< 4 Hours	< 1 Hour	< 4 Hours	< 1 Hour
<b>Business Critical</b>	2	< 24 Hours	< 1 Hour	< 48 Hours	< 24 Hours
<b>Significant</b>	3	< 72 Hours	< 24 Hours	< 7 Days	< 24 Hours
<b>Important</b>	4	< 7 Days	< 48 Hours	< 30 Days	< 48 Hours
<b>No Impact</b>	Best Effort	> 30 Days	< 48 Hours	> 90 Days	< 48 Hours

# Business Impact Analysis (BIA) Worksheet



## ▸ Data Gathering Worksheet - Business Impact Analysis (BIA) with Risk Assessment

### Background



Department Name	
Department Owner (Director/Manager)	
Products and Services Directly or Indirectly Delivered by This Department	<input type="checkbox"/> P&S #1 <input type="checkbox"/> P&S #2 <input type="checkbox"/> P&S #3 <input type="checkbox"/> P&S #4 <input type="checkbox"/> P&S #5

### Department Overview

The following table captures key department characteristics that may influence the assignment of recovery objectives and the selection of recovery strategies.

Department Narrative Description	
Customers and Outputs (Internal or External)	•
Peak Operating Periods or Seasonality	•

# Example BIA Output



## Human Resources

**Owners** Ryan Hutton  
**Contributors** Tobias  
**Last Updated** September 18, 2016 02:30PM

**DESCRIPTION**  
 This department is responsible for the attraction, selection, training, assessment, and benefits administration of employees, while also overseeing organizational leadership and culture, and ensuring compliance with employment and labor laws.

**PEAK OPERATING PERIODS OR SEASONALITY**  
 None noted.

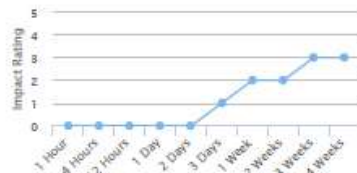
## Activities

### Administer Payroll

**DESCRIPTION**  
 This activity includes maintaining and updating employee records to enable payroll execution. Following a request to modify employee payroll records (e.g. raise, withholding, garnishment, new employee hire, time adjustment, etc), Human Resources makes the appropriate system changes. Human Resources enters the adjustments into the ADP system and documents the request in the employee file. A copy of records is kept for auditing purposes.

**FINANCIAL**  
 An inability to administer payroll for a week or more may result in employees not receiving their correct payment amounts which could in turn result in regulatory fines.

**REGULATORY**  
 A failure to perform employee payroll could result in regulatory fines or penalties.



**REQUESTED RTO**  
 4 Days

**RELATED PRODUCT/SERVICE**  
 Provide Employee Support

**PROVEN RTO**  
 8 Days

**COMMITTED RTO**  
 4 Days

**REPUTATIONAL**  
 An inability to administer payroll for a week or more could affect the ability to execute an accurate payroll, leaving employees unable or unwilling to report to work.

**OPERATIONAL**  
 An inability to administer payroll for a week or more may prevent or impact the accuracy of employee payroll, leaving employees unable or unwilling to report to work.



## Triggers and Escalation Criteria

Following the onset of a disruptive incident, the Recovery Team Leader will perform an initial assessment to determine if the incident has or will impact this department, its activities or resources. If resources or activities are affected, the Recovery Team Leader will activate this plan. This plan will also be activated based on directives from the Crisis Management Team

Following activation, staff will work to continue performing the most [important activities](#), but also prepare for instruction and guidance from the Department Recovery Team. Additionally, the department should prepare to communicate its status to the Crisis Management Team.

## Recovery Strategies

This recovery plan outlines procedures designed to enable effective and efficient response and recovery based on each of the following four scenarios:

### Scenario 1 – Loss of Facility

If a facility is damaged, inaccessible, or unavailable for use for any reason, loss of facility strategies outline the procedures required to support the recovery of in-scope activities, based on approved recovery requirements.

### Scenario 2 – Loss of Staff

If absenteeism occurs, which may result from no-notice (immediate) loss or a large-scale public health event such as a pandemic, loss of staff strategies describe the tasks necessary to support the staffing of the most essential activities throughout the course of the incident.

### Scenario 3 – Loss of Technology

If there is a pervasive interruption to the information technology environment, loss of technology strategies describe response activities to expedite technology restoration and sustain the business during downtime.

### Scenario 4 – Loss of Vendor/Supplier

If there is a disruptive incident affecting one or more vendors' ability to support the delivery of in-scope products or services, loss of vendor/supplier strategies describe the response activities needed to support the continuity of operations.

The recovery procedures documented in this plan are organized into six sections:

1. Initial Department Assessment/Evaluation
2. Recovery Scenario 1 - Loss of Facility
3. Recovery Scenario 2 - Loss of Staff
4. Recovery Scenario 3 - Loss of Technology
5. Recovery Scenario 4 - Loss of Key Vendor/Supplier
6. Ongoing Operations (until the disruptive incident ends)

Consult only the recovery procedures necessary, based on the circumstances of the disruptive incident that resulted in the activation of this recovery plan.





# Questions

# Thank You!

---

## **Jim Henry, C.C.I.B. ONT**

Senior Account Executive  
**HUB International**

[jim.henry@hubinternational.com](mailto:jim.henry@hubinternational.com)

## **Isaac Monson, CPP**

AVP, Senior Risk Consultant  
**HUB International**

[isaac.monson@hubinternational.com](mailto:isaac.monson@hubinternational.com)

