Business Continuity Toolkit

Continuity Plan Development
Methodology & Guide

March 2021

HALIFAX
PARTNERSHIP

Welcome to the Business Continuity Toolkit

- The COVID-19 pandemic has shone a spotlight on how quickly things can change for a business.

- You never really expect the unexpected, so it’s useful to plan ahead for change and crises.

- The Halifax Partnership has developed a Business Continuity Toolkit to help small- and medium-sized business plan for changes and crises, whether it is a pandemic or another type of disruption.

The Why, What and How of the toolkit

Why – The Halifax Partnership has prepared this guide to help small- and medium-sized business facing challenges in a time of crisis.

What – The toolkit is set of guides, templates, webinars and additional resources which will help businesses with planning and building resilience to prepare and respond to crises, whether it's a pandemic or any other critical challenge.

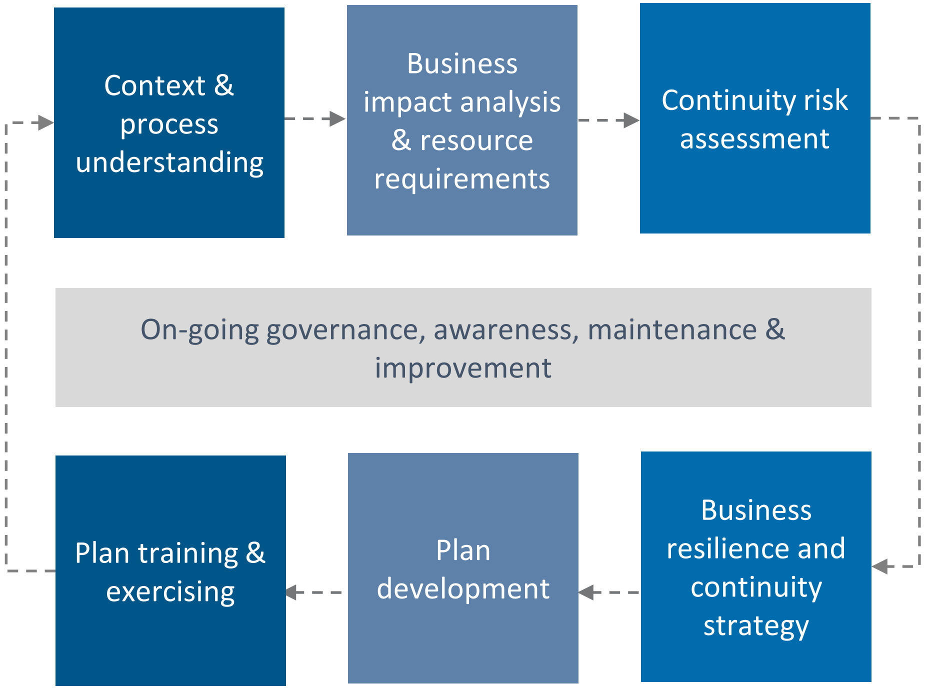
How – The toolkit has been designed for busy people who are juggling many challenges. It can be used to create a resilience plan to prepare for major disruptions and crises.

Business resilience overview

A business resilience program helps you to:

- Understand your business systems, supply chains, human resources and other types of critical resources
- Examine how each is affected by a disruption
- Develop responses to mitigate risks
- Communicate challenges and train teams
- Develop response plans
- Develop resilience and continuity plans and continue to revise and adapt them.

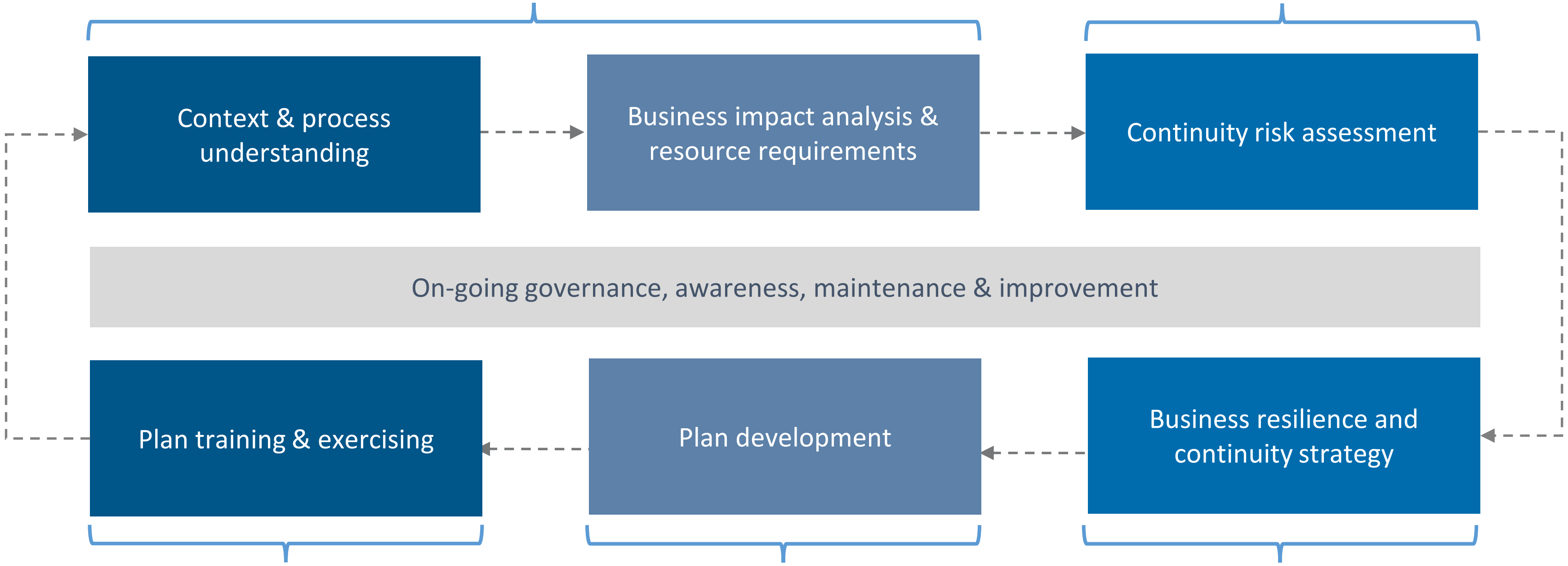
Business Resilience Lifecycle


Context & process understanding
Business impact analysis & resource requirements
Continuity risk assessment
On-going governance, awareness, maintenance & improvement
Business resilience and continuity strategy
Plan development
Plan training & exercising

Toolkit components

1. Impact analysis & resources guide
2. MS Excel workbook

3. Risk assessment guide
4. MS Excel workbook


Context & process understanding
Business impact analysis & resource requirements
Continuity risk assessment
On-going governance, awareness, maintenance & improvement
Plan training & exercising
Plan development
Business resilience and continuity strategy

14. Resources: examples of exercise scenarios and injects

8. Continuity plan development guide

9-12. MS Word plan templates

13. Resources: return-to-work checklist

5. Gap analysis & strategy guide

6. MS Excel workbook

7. Resources: examples of recovery alternatives

Webinar #1 – Business Resilience Basics

Webinar #2 – Business Resilience Lessons from the Pandemic

Webinar #3 – BCM Toolkit Walkthrough

Methodology

Developing Continuity Plans

HALIFAX
PARTNERSHIP

Continuity plan development

This guide will help you to develop the 4 types of continuity plans which are needed for a resilient business:

1. Emergency Response Plan: This type of plan includes documented guidance and procedures to enable emergency and incident response teams to respond to events which require immediate action to protect the business's people, its assets and the environment.

2. Crisis Management Plan: This type of plan includes provides guidance and documented procedures to assist the crisis management team (CMT) which is responsible for coordinating the business response to crises and overseeing business recovery activities.

3. Business Continuity Plan: This plan is an aid to recovering critical business processes following a significant disruption. It contains information on each process and how to recover the resources it depends on.

4. IT Disaster Recovery Plan: This type of plan includes documented procedures to assist the business to recover from an IT disruption, ensuring the effective recovery of key systems.

Emergency response plan

Emergency response plans (ERPs) are built for specific scenarios, for example, building evacuation or response to an ongoing cyber-attack.

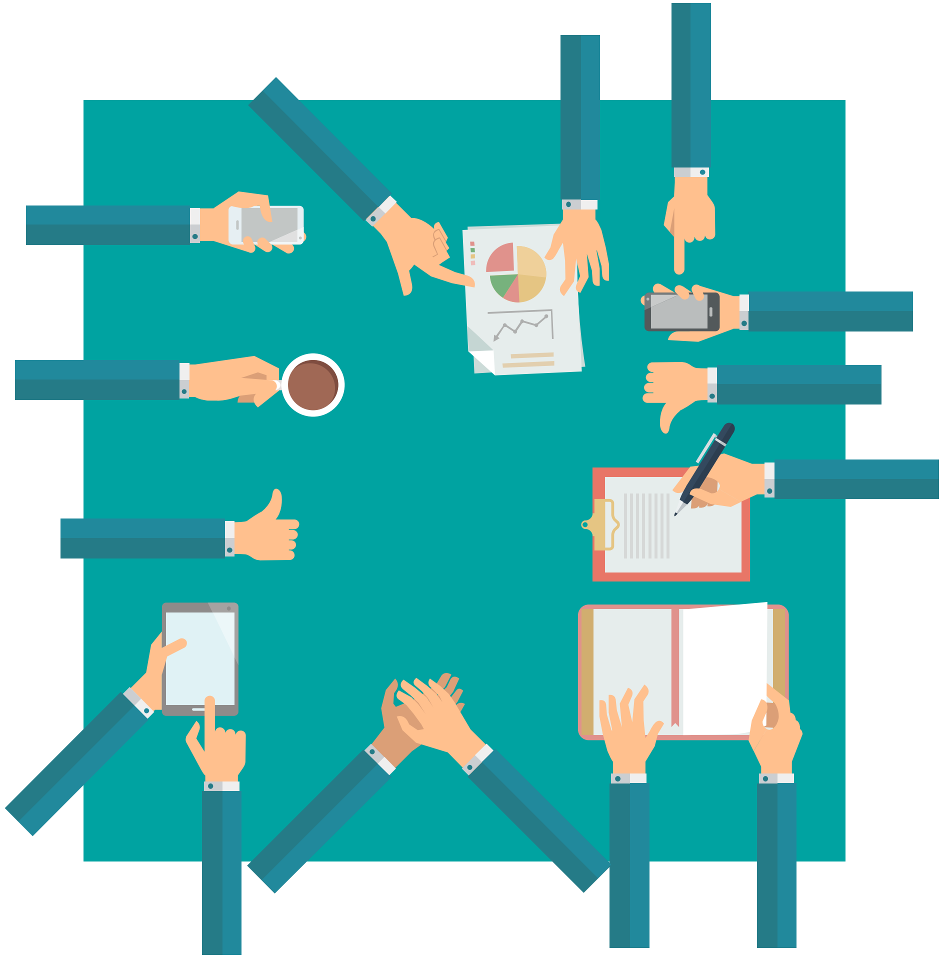
These plans focus on early detection and triage of negative events, which may escalate into an emergency or crisis. It also focuses on the immediate steps required to minimize damage to your business.

They also include warnings and alerts that can be issued during an emergency.

Crisis management plan

The crisis management plan (CMP) brings together a team to respond and recover from crises. It looks at which aspects of the business have been impacted and what has to be done to allow the business to continue.

This plan focuses on engaging the required decision-makers during a crisis, executing a communications strategy, setting up the command centre to monitor the situation, and supporting response and recovery activities throughout the business.



Business continuity plan

Business continuity plans (BCPs) aim to recover critical business processes following a significant disruption.

These plans focus on the steps to recover the resources needed by each critical business process.

BCPs include information on existing resilience measures which are relevant during recovery, detailed recovery procedures and steps to return to normal operations once the disruption is over.

People ✓
Equipment ✓
Facilities ✓
Technology □
Suppliers □
Vital Records □
Inventory □

IT disaster recovery plan

The IT disaster recovery plan (DRP) aims to recover a specific resource type (technology and communications systems) given the complexity associated with technology recovery.

Each technology resource supporting a critical business process has a combination of workarounds and resilience measures to reduce the likelihood/impact of a significant disruption and recovery procedures to restore the technology functionality following a significant disruption.

This plan focuses on the recovery procedures after a disruption occurs.

Next steps

Once the plans are developed, the following next steps should be taken:

1. Obtain sign-off on the plans from the business's management team.

2. Distribute plans to appropriate interested parties and stakeholders responsible for using them.

3. Test your plans through table-top simulations or field exercises to verify their effectiveness, and continually keep those plans updated.

Guide Samples

Continuity plan development

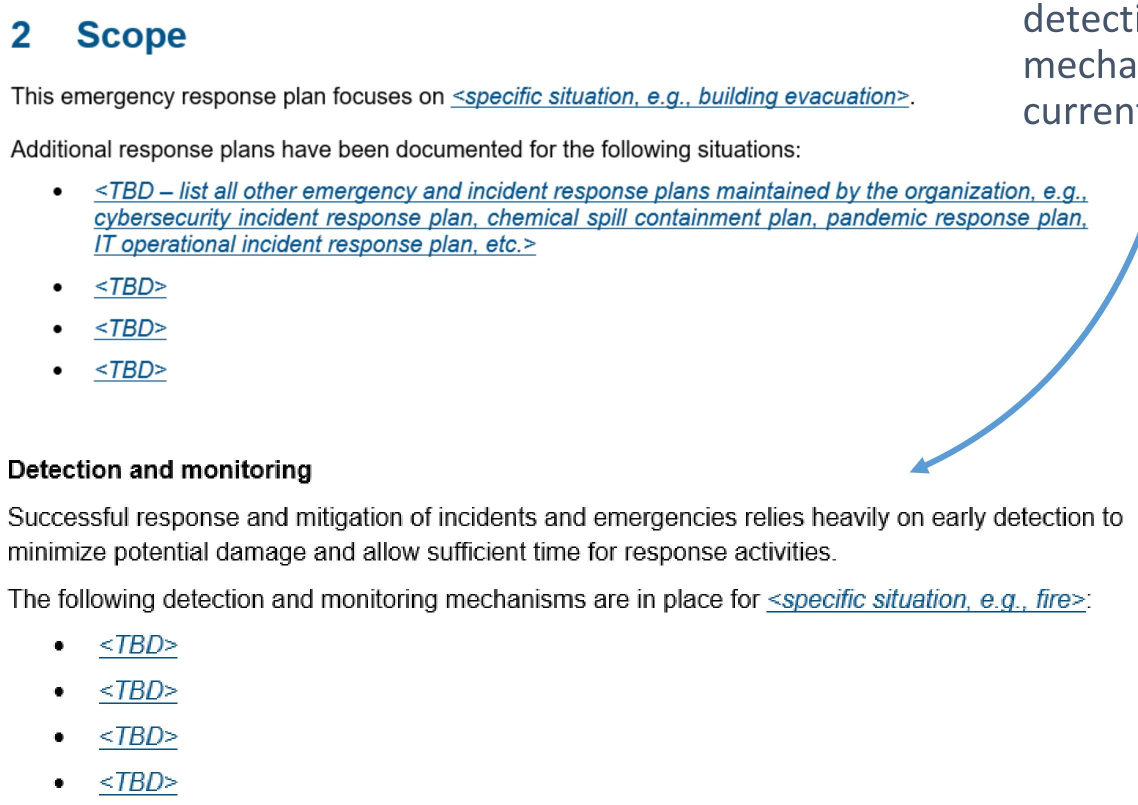
HALIFAX PARTNERSHIP

1. Generic emergency response plan – guide

1. Document the scenario which this plan focuses on and the scenarios which are in other emergency plans

2. Nominate the emergency response team members and identify their alternates

3. Document the detection & monitoring mechanisms you have currently in place



2 Scope

This emergency response plan focuses on <specific situation, e.g., building evacuation>.

Additional response plans have been documented for the following situations:

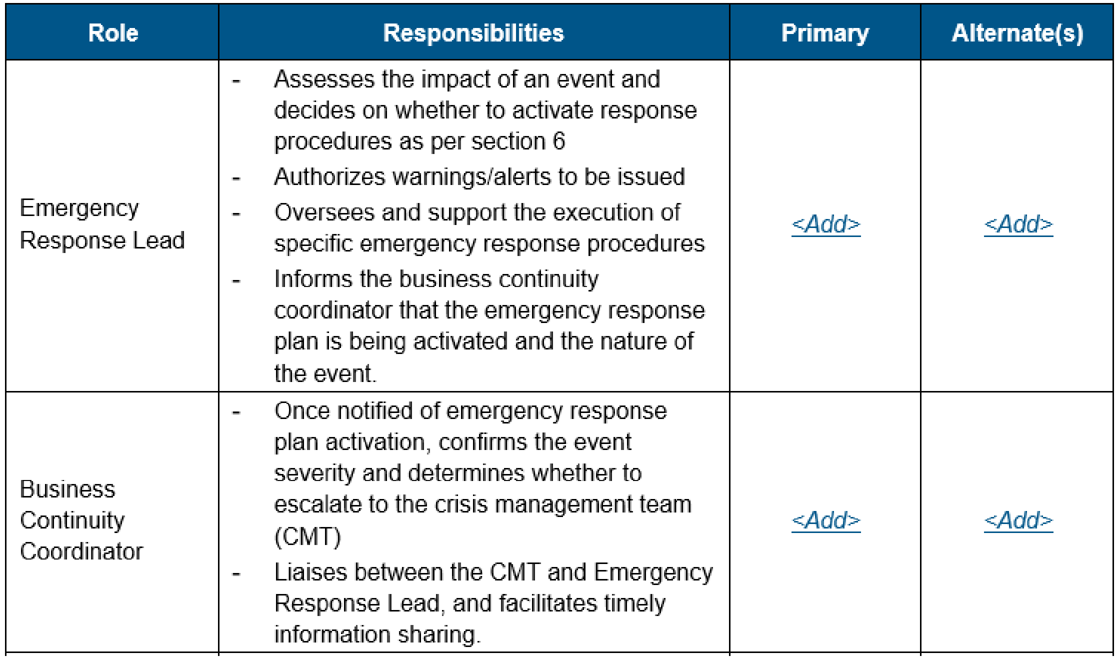
- <TBD – list all other emergency and incident response plans maintained by the organization, e.g., cybersecurity incident response plan, chemical spill containment plan, pandemic response plan, IT operational incident response plan, etc.>
- <TBD>
- <TBD>
- <TBD>

Detection and monitoring

Successful response and mitigation of incidents and emergencies relies heavily on early detection to minimize potential damage and allow sufficient time for response activities.

The following detection and monitoring mechanisms are in place for <specific situation, e.g., fire>:

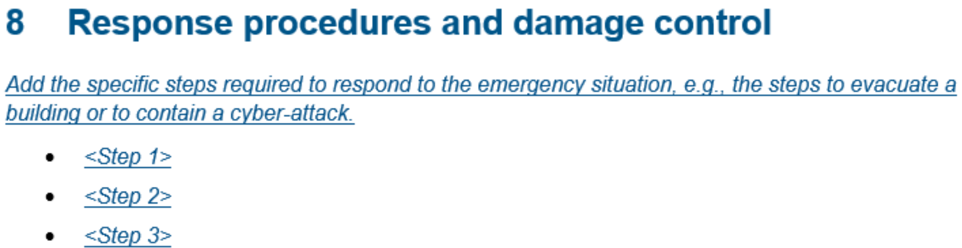
- <TBD>
- <TBD>
- <TBD>
- <TBD>



Role	Responsibilities	Primary	Alternate(s)
Emergency Response Lead	- Assesses the impact of an event and decides on whether to activate response procedures as per section 6 - Authorizes warnings/alerts to be issued - Oversees and support the execution of specific emergency response procedures - Informs the business continuity coordinator that the emergency response plan is being activated and the nature of the event.	<Add>	<Add>
Business Continuity Coordinator	- Once notified of emergency response plan activation, confirms the event severity and determines whether to escalate to the crisis management team (CMT) - Liaises between the CMT and Emergency Response Lead, and facilitates timely information sharing.	<Add>	<Add>

1. Generic emergency response plan – guide

4. Document the specific steps to be taken to respond to this specific emergency scenario

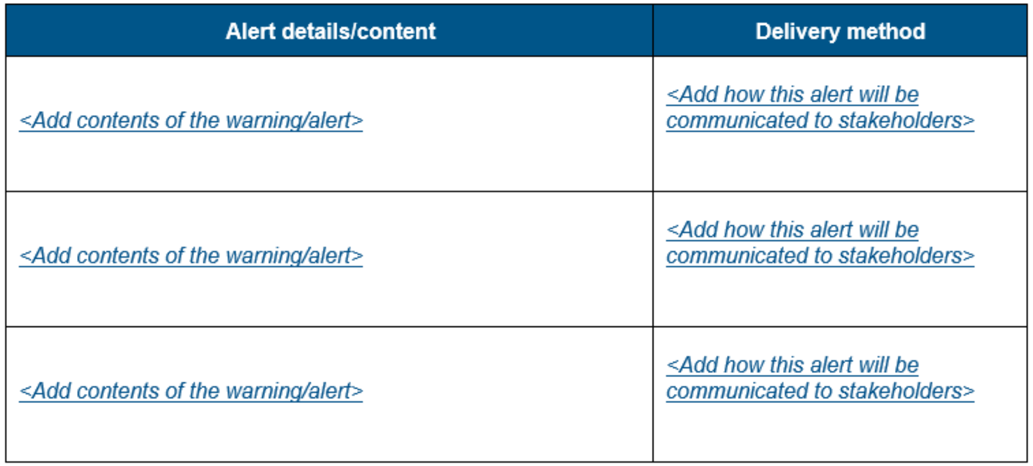


8 Response procedures and damage control

Add the specific steps required to respond to the emergency situation, e.g., the steps to evacuate a building or to contain a cyber-attack.

- <Step 1>
- <Step 2>
- <Step 3>
- <Step 4>
- <Step 5>

5. Determine what alerts and warnings need to be issued to protect people and assets



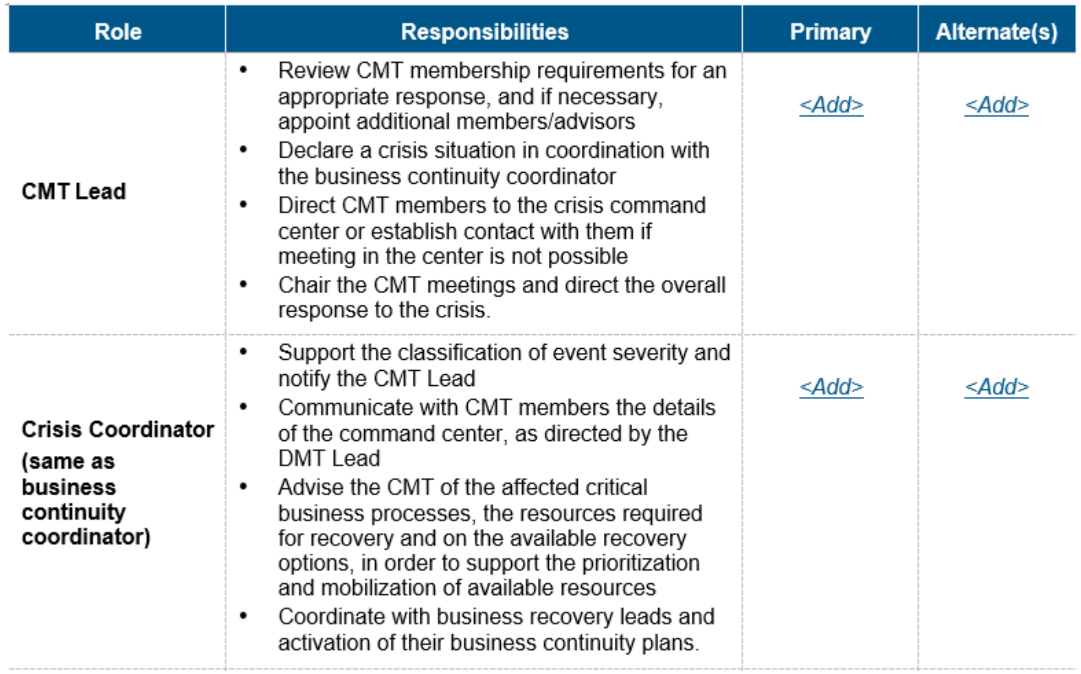
Alert details/content	Delivery method
<Add contents of the warning/alert>	<Add how this alert will be communicated to stakeholders>
<Add contents of the warning/alert>	<Add how this alert will be communicated to stakeholders>
<Add contents of the warning/alert>	<Add how this alert will be communicated to stakeholders>

6. Prepare a list of emergency contact information

Name	Role	Phone number(s)	Email address

2. Crisis management plan – guide

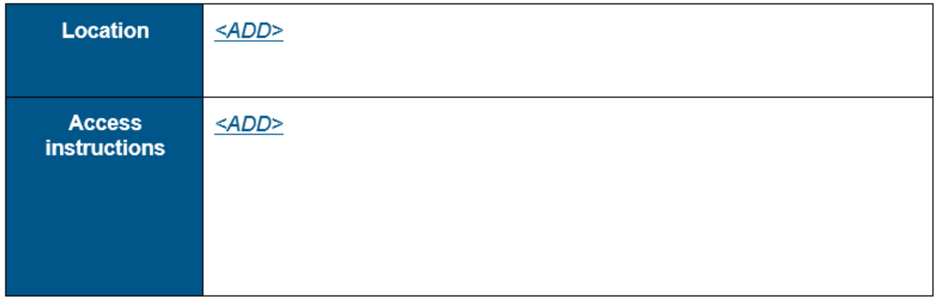
1. Nominate the crisis management team members and identify their alternates



Role	Responsibilities	Primary	Alternate(s)
CMT Lead	• Review CMT membership requirements for an appropriate response, and if necessary, appoint additional members/advisors • Declare a crisis situation in coordination with the business continuity coordinator • Direct CMT members to the crisis command center or establish contact with them if meeting in the center is not possible • Chair the CMT meetings and direct the overall response to the crisis.	*<Add>*	*<Add>*
Crisis Coordinator (same as business continuity coordinator)	• Support the classification of event severity and notify the CMT Lead • Communicate with CMT members the details of the command center, as directed by the DMT Lead • Advise the CMT of the affected critical business processes, the resources required for recovery and on the available recovery options, in order to support the prioritization and mobilization of available resources • Coordinate with business recovery leads and activation of their business continuity plans.	*<Add>*	*<Add>*

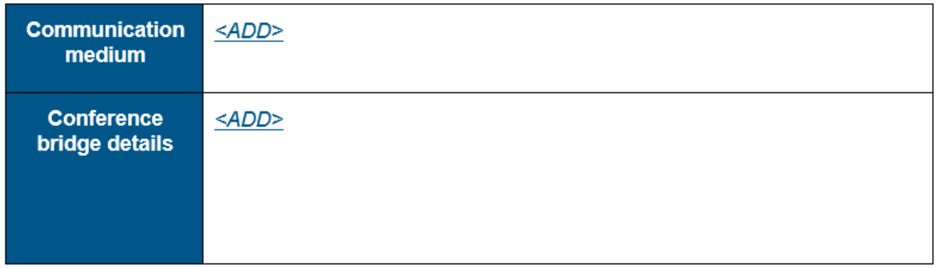
2. Select physical and virtual command center locations and document their details

Physical command center details



Location	*<ADD>*
Access instructions	*<ADD>*

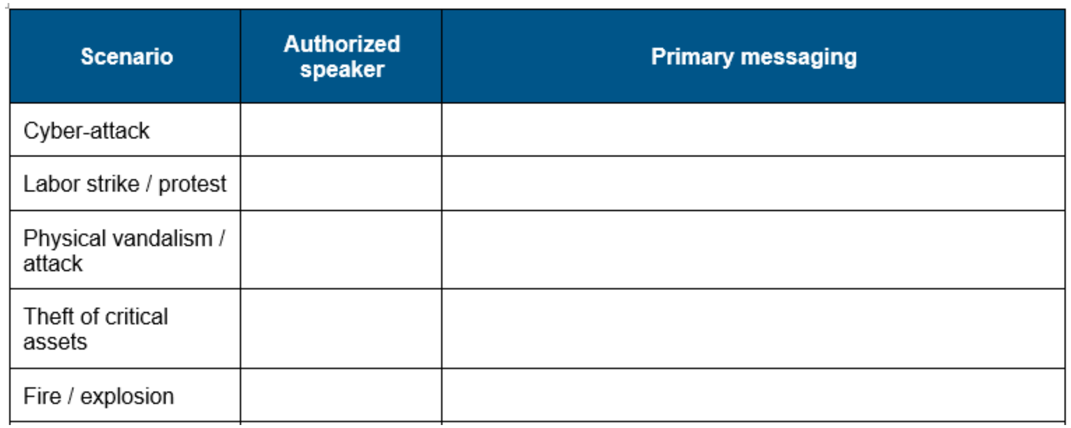
Virtual command center details



Communication medium	*<ADD>*
Conference bridge details	*<ADD>*

2. Crisis management plan – guide

3. Develop pre-prepared media statements for each scenario and nominate a speaker for each one



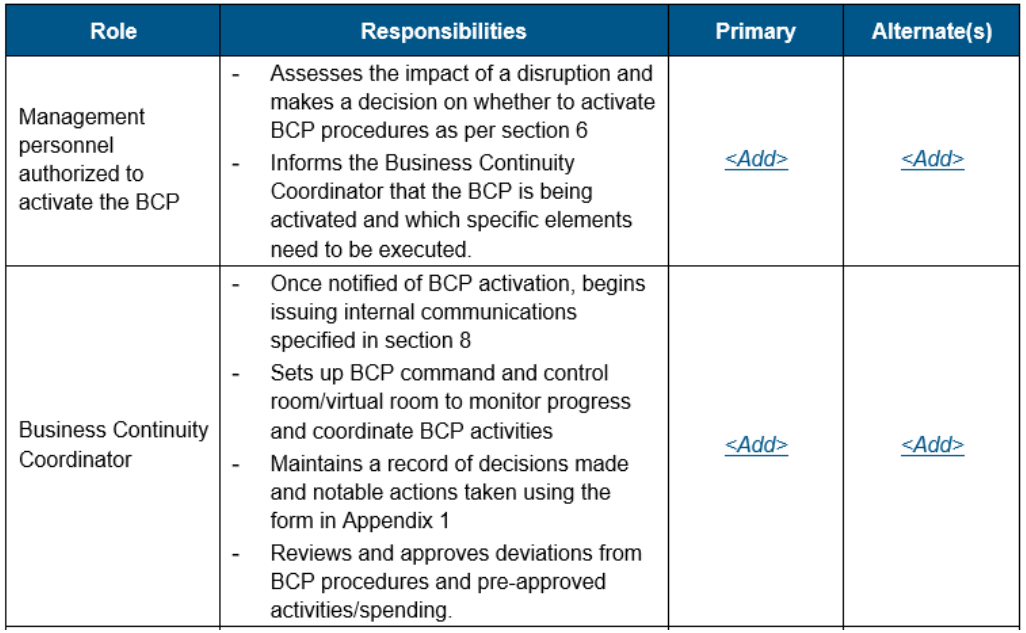
Scenario	Authorized speaker	Primary messaging
Cyber-attack		
Labor strike / protest		
Physical vandalism / attack		
Theft of critical assets		
Fire / explosion		

4. Prepare a list of contact information for crisis management team members and emergency response team leads (and their alternates)

Name	Role	Phone number(s)	Email address

3. Business continuity plan – guide

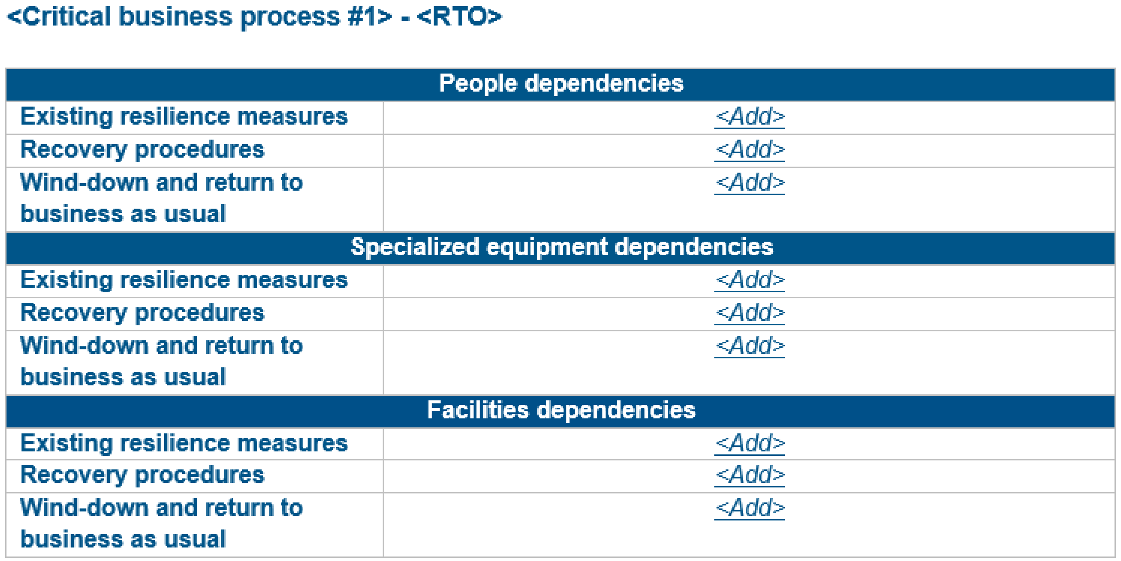
1. Nominate the business continuity team members and identify their alternates



Role	Responsibilities	Primary	Alternate(s)
Management personnel authorized to activate the BCP	- Assesses the impact of a disruption and makes a decision on whether to activate BCP procedures as per section 6 - Informs the Business Continuity Coordinator that the BCP is being activated and which specific elements need to be executed.	<Add>	<Add>
Business Continuity Coordinator	- Once notified of BCP activation, begins issuing internal communications specified in section 8 - Sets up BCP command and control room/virtual room to monitor progress and coordinate BCP activities - Maintains a record of decisions made and notable actions taken using the form in Appendix 1 - Reviews and approves deviations from BCP procedures and pre-approved activities/spending.	<Add>	<Add>

2. For each critical business process, document the following for the resources it requires:

- Any existing resilience measures that are in place, e.g., spare bank cheques stored in a vault offsite
- Detailed recovery procedures, e.g., going to the bank and re-running the last payroll cycle without modification
- Return to normal activities, e.g., reconciling payroll discrepancies from re-running the last payroll without modification



<Critical business process #1> - <RTO>

People dependencies	
Existing resilience measures	<Add>
Recovery procedures	<Add>
Wind-down and return to business as usual	<Add>
Specialized equipment dependencies	
Existing resilience measures	<Add>
Recovery procedures	<Add>
Wind-down and return to business as usual	<Add>
Facilities dependencies	
Existing resilience measures	<Add>
Recovery procedures	<Add>
Wind-down and return to business as usual	<Add>

3. Business continuity plan – guide

3. Add critical process details from the business impact analysis workbook

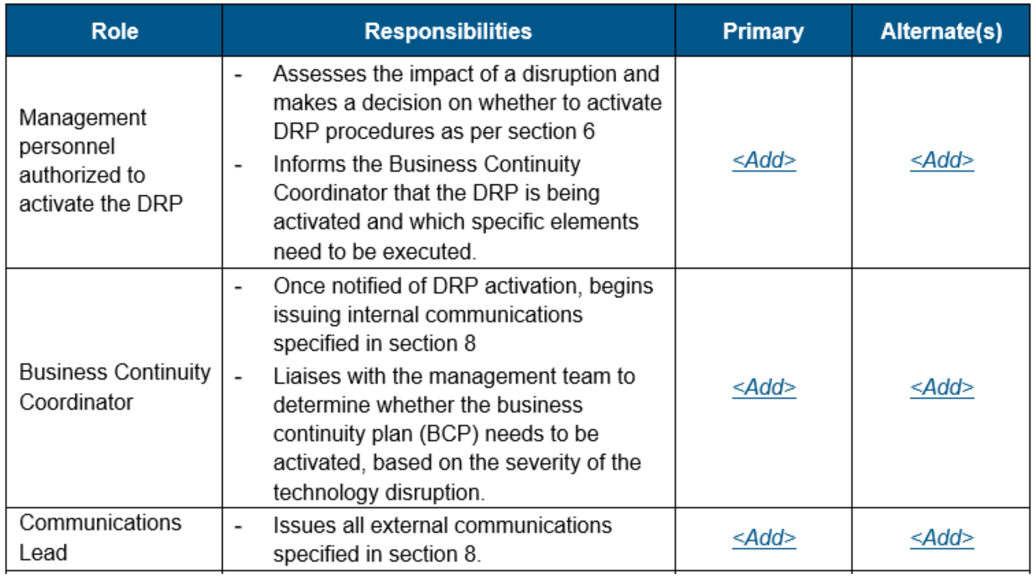
Department	Process name	Recovery time objective	Minimum service level

4. Prepare a list of business continuity stakeholder contact information

Name	Role	Phone number(s)	Email address

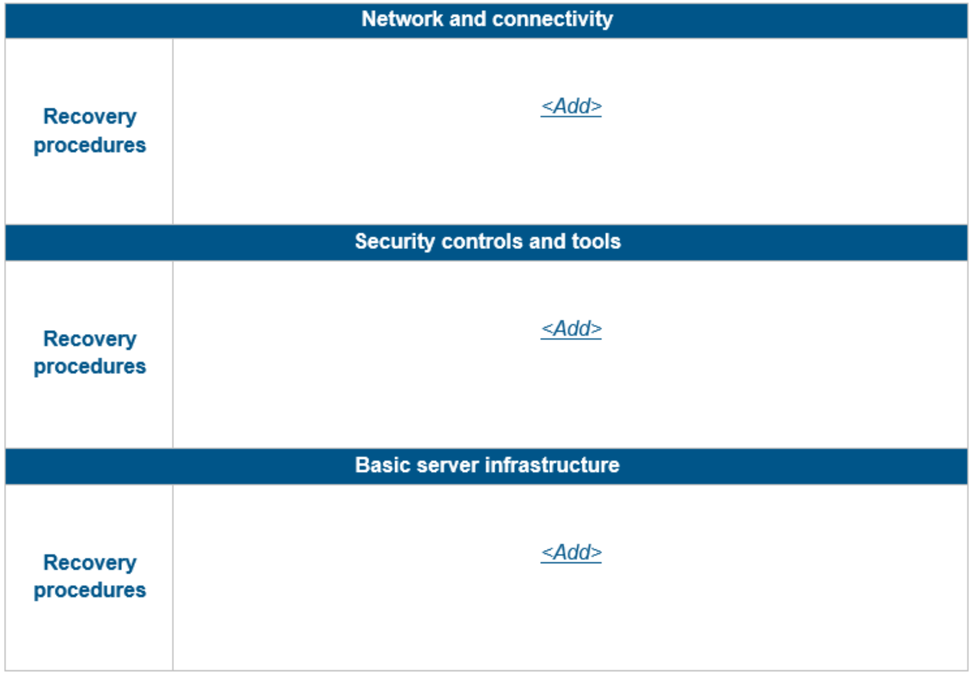
4. IT DR plan – guide

1. Nominate the IT disaster recovery team members and identify their alternates



Role	Responsibilities	Primary	Alternate(s)
Management personnel authorized to activate the DRP	- Assesses the impact of a disruption and makes a decision on whether to activate DRP procedures as per section 6 - Informs the Business Continuity Coordinator that the DRP is being activated and which specific elements need to be executed.	<Add>	<Add>
Business Continuity Coordinator	- Once notified of DRP activation, begins issuing internal communications specified in section 8 - Liaises with the management team to determine whether the business continuity plan (BCP) needs to be activated, based on the severity of the technology disruption.	<Add>	<Add>
Communications Lead	- Issues all external communications specified in section 8.	<Add>	<Add>

2. Document the steps needed to recover the core network infrastructure and/or cloud infrastructure, before individual systems can be recovered. This includes network connectivity, security controls and server infrastructure



Network and connectivity	
Recovery procedures	<Add>
Security controls and tools	
Recovery procedures	<Add>
Basic server infrastructure	
Recovery procedures	<Add>

4. IT DR plan – guide

3. For each critical system (ordered by shortest recovery time first), document the steps to restore the application software and underlying database, and the steps to test key functionality before notifying users that it is ready to use

<System #1> recovery procedures

Application recovery steps	<Add>
Database recovery steps	<Add>
Functionality testing steps	<Add>

4. Document the steps to be taken to migrate back to the original IT environment once the disruption is over/resolved. This includes ensuring the network and infrastructure are ready and that security controls are in place, followed by steps to migrate systems back to that environment and test their key functionality

Network and infrastructure readiness steps	<Add>
Security safeguards readiness steps	<Add>
System migration steps	<Add>
Functionality testing steps	<Add>

4. IT DR plan – guide

5. Add critical process details from the business impact analysis workbook

Department	Process name	Recovery time objective	Minimum service level

6. Prepare a list of disaster recovery stakeholder contact information

Name	Role	Phone number(s)	Email address

Halifax Partnership Resources:

halifaxpartnership.com/how-we-help/grow-your-business/

Minder Singh

msingh@halifaxpartnership.com

Hector Fraser

hfraser@halifaxpartnership.com

Jason Guidry

jguidry@halifaxpartnership.com

HALIFAX PARTNERSHIP

Thank you.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

HALIFAX PARTNERSHIP