Business Continuity Planning for Pandemics

Agenda

- **Introduction**
- **Learning objectives**
- **Risk**
- **Pandemics**
- **Business Continuity**

Introduction

An accomplished Information Communications Technology (ICT) Consultant who has successfully developed and implemented programs, information security and risk strategies and IT-Enabled projects, Mr. Anthony Peyson possess over 25 years of industry experience, having held various ICT positions at major companies within the Energy and Telecommunications Industries.
Currently the Security Architect for a financial services company, Mr. Peyson is also a member of the Board of Directors of The National Information and Communication Technology Company Limited (iGovTT).

Mr. Peyson has been a member of ISACA since 2012 and also hold membership with the Institute of Electrical and Electronics Engineers (IEEE), the Association of Certified Fraud Examiners (ACFE), the International Information System Security Certification Consortium (ISC)², and the EC-Council.

He is a Certified Information Security Manager (CISM), Certified in the Governance of Enterprise IT (CGEIT), Certified in Risk and Information Systems Control (CRISC), Certified Information Systems Security Professional (CISSP), Certified Fraud Examiner (CFE), Certified Ethical Hacker (CEH), Cisco Certified Design Associate (CCDA), Cisco Certified Network Associate (CCNA) and Huawei Certified Network Associate (HCNA).

Why are we doing all of this work?

For Business Survival !

Learning Objectives

At the end of this session you should be able to:

- Define the major characteristics of an influenza based pandemic
- Identify the effects of potentially disastrous or catastrophic events on business continuity
- Identify the differences between a Business Continuity Plan and a Disaster Recovery Plan
- Identify the basic steps in developing an effective Business Continuity Plan
- Identify and Recognize Pandemics and the potential risks they pose to your organisation
- Identify the resources that can aid your organisation’s Pandemic preparedness

What is a Risk?

In simple terms, risk is the possibility of something bad happening.
Source - Wikipedia

Risk – The Business Context

Risk is defined as an event having averse **impact** on **profitability** and/or **reputation** due to several distinct **sources** of uncertainty. It is necessary that the managerial process captures both the **uncertainty** and **potential adverse impact** on **profitability** and/or **reputation**.

https://www.yourarticlelibrary.com/business/risk-management/risk-meaning-concept-and-characteristics/89506

Key Risk Factors

Threats, Threat Sources and Threat Events

Threats

A threat is any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threat Source

A threat source is characterized as:

- the intent and method targeted at the exploitation of a vulnerability
- a situation and method that may accidentally exploit a vulnerability. In general,
    - types of threat sources include:
        - hostile cyber or physical attacks
        - human errors of omission or commission
        - Structural failures of organization-controlled resources
        - natural and man-made disasters, accidents
        - failures beyond the control of the organization

Threat Events

Events are caused by threat sources e.g. cyber attacks, earthquakes, pandemics

Key Risk Factors

Vulnerabilities and Predisposing Conditions

Vulnerabilities

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Predisposing Condition

A **predisposing condition** is a condition that exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operation, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, other organizations, or the Nation.

Predisposing conditions include, for example, the location of a facility in a hurricane- or flood-prone region (increasing the likelihood of exposure to hurricanes or floods) or a stand-alone information system with no external network connectivity (decreasing the likelihood of exposure to a network-based cyber attack)

Key Risk Factors

Likelihood and Impact

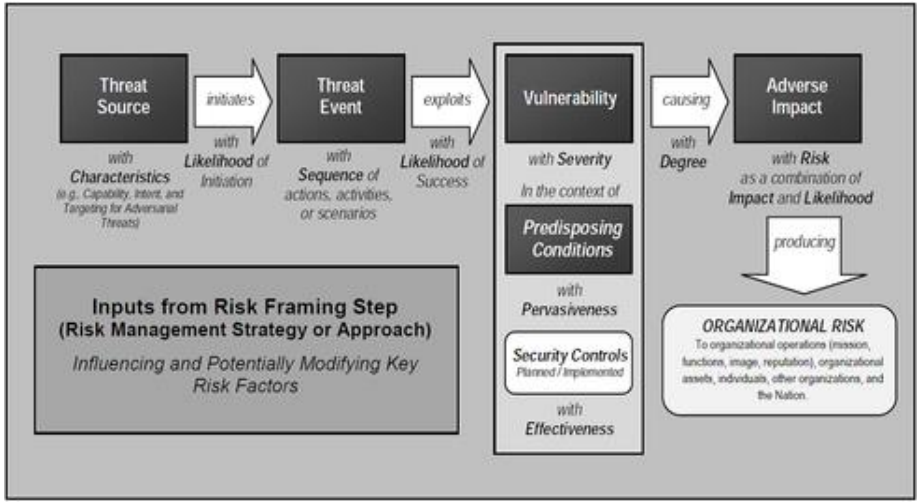
Likelihood

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities).
The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact.

Impact

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Risk Model



1. **Simplified Flow for Risk Generation**
2. Threat Source initiates Threat Event
3. Threat Events Exploits Vulnerability
4. Exploited Vulnerability causes Impact
5. Impact and Likelihood produces Risk

Source: NIST - Generic Risk Model with demonstrating the relationship among Key Risk Factors

Pandemics

Pandemics

What is a pandemic?
A pandemic is the worldwide spread of a new disease.
Source - World Health Organization

Pandemics are large-scale outbreaks of infectious disease that can greatly increase morbidity and mortality over a wide geographic area and cause significant economic, social, and political disruption. Evidence suggests that the likelihood of pandemics has increased over the past century because of increased global travel and integration, urbanization, changes in land use, and greater exploitation of the natural environment (Jones and others 2008; Morse 1995).

Recent pandemics include HIV, Ebola, H1N1,Novel coronavirus (2019-nCoV), SARS.

Influenza Pandemics

An influenza pandemic is a global epidemic caused by a new influenza virus to which there is little or no pre-existing immunity in the human population. Influenza pandemics are impossible to predict; and they may be mild, or cause severe disease or death. Severe disease may occur in certain risk groups, which may correspond to those at risk of severe disease due to seasonal influenza.
However, healthy persons are also likely to experience more serious disease than that caused by seasonal influenza.
Source - World Health Organization

- The Novel coronavirus (2019-nCoV) is categorized as an influenza pandemic.

Pandemic Risk

- Pandemics have occurred throughout history and appear to be **increasing in frequency**, particularly because of the increasing emergence of viral disease from animals.

- Pandemic risk is driven by the combined effects of spark risk (*where* a pandemic is likely to arise) and spread risk (*how likely* it is to diffuse broadly through human populations).

- Some geographic regions with high spark risk and lag behind the rest of the globe in pandemic preparedness.

- Probabilistic modeling and analytical tools such as exceedance probability (EP) curves are valuable for assessing pandemic risk and estimating the potential burden of pandemics.

- Influenza is the most likely pathogen to cause a severe pandemic. EP analysis indicates that in any given year, a 1 percent probability exists of an influenza pandemic that causes nearly 6 million pneumonia and influenza deaths or more globally.

Key Risk Facts about Influenza Pandemics

Frequency
Since the 16th century, influenza pandemics have been found to occur every ten to fifty years.
Annualized Rate of Occurrence (ARO) range is between 0.1 to 0.05

Evidence suggests that the likelihood of pandemics has increased over the past century because of increased global travel and integration, urbanization, changes in land use, and greater exploitation of the natural environment (Jones and others 2008; Morse 1995). These trends likely will continue and will intensify.
Source: Jones K E, Patel N G, Levy M A, Storeygard A, Balk D., and others. 2008. "Global Trends in Emerging Infectious Diseases."

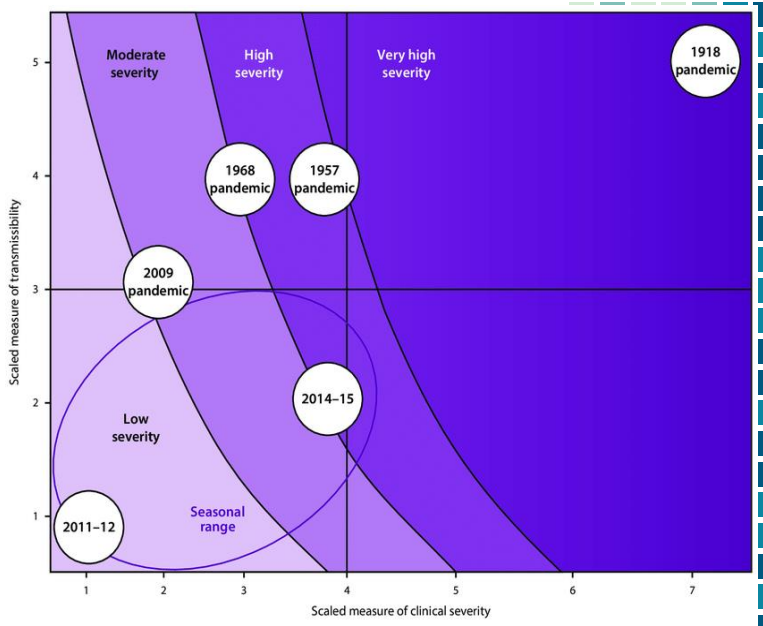
Impact to Businesses
<u>The impact of influenza pandemics on businesses include the following:</u>

- Threat to the physical and mental health of the workforce
- Increased absenteeism of up to 40%
- Unavailability or reduced access to supply chains (border closings, trade suspensions, panic buying)
- Reduced reliability of utilities (electricity, water, internet etc.)
- Reduced reliability of transportation systems
- Drop in walkin-customers due to social distancing policies especially to storefronts

Assessment of Pandemics

Assessment of a probable pandemic?
Once a novel influenza A virus is identified and is spreading from person-to-person in a sustained manner, public health officials use the Pandemic Severity Assessment Framework (PSAF) to determine the impact of the pandemic, or how “bad” the pandemic will be. There are two main factors that can be used to determine the impact of a pandemic. The first is clinical severity, or how serious is the illness associated with infection. The second factor is transmissibility, or how easily the pandemic virus spreads from person-to-person. *Source – CDC*

Influenza pandemic or flu season	Transmissibility	Clinical Severity
Swine Flu 2020 ???	?	?
COVID-19 pandemic	5	4~7
Spanish flu 1918 pandemic	5	7
1957–1958 influenza pandemic	4	4
1968 influenza pandemic	4	3
1977-1978 influenza epidemic	2	2
2009 swine flu pandemic	3	2



Reports - New Flu with Pandemic Potential

HONG KONG — A new strain of the H1N1 swine flu virus is spreading silently in workers on pig farms in China and should be “urgently” controlled to avoid another pandemic, a team of scientists says in a new study**.** *Source – New York Times*

Pandemic Phases

Phase 1: Pre-Pandemic
During this phase, the Business Continuity Plan will be designed, developed, amended, implemented and tested.
This phase involves planning.

Phase 2: During-Pandemic
During this phase, the Business Continuity Plan will be executed.
This can be referred to as the Pandemic Response.

Phase 3: Post-Pandemic
During this phase, business operations will be returning to optimum levels
The effectiveness of the Business Continuity Plan will be examined.
This can be referred to as the Pandemic Recovery.

Business Continuity

Business Continuity

Business continuity is the capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Business continuity management (BCM) is the process of achieving business continuity and is about preparing an organization to deal with disruptive incidents that might otherwise prevent it from achieving its objectives.

Business Continuity Management System (BCMS)

Placing BCM within the framework and disciplines of a management system creates a business continuity management system (BCMS) that enables BCM to be controlled, evaluated and continually improved.

Approach to Business Continuity

A Project management approach is recommended for Business Continuity Planning and Management.

Basic Project Outline

1. Project Management and Initiation
2. Functional Requirements (Business Analysis, Business Impact Analysis (BIA) and Risk Analysis)
3. Design and Development (Recovery Strategies and Plan Development)
4. Implementation
5. Testing
6. Maintenance
7. Execution

Methodology for Business Continuity

Follows: ISO 22301:2019
ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies).

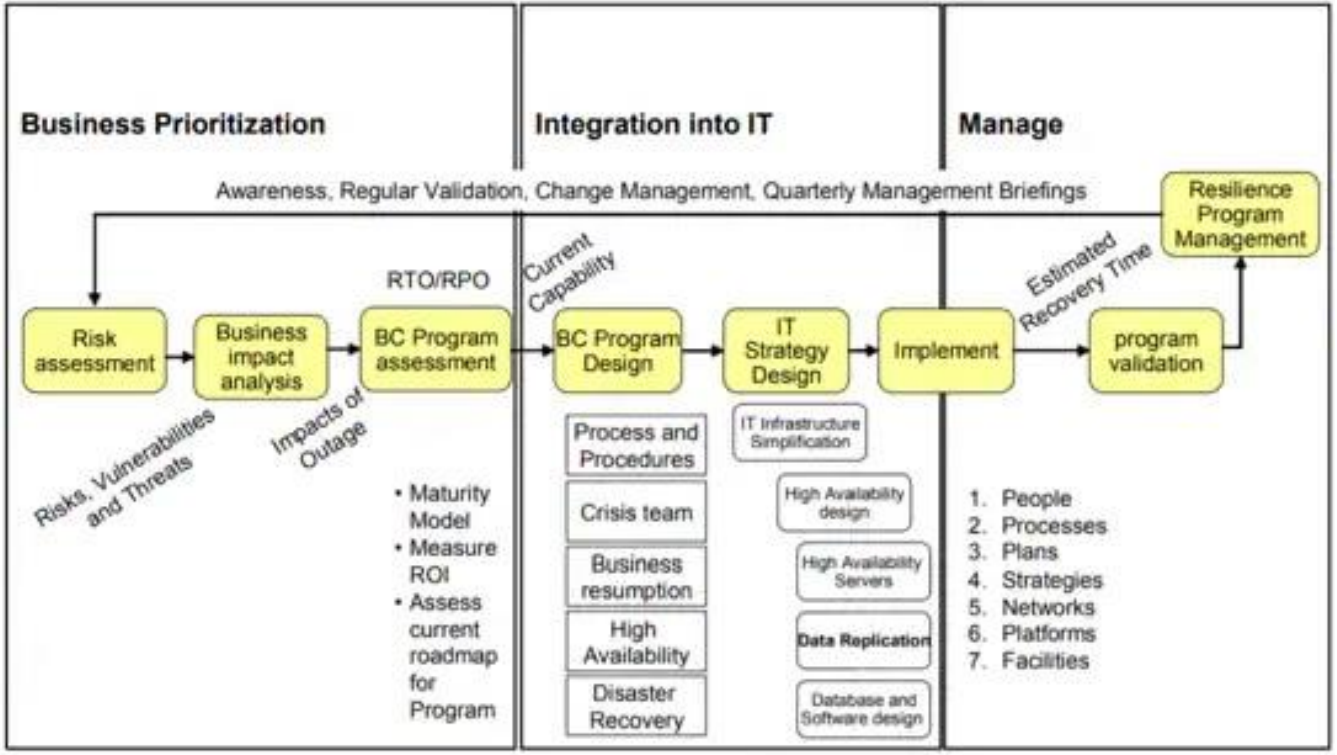
The ISO Standard specifies the structure and requirements for implementing and maintaining a business continuity management system (BCMS) that develops business continuity appropriate to the amount and type of impact that the organization may or may not accept following a disruption.

The Business Continuity Management System (BCMS)
The purpose of a BCMS is to prepare for, provide and maintain controls and capabilities for managing an organization's overall ability to continue to operate during disruptions.

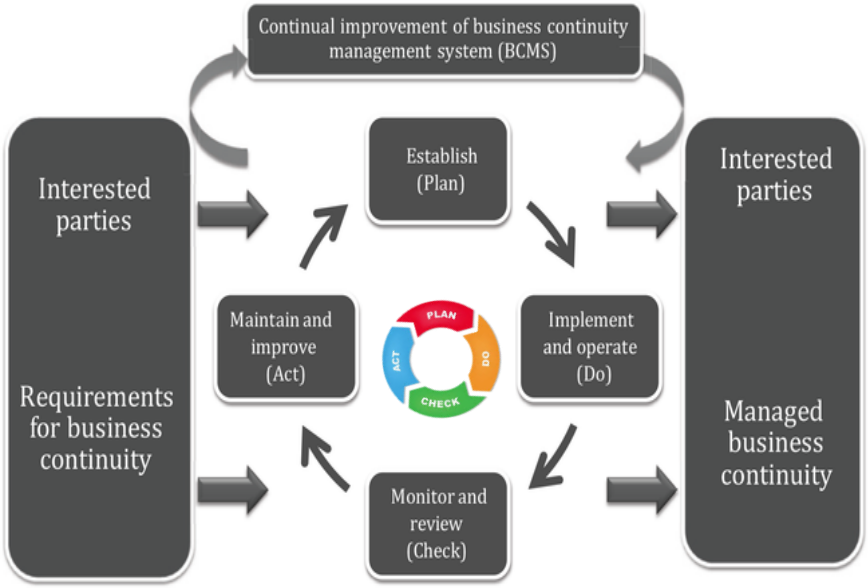
Components of a BCMS

1. policy
2. competent people with defined responsibilities
3. planning
4. implementation and operation
5. performance assessment
6. management review
7. continual improvement

Model of A Business Continuity Management System

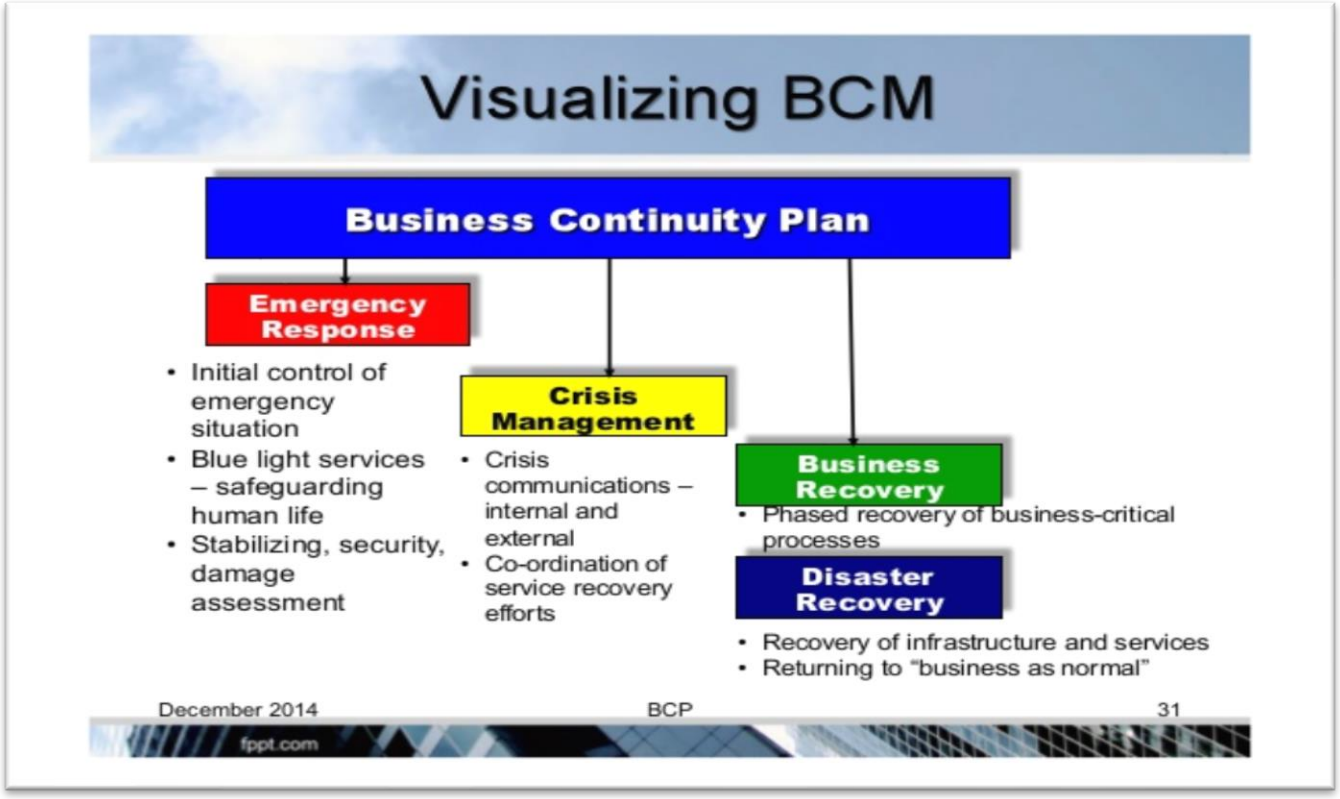


Process Approach of a Business Continuity Management System



Plan (Establish)	Establish business continuity policy, objectives, controls, processes and procedures relevant to improving business continuity in order to deliver results that align with the organization's overall policies and objectives.
Do (Implement and operate)	Implement and operate the business continuity policy, controls, processes and procedures.
Check (Monitor and review)	Monitor and review performance against business continuity objectives and policy, report the results to management for review, and determine and authorize actions for remediation and improvement.
Act (Maintain and improve)	Maintain and improve the BCMS by taking corrective actions, based on the results of management review and re-appraising the scope of the BCMS and business continuity policy and objectives.

Business Continuity Plan – The Big Picture



The Plans

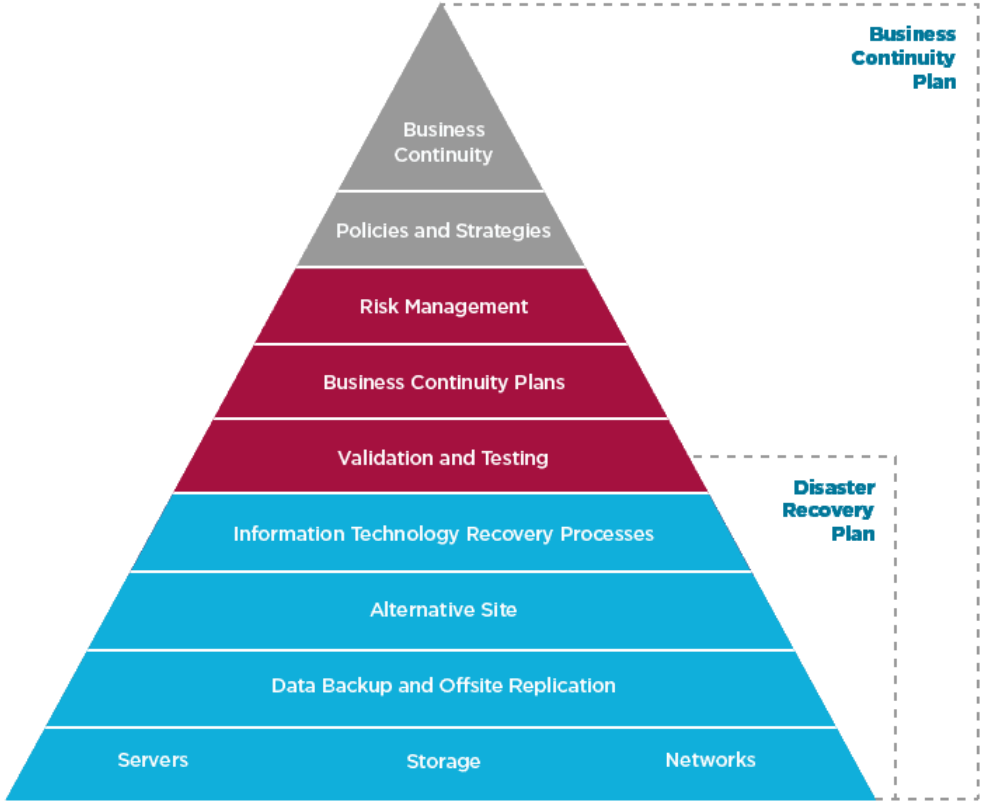
Business Continuity Plan

Business continuity planning is the process of creating systems of prevention and recovery to deal with potential threats to a company. In addition to prevention, the goal is to enable ongoing operations before and during execution of disaster recovery.
Source - Wikipedia

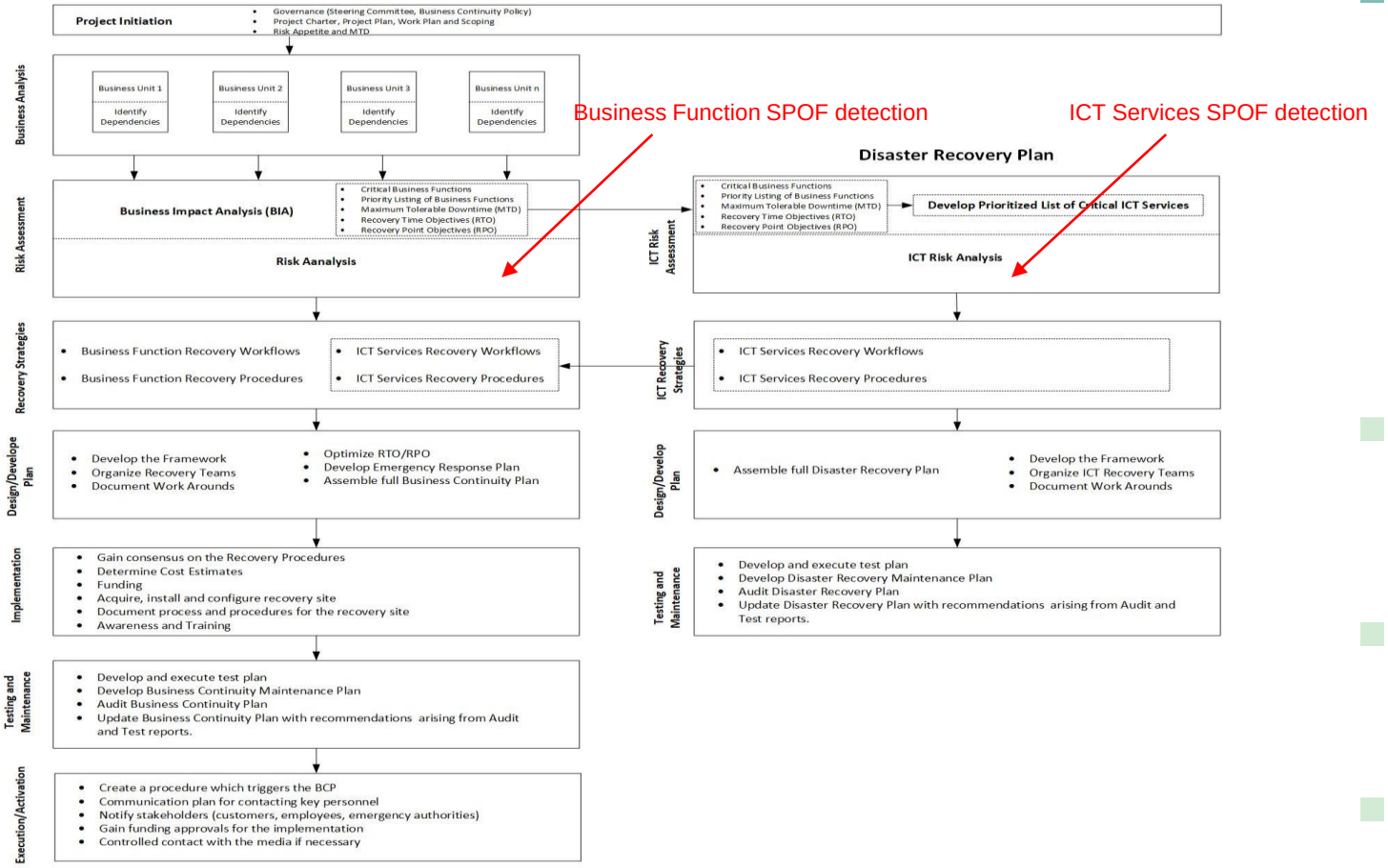
Disaster Recovery Plan

Disaster Recovery involves a set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
Source - Wikipedia

Business Continuity and Disaster Recovery Plans



Business Continuity Plan



Pandemic Phase 1

Phase 1: Pre-Pandemic
During this phase, the Business Continuity Plan will be designed, developed, amended, implemented and tested.
This phase involves planning.

Phase 2: During-Pandemic
During this phase, the Business Continuity Plan will be executed.
This can be referred to as the Pandemic Response.

Phase 3: Post-Pandemic
During this phase, business operations will be returning to optimum levels
The effectiveness of the Business Continuity Plan will be examined.
This can be referred to as the Pandemic Recovery.

Business Continuity Phase 1 - (Project Initiation)

Governance

- Establish a Steering Committee or include in the Steering Committee's Portfolio of Projects
- Define goals, objectives and deliverables
- Define the organization's risk appetite
- Define the project's scope
- Define the work plan
- Define the project team
- Develop the project charter
- Decide on a methodology and approach
- Develop the project plan

Business Continuity Phase 2 - (Functional Requirements)

Business Analysis

- Use the project scope to determine which business units are to be included in the BCP
- **Create process maps and workflows for business functions**
- **Identify critical business processes or functions**
- **Identify all dependencies for all business functions**
    - People (internal or external)
    - Processes
    - IT services (networking, printing, applications etc.)
    - Hard files/documents
    - Facilities (building, furniture, lighting, water etc.)
    - Utilities (Electricity, water, telecommunications, internet etc.)
    - Suppliers
    - Customers
- **Create or update a business Process Inventory**

Business Continuity Phase 3 - (Risk Assessment)

Business Impact Analysis

- Gather data by use of interviews, questionnaires, surveys, workshops, software etc.
- **Determine for each business function:**
    - **Maximum Tolerable Downtime (MTD)** – The longest allowable time a business unit can be unavailable before threatening the survival of the business.
    - **Recovery Time Objective (RTO)** - The maximum allowable time for a business unit to be unavailable. The RTO must be less than the MTD.
    - **Recovery Point Objective (RPO)** - The RPO is the maximum amount of data that can be lost without affecting the business operations.
- **Identify all dependencies for all critical business functions**
- **Determine business impact losses (financial, goodwill, reputation etc.)**
- **Assign priorities to the critical business functions (based on MTD)**
- **Determine the priority for recovery**
- Determine required staff levels for the recovery of each critical business function

Business Continuity Phase 3 - (Risk Assessment)

Risk Analysis

- Identify Threats to each critical business function
- Identify Vulnerabilities associated with the critical business function
- Identify all Single Points of Failure (SPoF) – (Person, Process, Function, Supplier, Customer etc.)
- Determine the Annualised Loss Expectancy (ALE)
- Determine the Risk
- Analyse the effectiveness of existing controls
- Analyse the value of new or augmented controls to provide a cost to benefit
- Update the Risk Register
- Make recommendations in the Business Impact Assessment report

Disaster Recovery – Risk Assessment

ICT Risk Analysis

INPUT: Critical Business Functions (MTD, RTO and RPO values) are forwarded to the DRP development team.

- Develop a list of critical ICT services (Any service used by a critical business process or function)
- Conduct an ICT Risk Assessment
    - Identify Threats to each critical ICT services
    - Identify Vulnerabilities associated with the critical ICT services
    - Identify all Single Points of Failure (SPoF) – (Person, Process, Function, Supplier, Customer etc.)
    - Determine the Annualised Loss Expectancy (ALE)
    - Identify the Risk
    - Analyze the effectiveness of existing controls
    - Analyze to value of new or augmented controls to provide a cost to benefit
    - Update the IT Risk Register
    - Make recommendations in the Business Impact Assessment report

Business Continuity Phase 4 - (Recovery Planning)

Recovery Strategies

- Develop recovery workflows for each business function
- Develop recovery procedures for each business function
- Develop recovery ICT workflows for each IT Service – ***Input from the DRP***
- Develop ICT recovery procedures for each IT Service – ***Input from the DRP***

Business Continuity Phase 4 - (Recovery Strategies)

Examples of Business Recovery Strategies

- Moving to Alternate sites – (Hot, Warm or Cold)
- Provision of safety equipment to prevent disease transmission within the workforce
- Work from home (Teleworking)
- Use of collaborative applications such as Zoom, Cisco Webex, Microsoft Teams etc.
- Alternate suppliers
- The use of eCommerce
- The use of curb-side delivery for products to customers
- Early procurement of medical supplies, PPE and personal hygiene products

(Please, No HOARDING)

Business Continuity Phase 4 - (Recovery Strategies)

Examples of IT Recovery Strategies

- Moving to Alternate sites – (Hot, Warm or Cold)
- Load balancing
- Backups and Restoration Systems
- Failovers
- Data Replication
- Clustering
- Public Cloud Services
    - Cloud Storage
    - Cloud Unified Communications (Hosted PBX)
    - Cloud Based Applications/Platforms (SaaS, PaaS)
    - Cloud Based Infrastructure (IaaS)

Business Continuity Phase 5 - (Design and Development)

Developing the PLAN

- Develop the framework to be used for the Business Continuity Plan – ***(ISO22301:2019)***
- Define the recovery team
  - Identify key individuals for the recovery team
  - Organize the recovery teams (primary and secondary)
- Optimise RTO/RPO
  - RTOs must be less than respective MTDs
  - Reduction of RTO/RPO gap with controls
- Develop an Emergency Response Plan
  - Prepare an Emergency Procedure (Identifies a disaster, communications, emergency contacts e.g. fire, police, ambulance etc.)
- Assemble full plan from all Business Units (BCPs and the DRP)

Business Continuity Phase 5 - (The Plan)

The BCP Document/Library should be designed using a similar structure as shown below:

- Scope, goals and Objectives
- Assumptions
- Emergency Management Procedures
    - Communication (warnings, alerts, announcements)
    - Evacuation (building, facilities, labs etc.)
    - Rendezvous (recovery site(s), alternate site(s))
    - Containment (fire, chemical leakage, flood, bio-hazard, disease etc.)
- Contacts of recovery team, key personnel, clients, vendors and emergency services
- List of critical business units and services (business process inventory, critical services inventory)
- Inventory of all critical recovery requirements
- Transition to alternate sites, work from home
- Primary site recovery
- Repatriation plan, procedures

Business Continuity Phase 6 – (Implementation)

Development of Implementation Strategies and Plans

- Assemble implementation team for the implementation exercise
- Gain consensus on the Business Continuity and Disaster Recovery procedures
- Determine overall implementation costs (recovery facilities, infrastructure etc.)
- Gain funding approvals for the implementation
- Acquire recovery assets
- Install and configure recovery site
- Document process and procedures for the recovery site
- Conduct Awareness and Training for the recovery team (Training) and staff (Awareness)

Business Continuity Phase 7 - (Test and Maintenance)

Development of Maintenance and Testing Strategies and Plans

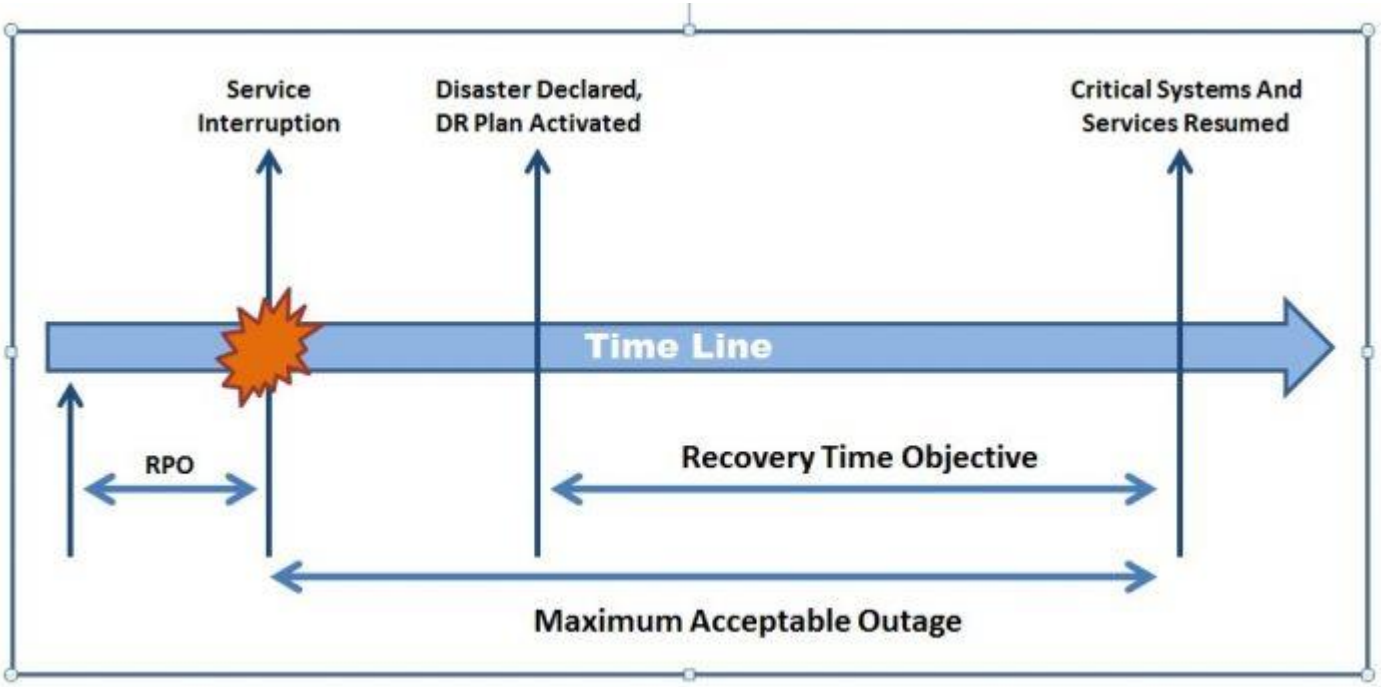
- Develop a test plan
- Select the type of test to be executed
- Select the Test team
- Document the test results
- Maintenance
  - Create a maintenance plan with schedules, responsibilities, version control etc.
  - Assign a group or individuals with the responsibility of maintaining the BCP
- Create a list of approved users
- Apply security controls to the BCP through the information lifecycle
- To manage updates to the BCP when changes occur to Business Processes and IT Services
- Plan to conduct regular audits to determine gaps in the BCP; Updates BCP.

Business Continuity Phase 8 - (Execution/Activation)

Development of Execution/Activation Strategies and Plans

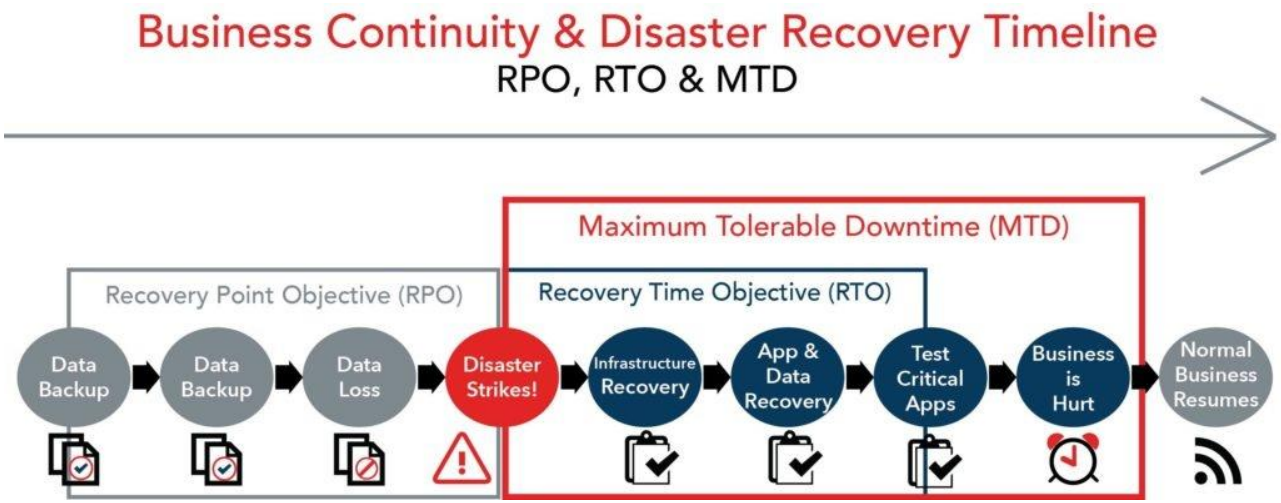
- Create a procedure which triggers the BCP
- Communication plan for contacting key personnel
- Notify stakeholders (customers, employees, emergency authorities)
- Gain funding approvals for the implementation
- Control contact with the media if necessary

Business Continuity during an Incident



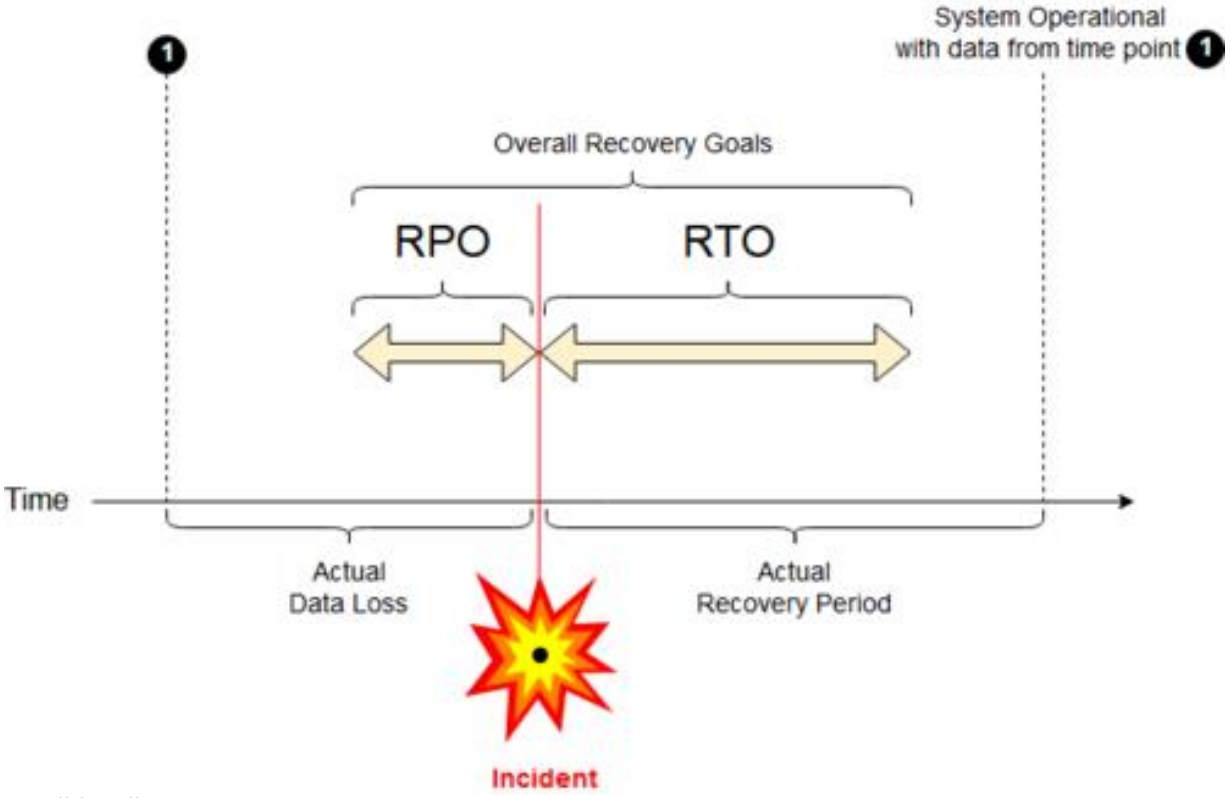
Source: https://www.asianjournal.ca/are-you-absolutley-clear-on-your-disaster-backup-recovery-rto-rpo-and-mto-by-bob-milliken/

Business Continuity during an Incident



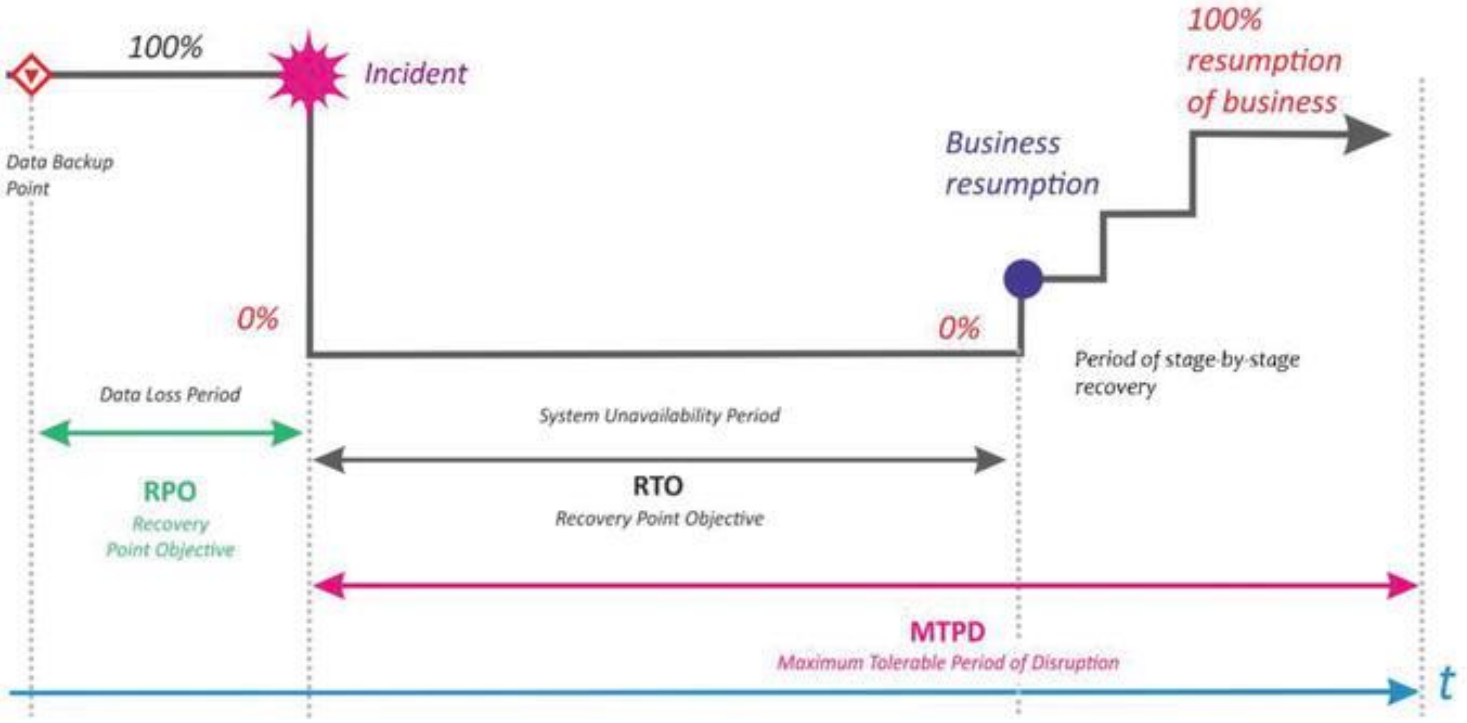
Source: http://blog.centretechnologies.com/maximum_tolerable_downtime

Business Continuity during an Incident

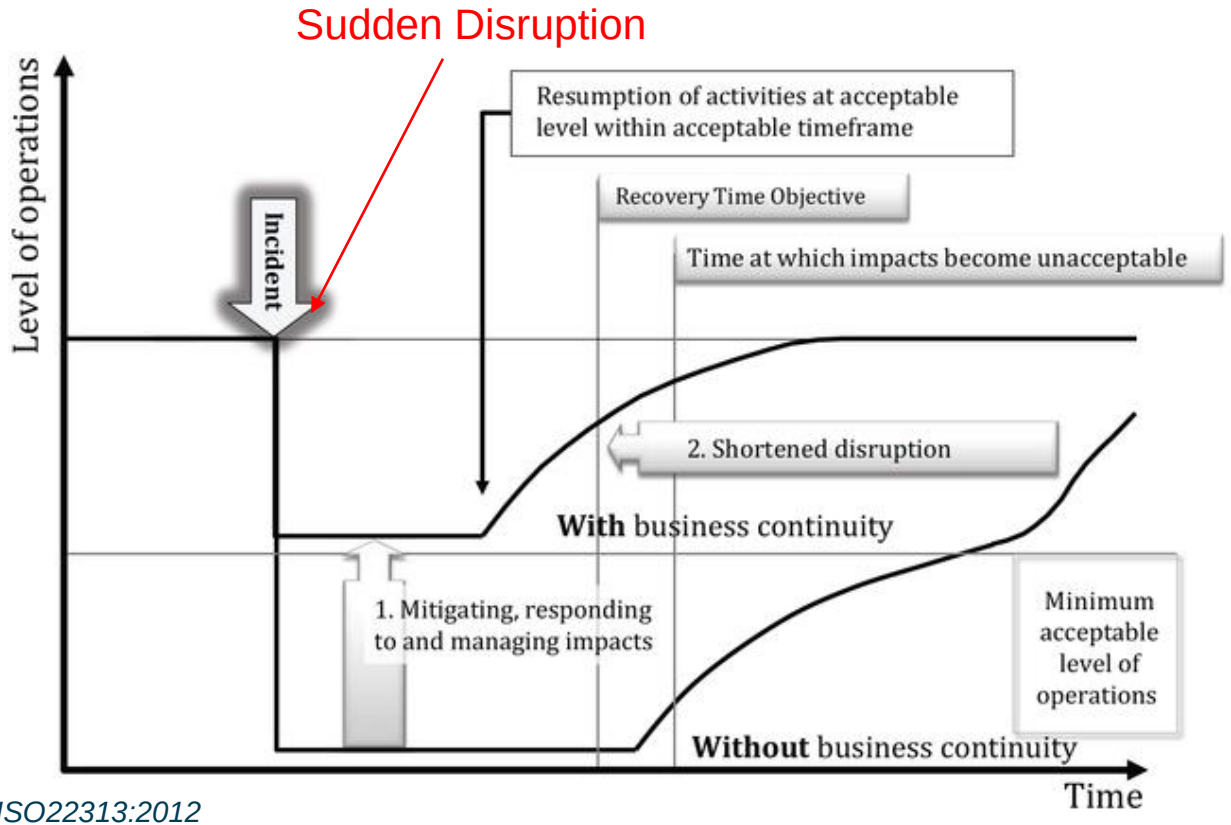


Source: Wikipedia

Business Continuity during an Incident

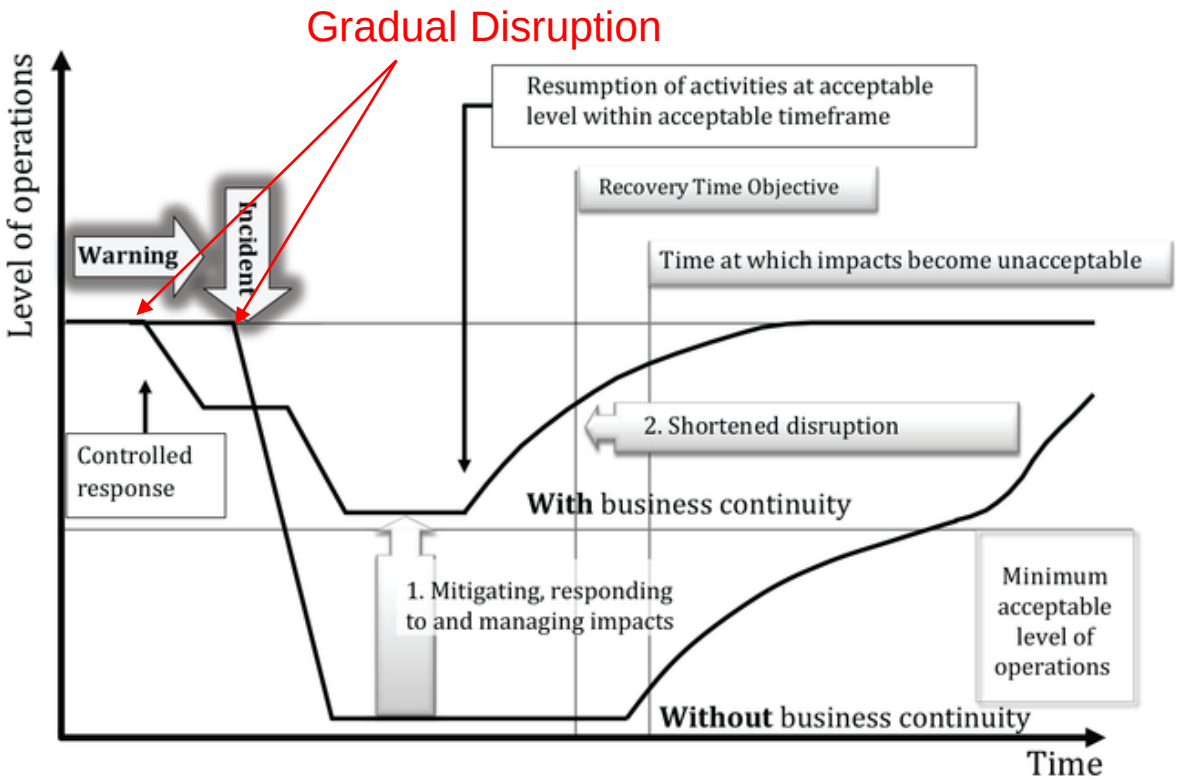


Business Continuity during an Incident



Source: ISO22313:2012

Business Continuity during a Pandemic



Source: ISO22313:2012

Pandemic Preparedness

Action	Things to Consider
Develop/update business continuity and crisis/emergency response plans	• What is the process for decision-making during times of crisis? • How are you identifying and safeguarding your company's essential corporate records and documents? • What are the critical services, positions and skills required to keep your business running? • How and when are you communicating to internal and external stakeholders and managing the flow of information? • What is your plan for recovery?
Plan for the potential impact of the pandemic on your business.	• What is the risk of the pandemic to your employees, partners, suppliers and customers? • Who are the members of the pandemic response team and what are their roles and responsibilities? • What are the triggers and procedures for activating and terminating the pandemic response plan? • What is the decision-making process related to the pandemic and the execution of the business continuity plan? • Who are your most essential employees and what are the other critical inputs (e.g. raw materials, suppliers, sub-contractor services/products, and logistics) required to maintain business operations by location and function during a pandemic? • How are you planning for significant staff absences? • Do you have the tools and technology in place to enable staff to work remotely? • Have you trained and prepared your workforce and your backup resources? • If you were forced to close your doors for two weeks or more, do you have access to a line of credit that will cover ongoing expenses until you can reopen and your cash flow resumes? • What is your plan for scenarios that are likely to result in an increase or decrease in demand for your products and/or services during a pandemic (e.g. effect of restriction on mass gatherings, need for hygiene supplies)? • How are you assessing and managing the potential impact of a pandemic on your financials using multiple possible scenarios? • What is the impact of the pandemic on domestic and international business travel? • What are your sources of relevant, credible up-to-date, pandemic information from federal, provincial, and local public health, emergency management, and other sources?

Pandemic Preparedness

Action	Things to Consider
Plan for the potential impact of the pandemic on your business.	• Is your emergency communications plan up to date and are key roles and responsibilities outlined and communicated? This plan should include identification of key contacts (with back-ups), chain of communications (including suppliers and customers), and processes for tracking and communicating business and employee status. • What is your current travel policy and does it need to be updated? • Has your plan been tested?
Plan for the potential impact of the pandemic on your people.	• What steps can you be taking to protect the health and safety of your staff and visitors to your workplace? • What are the infection control practices in your workplace? • What protective and preventative equipment and tools do you need to put in place to prevent the spread of infection? • How and how often are you communicating with employees, customers and suppliers? • How are you monitoring and managing employee fear, anxiety, rumours and misinformation? • Do you have platforms (e.g. hotlines, website etc.) in place for communicating pandemic status and actions to employees, vendors, customers, etc. and responding to their questions? • Are there guidelines and practices you can modify or put in place to curtail direct contact with the public if necessary? • Do your employee leave policies need to updated to reflect the unique circumstances of a pandemic? Are they compliant with your provincial labour regulations? • Do you have a policy in place for flexible work sites and work hours? • Do you have a policy in place for employees who may, or think they may have been exposed to the virus? • What healthcare services are available to employees? • What mental health services could be provided during a pandemic and possible quarantine? • Are there employees and customers with special needs that need to be accommodated?

Pandemic Preparedness - Resources

Checklists:

Centre for Disease Control: https://www.cdc.gov/flu/pandemic-resources/pdf/businesschecklist.pdf

Information and Advice: (updates will be posted as available)

Borden, Ladner, Gervais (BLG) issued this communiqué:

Deloitte has numerous tools on their web site:
https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/COVID-19/gx-workforce-strategies-for-post-COVID-19-recovery.pdf

Fasken has uploaded information for employers and employees:

https://www.fasken.com/en/knowledge/2020/03/pandemic-planning-for-employers-responding-tothe-coronavirus-disease-2019

World Health Organization planning document:
https://www.who.int/influenza/resources/documents/FluCheck6web.pdf

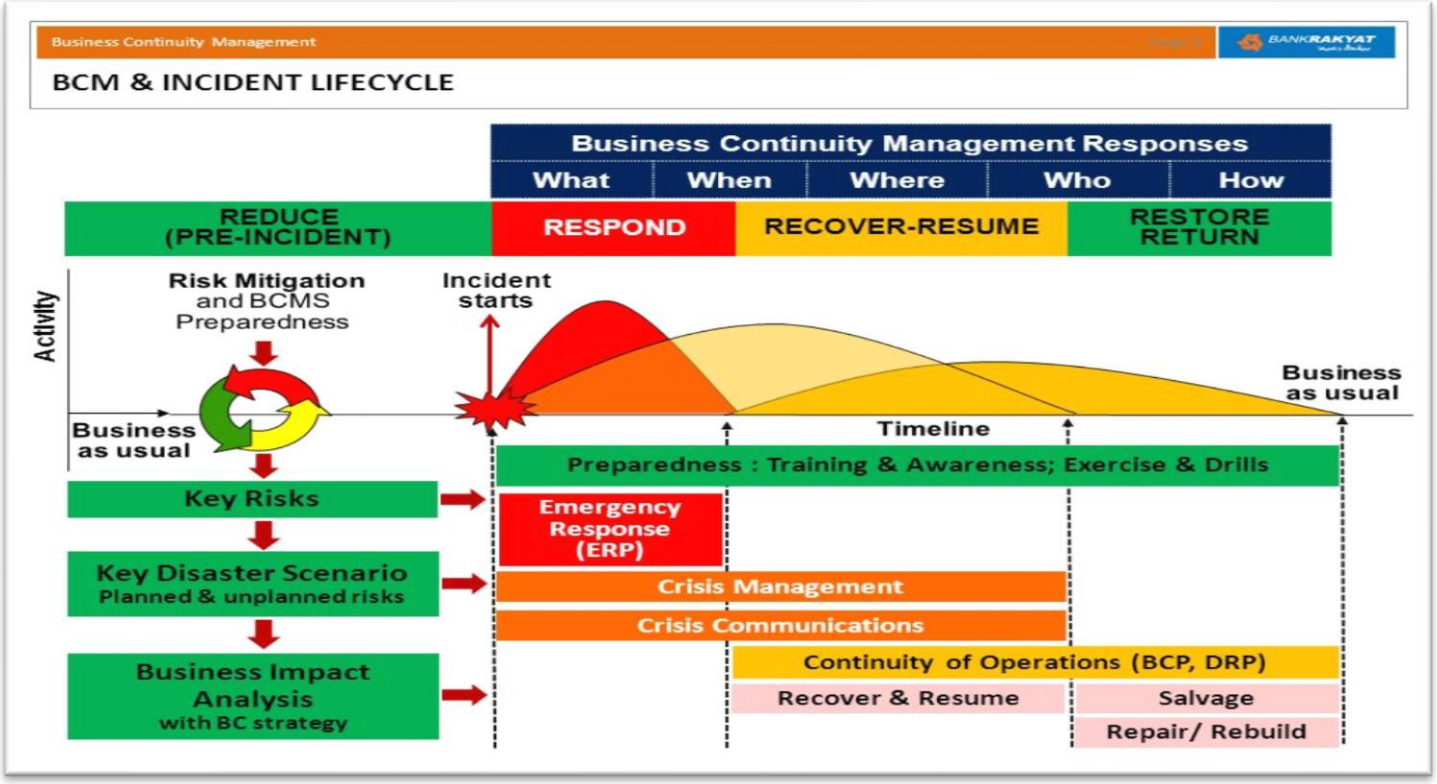
Pandemic Phase 2

Phase 1: Pre-Pandemic
During this phase, the Business Continuity Plan will be designed, developed, amended, implemented and tested.
This phase involves planning.

Phase 2: During-Pandemic
During this phase, the Business Continuity Plan will be executed/activated.
This can be referred to as the Pandemic Response.

Phase 3: Post-Pandemic
During this phase, business operations will be returning to optimum levels
The effectiveness of the Business Continuity Plan will be examined.
This can be referred to as the Pandemic Recovery.

Pandemic Response



Source: http://www.bankrakyat.com.my/

Pandemic Response

Triggers for a BCP during a

- **Disruption to single or multiple critical business functions**
- **Elevated levels of risk to business functions**
- **Specific Disaster Event Occurs**

Response Actions

- Activate the Emergency Response/Crisis Management plan
- The BCP is activated at some point during the crisis
- Monitor the local situation (Government Information Services, Emergence response Services etc.)
- Monitor the international developments on the pandemic (World Health Organisation WHO, CDC)
- Follow recommendations and guidelines by local and international governmental and health organisations e.g. Local Government Information Services, CDC, WHO

Pandemic Phase 3

Phase 1: Pre-Pandemic
During this phase, the Business Continuity Plan will be designed, developed, amended, implemented and tested.
This phase involves planning.

Phase 2: During-Pandemic
During this phase, the Business Continuity Plan will be executed.
This can be referred to as the Pandemic Response.

Phase 3: Post-Pandemic
During this phase, business operations will be returning to optimum levels
The effectiveness of the Business Continuity Plan will be examined.
This can be referred to as the Pandemic Recovery.

Pandemic Recovery

Recovery Actions

- Preparation of the Primary Site
  - Review and restoration of ICT systems/services
  - Preparation of the employee work environment (sick-bays, medical supplies, PPE)
- Repatriation plan (HR and IT)
  - Employee work arrangements (social distancing, provision of face masks, testing for elevated temperature, clean work-desk policy, alternate work days, work-from-home policy, awareness etc.)
  - Full Daily Cleaning (offices, office buildings, wash-rooms etc.)
  - IT Services are restored at the primary site (Backups, data-replication, internet, email etc.)
- Deactivate the BCP (once business functions have been restored to an acceptable level)
- Audit BCP (determine gaps in the BCP)

Tips for better BCP Development

- Digital Transformation of your Organization
- Develop an Emergency Response Plan
- Develop a plan for the BCP plan
- Get executive management support
- Training and Awareness of Staff is Vital
- Always test your plans
- Audit your plans to assure continuous improvement
- Update your plans with recommendations after testing or audits

Important Resources

- **The World Health Organization** – www.who.int
  - https://www.who.int/influenza/preparedness/pandemic/en/
- **Centers for Disease Control and Prevention** – www.cdc.gov
- **Canadian Chamber of Commerce**
  - http://www.chamber.ca/resources/pandemic-preparedness/BusinessPrepGuidePanPrep2020

THANKS!

Any questions?

You can find me at:

apeyson@gmail.com