Business Continuity & Disaster Recovery
(Module - 3 : DISSA Course)

Arijit Chakraborty

Jan 29, 2022

WHAT IS BUSINESS CONTINUITY:

- Business continuity : **plan to deal with difficult situations**, so organization can continue with **as little disruption** as possible.
- Whether it's a business, PSU , or charity, - BCDR is vital

DISASTER RECOVERY PLANNING:

- **Disaster recovery plan (DRP)** : documented, structured approach that describes how an organization can quickly resume work after an unplanned incident.
- **DRP =** essential part of business continuity plan (BCP).
- Applied to aspects of organization that depend on functioning IT infrastructure.
- DRP : help an organization **resolve data loss & recover system functionality** so that it can perform after incident, even if it operates **at a minimal level**.

Standards Supporting BCP & DRP

- ISO 27001: Requirements for Information Security Management Systems.
- Section 14 addresses business continuity management.
- ISO 27002: Code of Practice for Business Continuity Management.
- ISO 22301 – BCMS
- RBI – BCP & DRP
- IRDAI - -do-
- SEBI - -do-
- NIST 800-34
  - Contingency Planning Guide for IT Systems.
  - 7 step process for BCP & DRP projects
  - From U.S. National Institute for Standards and Technology

- HIPAA: Requires a documented & tested disaster recovery plan
  - U.S. Health Insurance Portability and Accountability Act

BCP & DRP Differences

- **BCP**
  - Activities required to ensure **continuation of critical business processes** in an organization
  - Alternate personnel, equipment, and facilities
  - Often includes non-IT aspects of business
- **DRP**
  - **Assessment, salvage, repair, & eventual restoration** of damaged facilities and systems
  - Often **focuses on IT systems**

Business Continuity Planning vs. Disaster Recovery Planning

- Both are directed at recovery of operations
- BCP = directed at **recovery and resumption of business activities** across entire enterprise
- DRP = usually directed **at the recovery of IT systems** & Biz apps , including corporate data
- BCP addresses **Processes, People and Property**

Excerpt from DISSA Study Material

What is disaster recovery? A subset of BC

Disaster recovery includes the backup systems and IT contingency methods for organization's critical functions and applications.

Disaster recovery, as part of an overall BC plan, is about restoring IT systems and operations as efficiently as possible following a disaster. DR includes the backup systems and IT contingency methods for organization's critical functions and applications.

What's the difference between business continuity and disaster recovery?

The former is the overarching plans that guide operations and establish policy. Disaster recovery is what happens when an incident occurs.

Disaster recovery is the deployment of the teams and actions that are sprung. It is the net results of the work done to identify risks and remediate them. Disaster recovery is about specific incident responses, as opposed to broader planning.

After an incident, one fundamental task is to debrief and assess the response, and revising plans accordingly.

Business Impact Assessment

The impact assessment is a cataloguing process to identify the data of company holds, where it's stored, how it's collected, and how it's accessed. It determines which of those data are most critical and what the amount of downtime is that's acceptable should that data or apps be unavailable.

Natural Disasters

1. **Geological:** earthquakes, volcanoes, tsunamis, landslides
2. **Meteorological:** hurricanes, tornados, wind storms, hail, ice storms, snow storms, rainstorms, & lightning
3. **Other**: avalanches, fires, floods, meteors - meteorites, & solar storms
4. **Health:** widespread illnesses, quarantines, pandemics

Not all disruptions are disasters

Man-made Disasters

1. **Labor:** strikes, walkouts, & slow-downs that disrupt services and supplies
2. **Social**-political: war, terrorism, sabotage, vandalism, civil unrest, protests, demonstrations, cyber attacks, & blockades
3. **Materials**: fires, hazardous materials spills
4. **Utilities**: power failures, communications outages, water supply shortages, fuel shortages, and radioactive fallout from power plant accidents

Terrorism Risk Analysis

1. Explosions
2. Biological Threats – *aerosols ,animal infection, food & water poisoning , epidemic* –
3. Chemical threats
4. Nuclear blasts
5. Radiological Dispersion Device (RDD)

Threats

- ✓ Roof leaks /collapse
- ✓ Pipes burst / leak
- ✓ Hydrant / vents leak
- ✓ Localised flooding
- ✓ Chemical spills
- ✓ Fire damage
- ✓ Improper housekeeping – cleaning solvents, flammable liquids'
- ✓ Thefts
- ✓ Sabotage, loss
- ✓ Mishandling

BCP & Crisis management

The Show Must Go On

- **Business Continuity Plan**
- A documented description of

✓ actions to be taken

✓ resources to be used

✓ procedures to be followed before, during & after an event

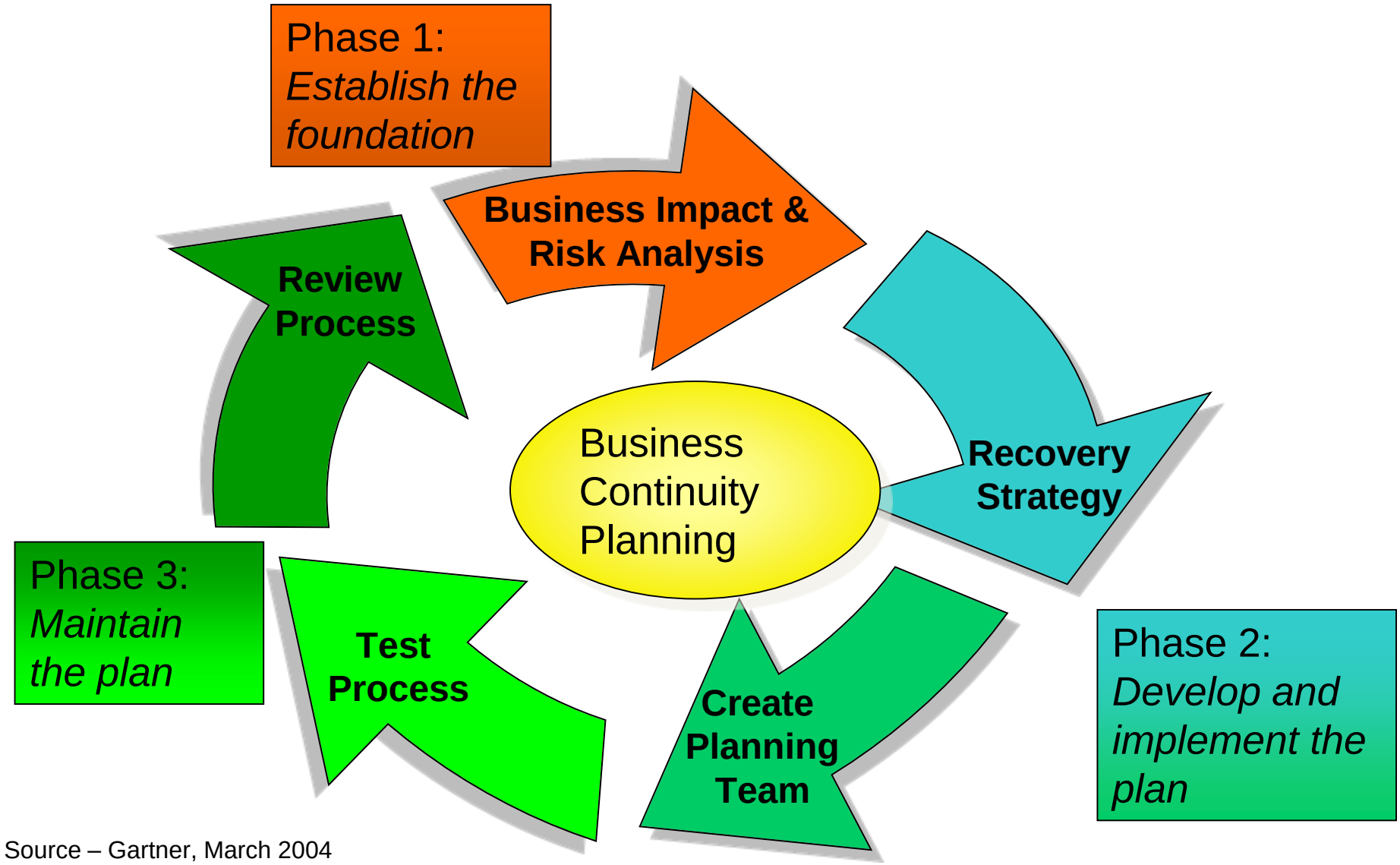
✓ functions vital to continue business operations are recovered

✓ operational in an acceptable time frame

BCP & DRP
= aid in CIA

- BCP & DRP
- Security pillars: C-I-A
  - Confidentiality
  - Integrity
  - Availability
- BCP and DRP **directly support availability**

BCP Process



Source – Gartner, March 2004

ELEMENTS OF BCP:

- **1. Threat Analysis**

Identification of potential disruptions, & potential damage they can cause to affected resources.

2. Role assignment

•Every organization needs a well-defined chain of command **to deal with crisis scenario**.
• Employees must be **cross-trained on their responsibilities**
•Internal departments (e.g., marketing, IT, human resources) to broken down into teams based on their skills and responsibilities.
•Team leaders can then assign roles and duties to individuals according to organization's threat analysis.

3. Communications

•A communications strategy details how information is disseminated **immediately following and during a disruptive event, as well as after it has been resolved.**

•Strategy should include:

✓**Methods of communication** (e.g., phone, email, text messages)
✓**Established points of contact** (e.g., managers, team leaders, human resources) responsible for communicating with employees
✓**Means of contacting** employee family members, media, government regulators, etc.

4. Backups

From **electrical power to communications and data**, every **critical business component** must have adequate backup plan that includes:

- **1. Data backups to be stored in different locations**. - prevents destruction of both original & backup copies at same time.
- If necessary, offline copies may be kept
- 2. **Backup power sources, such as generators & inverters** to deal with power outages.
- 3. **Backup communications** (e.g., mobile phones and text messaging to replace land lines) and backup services (e.g., cloud email services to replace on-premise servers).

Benefits of DRaaS

- offers **cost-effective** reliability
- **addresses challenges** - mobility, portability and high performance,
- Vital for Businesses **where every minute lost = thousands of USD & where credibility matters,**
- **Models**
- On-premise Disaster Recovery Solutions
- Cloud-based Disaster Recovery