Business Continuity & Disaster Recovery

(Module - 3 : DISSA Course)

Arijit Chakraborty

Jan 30, 2022

DRaaS - Benefits

- DRaaS takes burden of DRP off from organization & puts it into hands of experts in disaster recovery.
- May be much more affordable than hosting own DR infrastructure in remote location with an IT staff standing by if disaster strikes.
- If no disaster , that expensive 2nd infrastructure and staff never get used.
- Many DRaaS providers charge only if client need their services.
- Ponemon Institute's "Cost of Data Center Outages"study, = reported : unplanned downtime costs organizations an average of $8,850 per minute.
- DRaaS = Focus on short recovery point objective. RTO Target = 4 hrs approx
- If DC in Florida gets affected by hurricane, DRaaS ensures = data will not be lost by switching to live mirrored servers in Nevada, not affected by hurricane.
- **DRaaS Models : 1. Managed DRaaS**:
- 3rd third party takes over all responsibility for DR.
- organization to stay in close contact with their DRaaS provider to ensure that it stays up to date on all infrastructure, application & services changes

- **2. Assisted DRaaS**:
- If Client prefers to maintain responsibility for some aspects of DRP, or if Client have unique or customized apps that might be challenging for 3rd party to take over = assisted DRaaS
- Service provider offers its expertise for optimizing DR procedures, but customer is responsible for implementing some / all of DRP.
- **3. Self-service DRaaS**:
- least expensive option = customer is responsible for planning, testing and management of DR, & customer hosts its own infrastructure backup on virtual machines in a remote location.
- Careful planning & testing = required to ensure = processing can fail over to virtual servers instantly in the event of a disaster.
- Option = Clients who have experienced DRP experts on staff.

DRaaS vs. backup as a service (BaaS)

- DRaaS = service provider moves an organization's computer processing to its cloud infrastructure in the event of a disaster.
- Business can continue to operate, even if the original IT infrastructure is totally destroyed or held hostage.
- BaaS = *Only the data, but not the ability to process the data*, is duplicated by a 3rd-party provider.
- As BaaS is *only protecting data, & not the infrastructure*, = typically less expensive than DRaaS.
- BaaS = companies that need to archive data or records for legal reasons, most organizations who use BaaS want to combine it with DRaaS to ensure business continuity.

Solar storms : Disaster ?

- Earth subject to : **11- year Cycle** of increased solar activity
- Solar storm = **thermonuclear explosion** on sun
- Sun releases flare. -- sends **huge energy out into space.**
- Flares have potential to hit Earth; many of them - completely harmless.
- If Sun releases very powerful flare & they enter Earth's atmosphere= **severe impact on satellite & IT systems.**
- Charged particles speed **= 4 million mph** – entry into earth atmosphere
- "*Extreme solar flares*" occur : **roughly every 25 years.**
- Considered as **''Disaster"** by Airbus TSOC

Solar storms : Impact

- **Disrupt communication** & navigational equipment,
- **Damage satellites**
- **Cause blackouts** : damaging power plants & electrical grid components

Vulnerable Industries:

1. **Power Grids**
2. **Oil & Gas Pipelines**
3. **Electronic communications** -radio communications, satellite communications, radars & navigation systems.
4. **Earth observation satellites**

- ✓ Satellite communications (200MHz to several GHz) » VHF to UHF Range :
- ✓ **Increased scattering** of satellite-to-ground UHF transmissions = interfere with direct satellite communications links
- ✓ **Severe distortion** of **data transmissions** from geosynchronous satellites
- ✓ **Erroneous positioning** information from GPS -Nav systems » position errors (Aviation)
- ✓ **Fadeout** of signals

Contact Information - SOP

- **Full and updated staff member contact list**
- **Office management contacts**
- e.g. Services (gas, electricity, air-conditioning etc.), building services (landlord, local council., emergency services (also include disaster event numbers)
- **Full and updated customer list:**
- this should be reviewed and revised accordingly once a month
- **Full and updated supplier list:**
- this should be reviewed and revised accordingly once a month
- **Full and updated contractor list:**
- this should be reviewed and revised accordingly once a month

HFDC Bank – BCP Policy Document

- *HDFC Bank's mission is to be a world class Indian bank by adopting a single minded focus on service excellence and product quality.*
- *The Bank has adopted industry leading best practices in establishing a set of operating principles which govern how risks of a significant business disruption are mitigated to protect the Banks customers, employees and stakeholders.*
- *The Bank has a robust and well defined business continuity program which comprises of policies and procedures with clearly defined roles, responsibilities and ownership for Crisis Management, Emergency Response, Business recovery and IT Disaster Recovery Planning.*
- *The Bank's BCP steering committee, represented by the senior executive management of the Bank, approves and oversees the annual BCP strategy and road map.*

- *Regular drills and tests are conducted to cover all aspects of the Business Continuity Plan. Plans are reviewed and maintained regularly to incorporate any changes to environment, people, process and technology.*
- *The Bank's Business Continuity Office continuously works towards strengthening the business continuity preparedness of the Bank.*
- *The Bank's Business continuity program is developed to manage the impact of significant disruptions and will endeavor to resume business and operations to an acceptable level within a reasonable time in the event of a disaster.*
- *While the recovery time objectives (RTO) have been defined and documented in the plans, various external factors beyond our control could affect the actual recovery time.*
- *The Banks business continuity plan is in line with the guidelines issued by regulatory bodies and is subject to regular internal, external and regulatory reviews.*

- ***When a significant disruption occurs:***
- *After a significant disruption or a disaster, if your usual access to funds, transactions or branch is affected,* ***please contact us through our phone banking numbers****.*
- ***Phone banking numbers*** *of your nearest location are published on our website.*
- ***Contact numbers for credit card and debit cards*** *are also printed on the rear of your debit / credit / ATM card.*
- *If you are not able to contact us through phone banking, you could visit our web-site at www.hdfcbank.com and send us your queries and requests through online contact links.*

- ***Alternative Channels for transacting Government Business during calamity / strike / disruptions***
- *The Bank provides multiple modes of payment for fulfilling Government business, such as payment through cash or cheque directly at the Bank's branches, payment through credit cards, debit cards or net banking accounts from the Bank's website.*
- ***If RBI or other Banks are not available**: Tax payments can be processed at our branches or any of the methods mentioned above*
- ***If cheque-based clearing facility is not available**: Funds Transfer can be processed from our branch or website (Net Banking) through NEFT or RTGS*

BCP Policy
Aditya Birla Sun Life Insurance

- Aditya Birla Sun Life Insurance = ISO 22301 certified organization and is one of the few Indian companies to have a fully operational Business Continuity Plan (BCP).
- *'' Our is a response plan, which would kick start in the event of a disaster. We would be able to restore and recover operations for critical processes within a predetermined time after the disaster.*
- *The plan would ensure minimal impact to the organization, its people, and most importantly, its customers."*

ABSLI's Business Continuity Management Policy

- Objective = *to have a planned response in the event of any contingency ensuring recovery of critical activities within agreed timeframes.*
- The plans would comply with various regulatory requirements and minimize the potential business impact to ABSLI.
- Additionally it helps to create a system that fosters continuous improvement of business continuity management.

Programme Overview

- As part of BCP, ABSLI has documented crisis response and recovery procedure for quick response to stabilise the situation,
- BCP procedure to ensure recovery of critical activities.
- **Highlights of BCMS Plan Document:**

✓ Crisis Management & incident response

✓ Data back-up, data and system recovery as documented in the Disaster recovery plan

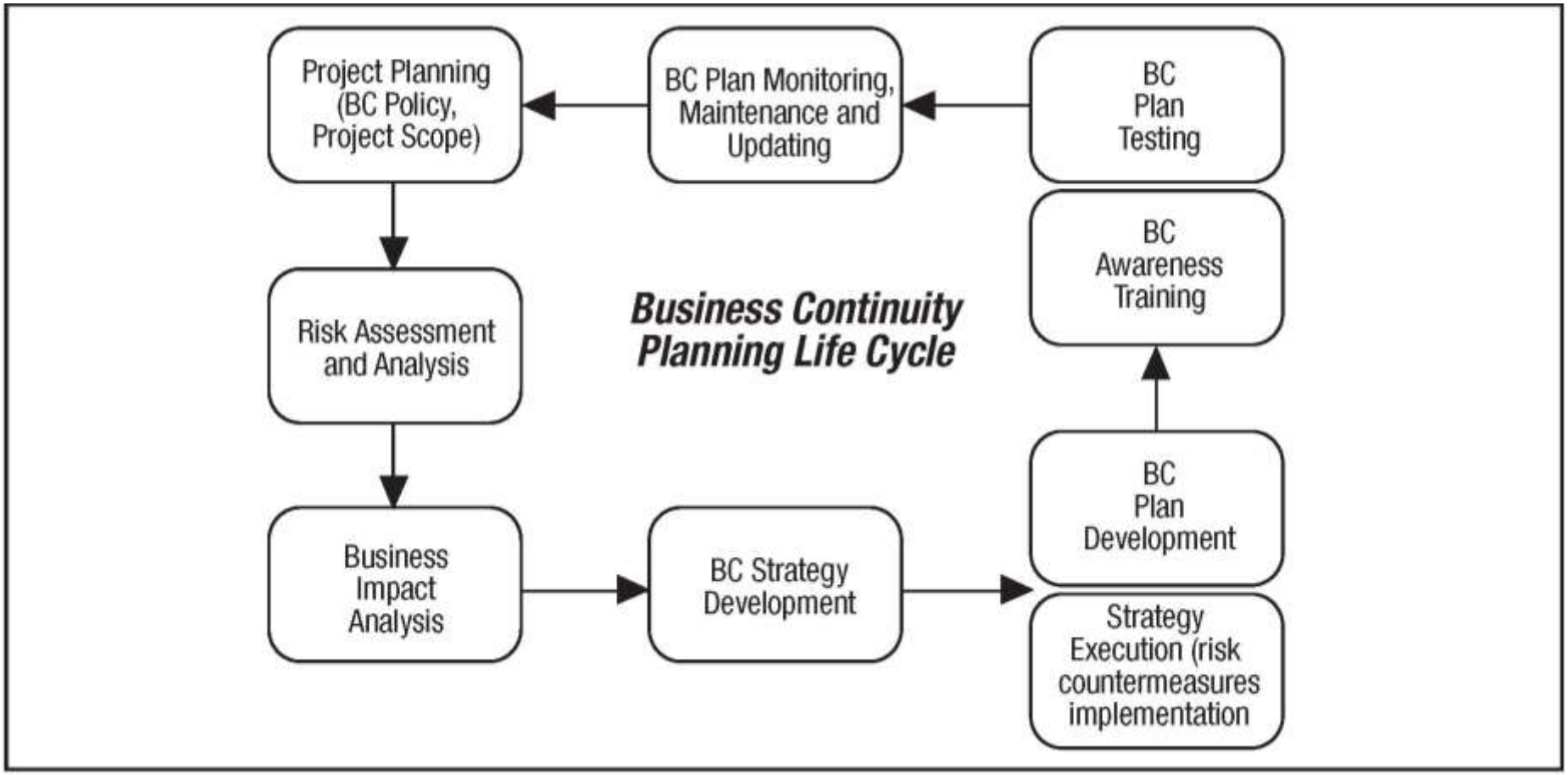
✓ Recovery of all critical business functions and supporting systems

✓ Alternate recovery sites if primary location is unavailable

✓ Communication with customers, employees and other stakeholders

✓ Assurance to customers that they will continue to receive optimum customer services at all times

Business Continuity Planning Process



STEPS OF BCP & DRP:

- **1. Define Key Assets & Operations**
  (BC/DR) efforts start with identification of key assets of infrastructure & processes - important to keeping business operational.
- **2. Determine Downtime, Availability, & Recovery Window**
  Time is money.
- Determine value of investment used to strengthen BC/DR Plan.
- **3. Define Recovery Solutions**
  Define appropriate approach & solutions based on defined assets & recovery window.

4. Draft a Plan

BC/DR plan : Key processes, communication SOP & assigned responsibilities

5. Establish a Communications Plan & Assign Roles

Establish communication plan & assign roles to key members of BC/DR team.

6. Disaster Recovery Site Planning

decide on systems or capabilities required to deliver BC/DR plan.

7. Accessing Data & Applications

Define communications & security protocols for accessing data & apps.

8. Update the BC/DR Plan, In Detail

Develop detailed plan for each system & review what needs to be in place **to implement failover to secondary/redundant connections & offsite storage.**

9. Test , Refine & Audit BC/DR Plan

Organize & execute according to each system's plan.