Business Continuity & Disaster Recovery

(Chapter - 3 : DISSA Course)

Arijit Chakraborty

June 6 , 2021

Standards Supporting BCP & DRP

1. **ISO 27001**: Requirements for ISMS - Section 14 addresses business continuity management.
2. **ISO 27002**: Code of Practice for Business Continuity Management.
3. **ISO 22301** - BCMS
4. 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
5. **HIPAA**: Requires a documented & tested DRP

STEPS OF BCP & DRP:

- **1. Define Key Assets & Operations**
  (BC/DR) efforts start with identification of key assets of infrastructure & processes - important
- **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.

- **Risk Analysis**
  - Critical
    - Functions **cannot be performed unless** they are replaced by identical capabilities
    - Critical applications **cannot be replaced** by manual methods
    - **Tolerance** to interruption = **very low**
    - **Cost** of interruption = **very high**

- **Risk Analysis**
  - Vital
    - Functions can be performed **manually but only for brief** period of time
    - **Higher tolerance to interruption** than critical systems
    - Somewhat **lower costs of interruption** provided functions restored within certain time frame (5 days or less)
- **Critical time period**
  - window of time in which business processing **must be resumed** before suffering significant or unrecoverable losses

- **Risk Analysis**
  - Sensitive
    - Can be performed manually
    - **Tolerable cost**, for extended period of time
    - Manual performance usually difficult process & requires additional staff to perform
- **Risk Analysis**
  - Non-Critical
    - Maybe interrupted for extended period of time at little or no cost to company
    - Requires little or no catching up when restored

Determine Maximum
Step B: Tolerable Downtime (MTD)

For each business process

- Identify **maximum time that each business process can be inoperative** before significant damage or long-term viability is threatened
- Obtain **senior management input** to validate data
- Populate into same database / spreadsheet listing all business processes

Step C: Develop Statements of Impact

For each process:

1. **Describe impact -** on organization if process incapacitated

- **Examples: Criticality Analysis**
  - Inability to process payments
  - Inability to produce invoices
  - Inability to access customer data for support purposes

2. Record Other Key Metrics

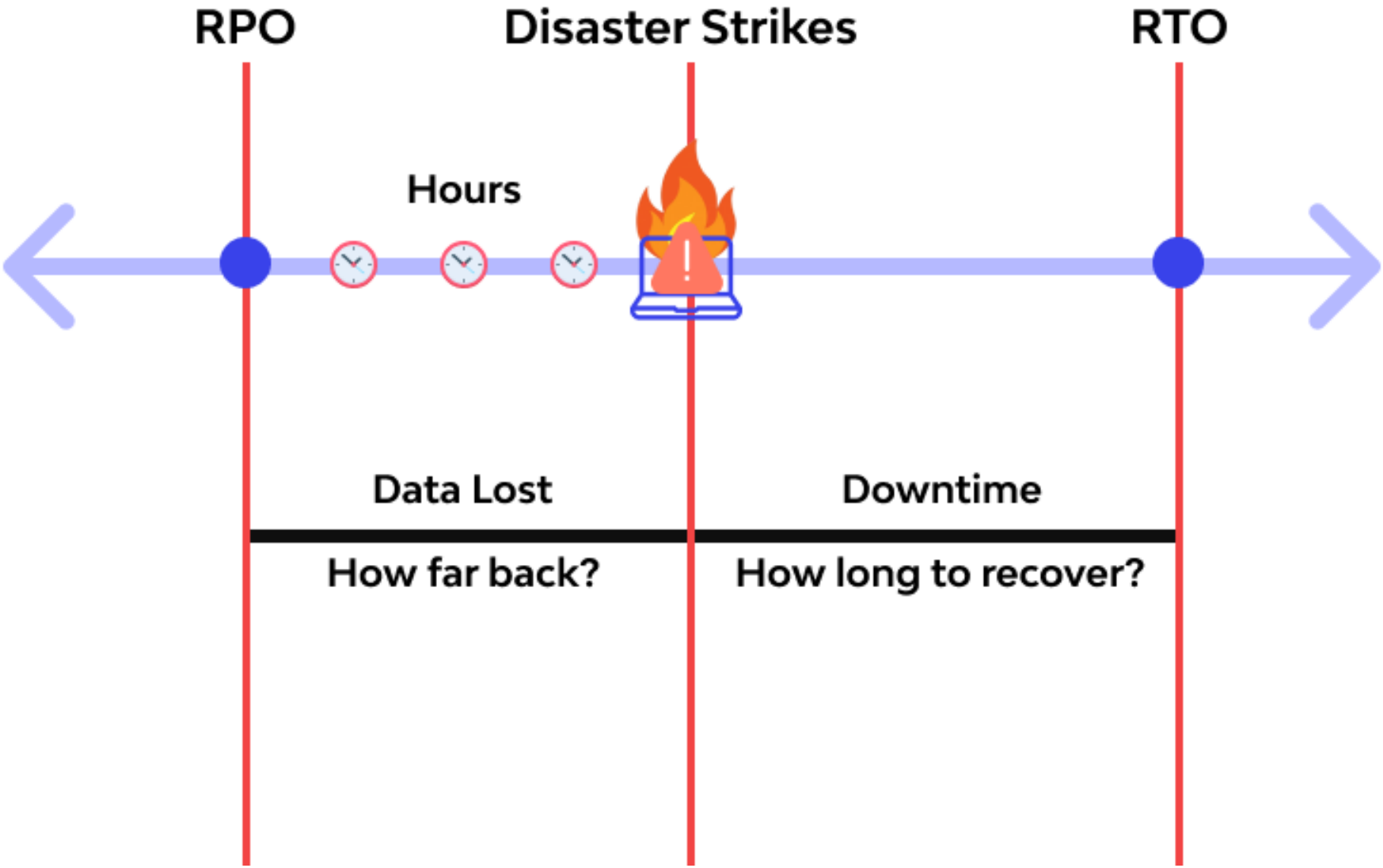
- Cost to operate process
- Cost of process downtime
- Profit derived from process

Step D : Develop Key Recovery Targets

- **Recovery time objective (RTO)**
  - Period of time from disaster onset to resumption of business process
  - Based on acceptable downtime
  - Indicates earliest point in time at which the business operations must resume after a disaster
- **Recovery point objective (RPO)**
  - Maximum period of data loss from onset of disaster counting backwards
  - Amount of work that will have to be done over

Recovery time objective (RTO) – The acceptable downtime for critical functions and components, i.e., the maximum time it should take to restore services. A different RTO should be assigned to each of business components according to their importance (e.g., ten minutes for network servers, an hour for phone systems).

Recovery point objective (RPO) – The point to which the state of operations must be restored following a disruption. In relation to backup data, this is the oldest age and level of staleness it can have. For example, network servers updated hourly should have a maximum RPO of 59 minutes to avoid data loss.


RPO
Disaster Strikes
RTO
Hours
Data Lost
How far back?
Downtime
How long to recover?

RPO, RTO

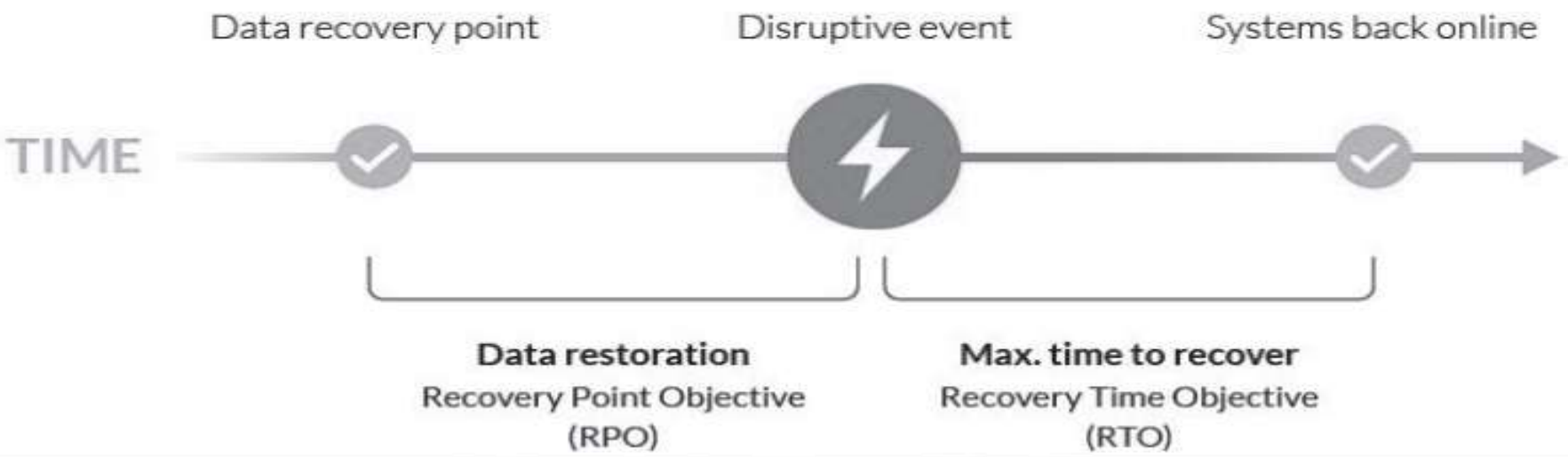
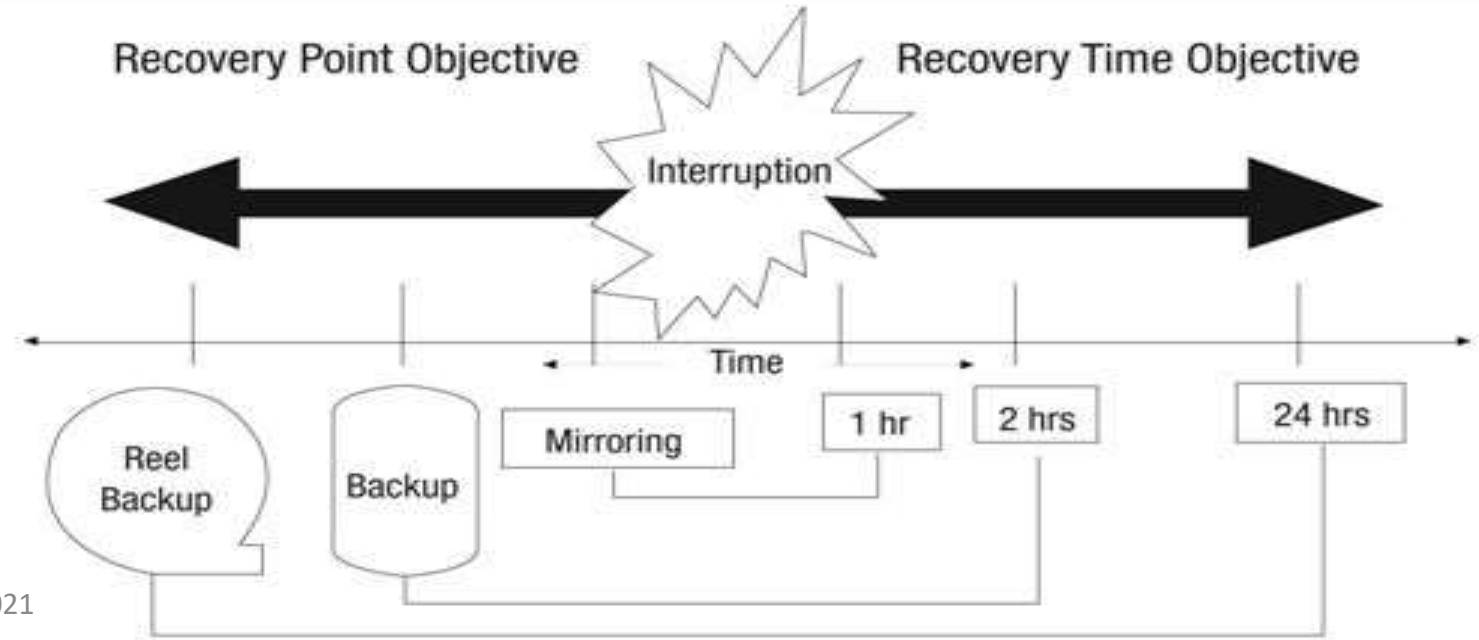


Exhibit 6.5—Relationship Between RTO and RPO



Recovery Point Objectives

RPO	Technology(ies) required
8-14 days	New equipment, data recovery from backup
4-7 days	Cold systems, data recovery from backup
2-3 days	Warm systems, data recovery from backup
12-24 hours	Warm systems, recovery from high speed backup media

RPO	Technology(ies) required
6-12 hours	Hot systems, recovery from high speed backup media
3-6 hours	Hot systems, data replication
1-3 hours	data replication
< 1 hour	near **real time data** replication

RTA & RPA

- Recovery time actual (RTA) & recovery point actual (RPA) = elapsed time & lost data of an **actual recovery process** & often different from RPO & RTO.
- Only ACTUAL business disruption & disaster rehearsals **can expose** these actuals.
- **Example**
- Backup plan that schedules backups twice a day at 6 AM & 6 PM. A primary **site failure at 2 PM** allows team to restore from 6 AM backup an RPA of 8 hours.
- RTA = how long restore takes, & additional work necessary to return the system to full operation.

Documentation review by IS Auditor

Look for documents covering:

- Evacuation
- Fire
- Occupational Health & Safety
- Environmental policies
- Equipment maintenance guides
- Security procedures
- Insurance
- Office closing plans
- Staff manuals
- Hazardous material plans

- Local emergency management office
- Fire department
- Hazardous materials response organization
- Hospitals
- Local police
- Utilities
- Contractors/suppliers
- Insurance contacts

Documents such as:

- Emergency contact details
- Building/facility/site maps identifying floor plans, network cables, stairways, designated escape routes, restricted areas, utility shutoffs, fire extinguishers and suppression systems, water mains, etc.
- Resources needed for emergencies
- Mutual aid/support agreements with other businesses and government organizations

Key Action points

Recovery Alternatives

Types of offsite backup facilities

Hot sites - Fully equipped facility

Warm sites - Partially equipped but lacking processing power

Cold sites - Basic environment

Duplicate (redundant) information processing facility

Mobile sites

Business Continuity Plan/Disaster Recovery Plan – IS Audit IC 15 Point Questionnnaire

- ***YES - NO Type***
- *1. Do you have a BCP/DRP?*
- *2. Were you affected and did you plans help?*
- *3. Do you have your plans and key documentation printed, stored safely and accessibly away from work? Does it include the following:*

❑ *.Names, addresses and phone numbers for the crisis management staff, staff members, clients and vendors?*

❑ *. Location of the offsite data backup storage media? Locations of alternative worksites?*

❑ *. Copies of sales contracts, agreements or other key business documents? Copies of insurance contracts?*

❑ *. Does the insurance policy include business interruption coverage?*

❑ *. Other critical materials necessary for business survival?*

- *4. Does the insurance policy include business interruption coverage?*
- *5.Do you know the potential financial and non-financial impact of a business interruption involving major human, physical and technology loss?*
- *6. Do you know what minimum resources needed to recover critical business functions ?*
- *7. Do you know what are your maximum tolerable outage and critical activities are in the event of a disaster?*
- *8. Have you identified alternates for all your personnel, especially your recovery team members who hold responsibilities during a disaster?*
- *9. Does the plan include backup facilities? Hot backup site?*
- *Cold site? Reciprocal agreement?*

- *10.Have you recently completed an impact/risk analysis?*
- *11. Have you recently completed an impact/risk analysis?*
- *12. Does your organisation have the project management skills or staff to identify, plan and execute the next steps in re-building as well as continuing to operate as a business?*
- *13. Are there alternatives for entering input normally keyed on-line?*
- *14. Is there a layout of your communications network? Is a copy of it stored off-site?*
- *15. Are you happy with your critical suppliers' and outsourced providers' business continuity plans, such that they will not have a significant impact on your business?*

IS Auditor opinion

We hereby opine as follows :

A BCP – DRP Continuity Planning Program exists (which includes all the company's / department's continuity planning documents, processes, and procedures) and that this program contains the key elements as listed in the checklist above;
A program is in place to ensure the confidentiality of the sensitive material in the documents and only persons authorized because of their operational functions will have access to sensitive portions of the document; and,
A maintenance cycle and protocol has been established to address any gaps identified on the checklist above and, per Executive Order _____, to ensure the regular update of the Continuity Plan and related documents.

Internal Audit role in BCP review -*IIA* Guidelines

Practice Advisory 2110-2: Internal Audit's Role in the Business Continuity Process

- During the audit, Internal Audit should consider:
  - Are all plans up to date?
  - Are all critical business functions and systems covered?
  - Are the plans based on the risks and potential consequences of business interruptions?
  - Are the plans fully documented?
  - Have functional responsibilities been assigned?
  - Is the organization capable of and prepared to implement the plans?
  - Are the plans tested and revised based on the results?
  - Are the plans stored properly and safely? Is the storage location known?
  - Are the locations of alternate facilities (backup sites) known to employees?
  - Do the plans call for coordination with local emergency services?

Ministry of Commerce & Industry-Guidelines on BCP-DRP for IT/ITES SEZ

सत्यमेव जयते

Ministry of Commerce and Industry
Government of India

No. D.12/25/2012-SEZ
Government of India
Ministry of Commerce & Industry
Department of Commerce
(SEZ Division)

Udyog Bhavan, New Delhi
Dated : 20 February, 2013
22nd

Subject: Guidelines for Setting up Disaster Recovery (DR) and Business Continuity Plans (BCP) Centers for IT / ITES SEZs

Disaster recovery (DR) may be seen as the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to a business organization after a natural or human-induced disaster occurs. Disaster recovery may be seen as a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.

DR/BCP are essential for businesses today and more especially for IT/ITES businesses. Businesses with no DR/BCP systems i.e. no saved information, no documentation, no backup hardware, and no contingency plan are unable to put into place any recovery time objectives (RTO) which is the duration of time and a service level within which a business process must be restored after a disaster (or disruption) and also are not in a position to assure "recovery point objective" (RPO), which is the maximum tolerable period in which data might be lost from an IT service due to a major incident, to its clients. Such businesses are unable to attract business as all business clients seek assurances on credible RTOs and RPOs which are written into their business contracts.

In addition IT sector can be adversely affected by major power outages, industrial sabotage, data theft, cyber attack etc. These events may also have a major disruptive effect of hindering the business activity of the IT/ITES unit or cause stoppage of work at the unit.

2. Movement of back up data on tapes/ storage devices from SEZs to locations outside the SEZ.

Prevention and creating data backup is an integral part of the IT/ITES sectors DR/BCP strategy. The data is regularly backed up at locations which are isolated from the main business centres to prevent its loss in the event of a disaster. This wouold entail movement of data from SEZ to a DR/BCP location outside the SEZ and movement of storage media back into the SEZ. This movement of data on storage

3. Setting up DRC/BCP Centres by SEZ Units:

a) The DRC/BCP location will be approved by the DC, SEZ on an application made by the SEZ unit. Such approval will allow the SEZ unit to relocate its operations, data and employees to the DRC/BCP location upon the occurrence of a disaster. If the DR/BCP location is within another SEZ / EOU the DC of such SEZ/EOU may also be consulted prior to issue of approval.

d) On the occurrence of events pre-defined under the category of 'disaster', the unit will not need to seek prior approval of DCs to put into operation the DR/BCP strategy. However within 48 hours of the DR/BCP being put into operation the unit must intimate the DC, SEZ

e) On the occurrence of a disaster, it will be necessary for the IT SEZs to carry out real time BCP/DRP operations including shifting of data, operations and employees to be shifted and re located to the DRC/BCP site on a temporary basis, till restoration of operations at the original location. The validity of the relocation will be initially for a period of 90 days and may be extended by DC office and any further extension will be granted based on application to DC

This has the approval of Commerce Secretary.

20.2.13

(Sanjeet Singh)
Director
Tel. 2306 2109
Fax: 2306 3418
e-mail; sanjeet@nic.in

To:

1. All Development Commissioners of SEZs
2. Department of Revenue (CBDT/CBEC), Govt. of India
3. DG, EPCES
4. Department of Information Technology, Electronics Niketan, 6 CGO Complex, New Delhi.
5. DG, National Disaster Management Authority, New Delhi.

IDBI Bank – BCM Document analysis

- *In order to ensure continuity of business operations during business disruptions/ disasters on account of process disruptions, technology break down, power failure, natural calamities, fire, riots etc, the Bank has put in place a well defined board approved BCM Policy.*
- *IDBI Bank implements Business Continuity Plans (BCP) within the Bank and regularly maintains and updates various Business Continuity documents for its critical functions, as per BCM policy.*

ISO 22301 Compliance

- *Business Continuity Management System of IDBI Bank is accredited to ISO22301:2012 standard which demonstrates the Bank's commitment towards maintaining uninterrupted banking services, thereby enhancing customer satisfaction, quality of customer service, superior delivery standards besides assuring organizational performance improvement.*
- **BCM Policy Statement**
- ***"The Bank endeavors to render critical banking services to all its customers, within shortest possible time, in the event of any business disruptions/disaster."***

Scope of BCM

- ***Scope of BCM Policy***
- *The scope includes following:*
  - *Core Functions:*
- *Retail Banking Group (RBG) Branches,*
- *Corporate Banking Group (CBG) Branches,*
- *DIFC Branch Dubai,*
- *Trade Finance Centers,*
- *Treasury,*
- *Information Technology Dept. (ITD),*
- *Retail Asset Center(RAC),*
- *Regional Processing Unit (RPU),*
- *Central Processing Unit (CPU), Central Clearing Unit (CCU),*
- *Cash Management Services (CMS)- Operations,*
- *Government Business Group (GBG)*
- *Operations,*
- *Currency Chest Operations and*
- *Electronic Transaction Processing Centre (ETPC)*

– *Support Functions:*

- *Human Resource Dept.,*
- *Finance & Accounts Dept.,*
- *Legal Dept.,*
- *Administration and*
- *Facilities & Infrastructure Management Dept (FIMD),*
- *Corporate Strategy and Communications Dept (CSCD),*
- *Data Centre and*
- *Disaster Recovery Site.*

- *IDBI Bank's Subsidiaries:*

- *IDBI Asset Management Limited, IDBI Trusteeship services Ltd*
  - *Premises for Disaster Management*
- *C.G. Road Ahmedabad,*
- *Mission Road Bangalore,*
- *Janpath Bhubaneswar,*
- *Sector 17B Chandigarh,*
- *Saidapet & Disaster Recovery Site at Nandanam Chennai,*
- *GS Road Guwahati, Chapel Road Hyderabad,*
- *Panampilly Nagar Kochi, S. Sarani Kolkata, BKC Bandra (E),*
- *IDBI Tower Cuffe Parade,*
- *Corporate Park Chembur,*
- *CPU-Sarju House Andheri (East),*
- *RPU Elemech Building Andheri (East),*
- *Central Clearing Unit Nariman Point,*
- *CBD Belapur Navi Mumbai,*
- *FC Road Pune and IDBI Asset Management Co. Ltd.*

- ***Objectives of BCM Policy***
- *The Bank intends to provide critical services to its valued customers during business disruptions/ disaster.*
- *To ensure safeguards and well being of people within Bank's premises.*
- *To minimize or prevent business/ financial losses on account of disruption/ disaster.*
- *To ensure compliance to RBI guidelines on BCP and follow best industry practices on BCM.*
- *To enhance Bank's reputation and brand value.*

- ***Data Centre and Disaster Recovery Site***
- *The Bank has established a* ***"State of art" Data Centre*** *at Belapur, Navi Mumbai and* ***Disaster Recovery (DR)*** *Site at Chennai and a* ***near DR Site at BKC, Mumbai*** *to provide : uninterrupted technology support to Bank's critical Operations.*
- ***In case of failure of Data Centre-Belapur****, the* ***Bank will switch over to DR site- Chennai*** *to continue its critical operations.*

- ***Business Continuity Plan (BCP) & Disaster Management Plan (DMP)***
- *In accordance with BCM Policy, the* ***Bank has prepared BCP & DMP to facilitate*** *the continuity of critical business processes in the event of various disaster scenarios which includes process* ***disruptions, technology break down, natural calamities, fire, riots*** *etc.*
- ***Regulatory Reporting***
- *The Bank is subjected to regulation by the Reserve Bank of India (RBI). As per regulatory requirement, the* ***Bank reports instances of major failures faced by the Bank, customer segment/ services impacted due to failures and corrective steps taken to avoid such failures in future.***
-

Updates & Review

- ***Updates and Annual Review***
- *The Bank shall update its BCM Policy whenever there is a material change to its operations, structure, business or location.*
- *In addition, the BCP of various functions shall be reviewed annually to incorporate changes in its operations, structure, business, or locations.*
- **Contacting Us**
- *If during or after any disruption/ disaster, the customers are unable to contact our affected branches/ units, please contact our 24 hours Customers Care Help lines:*
- ***1800-22-1070 , 1800-200-1947***

SEBI Circular

- ***CIRCULAR***
- ***SEBI/HO/MRD/DMS1/CIR/P/2019/43 March 26, 2019***
- *To,*
- ***All Stock Exchanges, All Depositories,***
- ***All Clearing Corporations***
- *Dear Sir/ Madam,*
- ***Guidelines for Business Continuity Plan (BCP) and Disaster Recovery (DR) of Market Infrastructure Institutions (MIIs)***

1. *SEBI vide circular CIR/MRD/DMS/12/2012 dated April 13, 2012 and CIR/MRD/DMS/17/2012 dated June 22, 2012* ***prescribed framework for Business Continuity Plan (BCP) and Disaster Recovery Site (DRS)*** *for stock exchanges and depositories.*
2. *With the advancement in technology and improved automation of processes in terms of transitioning time, wherein the operations can be moved from the* ***Primary Data Centre (PDC) to the DRS****, it was felt that the extant* ***framework needs to be re- examined.***
3. *Considering the fact that clearing corporations are systemically important infrastructure institutions, it has been decided that framework on* ***BCP and DR shall also be made applicable to all the clearing corporations.***

- *4. The stock exchanges, clearing corporations and depositories* ***(collectively referred as Market Infrastructure Institutions – MIIs) should have in place BCP and DRS so as to maintain data and transaction integrity.***
- *5. Apart from DRS, stock exchanges and clearing corporations should* ***also have a Near Site (NS) to ensure zero data loss*** *whereas, the depositories should also ensure zero data loss by adopting a suitable mechanism.*
- *6. The DRS should preferably* ***be set up in different seismic zones*** *and in case due to certain reasons such as operational constraints, change of seismic zones, etc.,* ***minimum distance of 500 kilometer shall be ensured between PDC and DRS so that both DRS and PDC are not affected by the same disaster.***
- *7. The manpower deployed at DRS /NS should have* ***same expertise as available at PDC in terms of knowledge/ awareness of various technological and procedural systems*** *and processes relating to all operations such that DRS /NS can function at short notice, independently. MIIs should have* ***sufficient number of trained staff at their DRS*** *so as to have the capability of running live operations from DRS without involving staff of the primary site.*
- *8. MIIs should endeavor to develop systems that do not require configuration changes at the end of trading members/ clearing members/ depository participants for switchover from the PDC to DRS. Further,* ***MIIs should test such switchover functionality by conducting unannounced 2 day live trading session from its DRS****. This would help to gauge the state of readiness of various other processes and procedure relating to business continuity and disaster recovery that may not get tested in a planned exercise.*
- ***9. MIIs shall have Recovery Time Objective (RTO) and Recovery Point Objective (RPO) of not more than 4 hours and 30 minutes, respectively***

- *10. The time taken to define/ establish/ declare a disaster* ***should not be more than 2 hours and the total RTO including the time taken to declare an incident as disaster should not be more than 4 hours****. Further, RTO shall be calculated* ***from the occurrence of disaster*** *and not from the time an incident is declared a disaster.*
- *11. Solution architecture of PDC and DRS / NS* ***should ensure high availability, fault tolerance, no single point of failure, zero data loss, and data and transaction integrity.***
- *12. The BCP – DR policy of stock exchanges, clearing corporations and depositories should be* ***well documented covering all areas*** *as mentioned above including disaster escalation hierarchy.*
- *13. The policy document and subsequent changes / additions / deletions should be* ***approved by Governing Board of the stock exchanges / clearing corporations/ depositories and thereafter communicated to SEBI****.*
- ***DR drills/Testing***
- ***14. DR drills should be conducted on a quarterly basis****. In case of exchanges and clearing corporations, these drills should be* ***closer to real life scenario (trading days****) with minimal notice to DR staff involved*
- *15. The drill should include running all operations from* ***DRS for at least 1 full trading day****.*
- *16. The* ***results and observations of these drills should be documented*** *and placed before the Governing Board of stock exchanges /clearing corporations/ depositories. Subsequently, the same along with the comments of the Governing Board should be forwarded to SEBI within a month of the DR drill.*

System Audit – MII

- *The system auditor while covering the BCP – DR as a part of mandated annual system audit* ***should check the preparedness of the MII to shift its operations from PDC to DRS unannounced*** *and also comment on* ***documented results and observations of DR drills***
- ***IS Auditor to review*** *:*
- *1.* ***MII documented Root Cause Analysis (RCA)*** *of their technical/ system related problems in order to identify the causes and to prevent reoccurrence of similar problems.*
- *2. Stock exchanges and clearing corporations* ***shall include a scenario of intraday shifting from PDC to DR*** *during the mock trading sessions in order to demonstrate its preparedness to meet RTO/RPO as stipulated above.*
- *3.* ***'Live' trading sessions*** *from DR site shall be scheduled* ***for at least 2 consecutive days in every 6 months****. Such live trading sessions from the DRS shall be organized on normal working days*

“The pessimist sees difficulty in every opportunity.

The optimist sees opportunity in every difficulty”

- Winston Churchill

Thank You