Business Continuity & Disaster Recovery

(Chapter - 3 : DISSA Course)

Arijit Chakraborty

June 12 , 2021

BC DR Templates
IS Auditor / BCDR Auditor review points

- **BCP Policy Document Control**

STAFF MEMBER	DATE APPROVED	SIGNATURE

Version Control

VERSION	DATE	AMENDMENTS	DETAILS	AMENDED BY
1.0		Initial Document	BCP & DR Plan	

DRP Contacts

	COMPANY	LANDLINE	MOBILE
Company Officer			
Other contacts			

Document Change Table

Change Number	Section	Date of Change	Individual Making Change	Description of Change

Document Transmittal Record

Date of Delivery	Number of Copies Delivered	Method of Delivery	Name, Title, and Organization of Receiver

Partial continuity personnel roster

Function	Title/ Position	Name	Telephone Numbers	Additional Information
Function #1: Approve and oversee cleanup of contaminated sites.	Division Head, Enforcement and Remediation Division **Alternate:** Deputy Division Head, Enforcement and Remediation Division	Abhijit Khanna Joseph Rodriques	Home: (###) ###- Work: (###) ###-#### Cell: (###) ###- Home: (###) ###-#### Work: (###) ###- Cell: (###) ###-	
	Chief, Enforcement Branch **Alternate:** Deputy Chief, Enforcement Branch	Nitai Sasmal Shreya Mishra	Home: (###) ###- Work: (###) ###- Cell: (###) ###- Home: (###) ###-#### Work: (###) ###- Cell: (###) ###-	

Corrective Action Program

Capability	Observation	Recommendation	Corrective Action	Capability Element	Primary Responsible Office	Organization POC	Start Date	End Date
Planning		.						

DRP Recovery Ranking

Priority Rank:	Organization Process:	Potential Impact:	Allowable Downtime:
1			
2			
3			

Recovery steps – SOP

Recovery Steps:

The following are the recovery tasks to be followed:

1. Retrieve important items form work area
2. Evacuate building
3. Go to primary staging area
4. Wait for all clear or activation notice
5. Go to designated recovery location
6. Execute calling tree
7. ______________________________
8.

Call & Records management

Calling List:

You are responsible for calling the following employees and/or companies:

1. ____

2. ____

3.

Vital Records:

The following documents and/or electronic media will be required for your recovery effort:

1. ____

2. ____

3. ____

MS service

- ***Microsoft's cloud [Azure] in 58 regions worldwide.***
- ***ISO/IEC 27001:2013 storage***
- currently support **over 1000 cloud destinations** & regions.

Hardware installation at DR

1. **Servers**
2. **Storage and Backup**
3. **Networking**

✓Router

✓Management Switch

✓Server Load Balancer

✓Link Load Balancer

Hardware

- **4. Security**

✓ Web proxy

✓ Firewall(External)

✓ Firewall(Internal)

✓ Network IPS

✓ Security Information and Event Management (SIEM) - *Real-time visibility across organization's IS systems & Event log management*

✓ Anti –Virus

✓ Email Anti-spam solution

✓ Anti- Advance Persistent Threat

✓ VA & PT by own tool of BCP agent

DR – MIS & Reporting

- **A. Daily reports**
- ▯ Summary of issues / complaints logged at Technical Support desk
- ▯ Summary of resolved, unresolved & escalated issues / complaints
- ▯ Summary of resolved, unresolved & escalated issues / complaints to vendors.
- ▯ Log of backup and restoration undertaken.

- **B. Weekly Reports**
- Issues / Complaints Analysis report for virus calls, call trend, call history,
- Summary of systems rebooted.
- Summary of issues / complaints logged with OEMs.
- Inventory of spare parts in DR site.
- **Summary of changes undertaken in DR site :**

✓ configuration changes,

✓ patch upgrades,

✓ database reorganization,

✓ storage reorganization, etc.

- **Minor changes like:**

✓ volume expansion,

✓ user creation,

✓ user password reset, etc

- **C. Monthly reports**
- **Component wise ICT infrastructure availability** and resource utilization.
- **Consolidated SLA / (non)-conformance report.**
- Summary of component wise **Data Centre uptime**.
- Summary of **changes in DR site.**
- Log of **preventive / scheduled maintenance** undertaken
- Log of **break-fix maintenance** undertaken
- Summary of attendance of DR Consultant’s staff at DR site.

- **D. Quarterly Reports**
- Consolidated component-wise ICT infrastructure availability & resource utilization.
-
- **E. Half-yearly Reports**
- DR Security Audit Report
- ICT infrastructure Upgrade / Obsolescence Report

BCP Technology solutions

- **Intelligent Business Continuity**
- Instant **On-site & Off-site** Virtualization
- Advanced **Screenshot Backup Verification**
- **Time-based or Infinite** Cloud Retention
- Identification of File or Application Changes between any 2 backup points
- **Ransomware** Detection

3 Tier RPTO Model – BCP

- **Tier-1: Mission-critical** applications that require RTPO of < 15 minutes
- **Tier-2: Business-critical** applications that require **RTO of 2 hours & RPO of 4 hours**
- **Tier-3:** Non-critical applications that require **RTO of 4 hours & RPO of 24 hours**

Granular Recovery Technology (GRT)

- **Granular data :** detailed data, lowest level data can be in target set
- GRT use : restore certain individual items from backup sets.
- Ex: use Agent for Microsoft Exchange Server to restore **email message** from backup without restore of entire mailbox.
- GRT feature must be enabled for backup

Toulouse Satellite Operations Center (SOC) - Case

- Toulouse Satellite Operations Center (TSOC)- Airbus
- TSOC = responsible for ensuring positioning & monitoring of fleet of telecom satellites, comprising 60 satellites
- TSOC = Operates on behalf of leading international operators in mobile, internet, television & radio telecom services sector.
- Piloting of satellites = lifespan ranges from 15 to 25 years, from launch & early orbit phase (LEOP) to their supervision, after its in position
- Mission –critical data CIA requirement

TSOC Ops & DRaaS App

- TSOC stores = equivalent of > 600 years of telemetry data history
- Daily collection & analysis of data :

❑ satellite's life

❑ from assembly to de-orbit.

Data, transmitted 24 hours * 7, = health of satellites, TSOC anticipate

- possible component failures.
- to identify trends in satellite performance
- improvement - Satellite design & manufacturing.
- **DRaaS :**

✓ Handles **550 VMs & 25TB** of telemetry data

✓ 1 TB = 1,000 GB or 10,00,000 MB

✓ **High-speed RTO reduced from 12 hours to 20 minutes**

DR Case study ; Hyundai Korea & IBM

- Summer of 2016, earthquakes shook South Korean cities
- Hyundai Heavy Industry (HHI) quickly realized how a disaster like earthquakes could seriously damage Hyundai’s mission-critical IT infrastructure.
- HHI IT leadership collaborated : IBM Business Resiliency Services to develop & implement DR solution with remote data center.
- HHI HQ : wide range of intelligence - information systems to design blueprints.
- Vital for HHI : data centers remain undisturbed & fully functional, enable HHI to continually work with 15 corporations, 24x7.
- HHI was able to implement and administer DR Blueprint in 5 months.
- HHI could monitor and prevent shutdowns & serious disruptions.

Implementation Steps

HHI performed :

- current state assessment,
- thorough BIA,
- sorting mission-critical elements
- systems that support the whole business.
- test its DR systems and centers and
- determine that DR center was stable and resilient.

BC DR IS Audit Checklists

1. Emergency Calling Directory
2. Emergency Relocation Team Checklist and Essential Functions Checklist
3. Continuity Site Acquisition Checklist
4. Emergency Operating Records and IT Checklist
5. Emergency Equipment Checklist
6. Delegations of Authority
7. Maps and directions to continuity facility & seating chart of the facility
8. **TT&E** (Test , Training, and Exercise) checklist
9. **ERG (**Emergency Relocation Group) Checklist

IS Audit : IT BCDR Mitigation Process

Integrated BCDR Platform executes
IT BCDR via following steps:

1. Threat Occurs
2. Systems Affected
3. Infrastructure and Applications Impact Identified and Input into the SIB Platform
4. Based on Pre-assessed RTO & RPO values Applications and relevant Recovery Procedures are Identified and Prioritized
5. Teams are notified of the IT Recovery Procedures.
6. Recovery Procedures of the affected functions and applications are carried out by the team members
7. Once Tasks are completed Platform is updated
8. Systems Restored
9. Threat status updated
10. Report Generated

ISO 22301

ISO 22301 = international standard for Business Continuity Management (BCM).

Published by the International Organization for Standardization,

ISO 22301 to help **organizations prevent, prepare for, respond to** and **recover from unexpected and disruptive incidents.**

Standard provides a practical framework for **setting up and managing** an effective BCMS.

ISO 22301 aims to safeguard an organization from a wide range of potential threats and disruptions.

RELATIONSHIP WITH ISO 22301

- **ISO 22301:2019** has replaced **ISO 22301:2012,** which was developed based on British standard BS 25999-2.
- This 2019 revision brings **more flexibility and less prescriptiveness**, adding more value to organizations & customers.
- The main focus/philosophy of ISO 22301 is based **on analyzing impacts and managing risks:**
- ***find out which activities are more important and which risks can affect them, and then systematically treat those risks.***
- The strategies and solutions to be implemented usually in form of :

✓ policies,

✓ procedures, and

✓ technical/physical implementation (e.g., facilities, software, and equipment).

BUSINESS CONTINUITY PLANNING

- According to ISO 22301, BCP = *“documented procedures that guide organizations to respond, recover, resume, and restore to a pre-defined level of operation following disruption.”*
- It specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure your business recovers from disruptive incidents.

ISO 22301 :10 Clauses

- 1. Scope
- 2.Normative references
- 3. Terms & definitions
- 4. Context of Organisation
- 5. Leadership
- 6.Planning
- 7.Support
- 8. Operation
- 9.Performance evaluation
- 10.Improvement

ISO 22301 : Implementation checklist

1. Get **commitment and support** from senior management.
2. Engage **whole business** with good internal communication.
3. **Compare existing BCMS** with ISO 22301 requirements.
4. Get **customer and supplier feedback** on current BCMS
5. Establish an **implementation team** to get the best results.
6. Map out and share **roles, responsibilities and timescales**.
7. Adapt **basic principles of the ISO 22301** standard to business.
8. **Motivate staff involvement** with training and incentives.
9. **Share ISO 22301 knowledge** and encourage staff **to train as internal auditors.**
10. Regularly **review ISO 22301 system** to make sure it remains effective and you are continually improving it.

ISO Case study : midcap company in Mumbai
Link failure

- maintain redundancy for every connectivity link with auto failover switching.
- IT team would ensure that link performance & link utilization monitored.
- All details of uptime and downtime consolidated & shown in regular report, which can later facilitate follow-up actions.
- **Hardware / Software failure**
- All infrastructure at primary data center is commissioned in high availability mode or auto failure switching.

- **Virus infection**
- Use best-in-class Antivirus solution to prevent situation from occurring.
- In case of virus outbreak quarantine entire system & up standby system.
- **Natural Calamities**
- Premise situated at higher altitude in Western coast of India which **is low seismic and non-flooding zone.**
- In case of major disaster, operation can be move to DR site
- **Fire accidents**
- Premise equipped with state-of-the-art integrated building management system which gives advance alert for any disaster like fire and any other disaster.

- **Vandalism**
- Main entrance of premises protected 24/7 by physical security
- under electronic surveillance.
- Entry to rest of premises is restricted by access control system.
- Only employees & authorized support group personnel provided access into premises

Catastrophic events

- In the case of Catastrophic events such as:

✓ • Floods

✓ • Earthquakes

✓ • Storms

✓ • Acts of terrorism

✓ • Accidents or sabotage

IRDAI

- **Circular**
- **Ref. No:**IRDAI/INSP/CIR/MISC/077/03/2020
- **Date:**30-03-2020
- *Insurance Regulatory and Development Authority of India*
- *Ref: IRDAI/INSP/CIR/MISC/077/03/2020 Date: 30th March 2020*
- *To*
- *All Insurers*

- ***C. Monitoring of the situation:***
- *6. Insurers shall put in place a **Business Continuity Plan (BCP) which inter alia deals with processes, transactions, reporting and customer services to be handled in a seamless manner to take care of the present situation.** A copy of the same may be submitted to the Authority.*
- *7. Insurers shall set up a **Crisis Management Committee**, comprising of key personnel to monitor the current situation on real time basis and to take appropriate timely decisions on :*
- *a. Issues pertaining to safety of staff, policyholders, intermediaries ,agents;*
- *b. Assessing new challenges that may emerge on a day-to-day basis and measures to mitigate them; and*
- *c. Adopting necessary measures to minimize business disruption.*
- *Further, the Crisis Management Committee **should provide regular inputs to the Risk Management Committee of the insurer.***

- *9. **Cyber risks and data security**: Due to enhanced remote working, it is possible that there could be an increase in the number of cyber-attacks on personal computer networks.*
- *Therefore**, insurers need to take precautionary measures to address such cyber risks and to mitigate such risks as soon as they are identified.***
- *Insurers shall also **educate their staff, through emails and other modes, of possible cyber risks** and the associated safeguards **to be taken by the staff while working from home.***

- ***Information System Audit Guidelines***
- ***23.1 Eligibility & Selection of Auditor:***
- ***Independent Assurance Audit shall be carried out by qualified external systems Auditor holding certifications like CISA/ DISA/Cert-in empaneled Auditor***
- *Annual IS Audits should also cover* ***branches on sample basis, with focus on large and medium branches****, in critical areas like :*

✓ *password controls,*

✓ *control of user ids,*

✓ *operating system security,*

✓ *anti-malware controls, maker-checker controls,*

✓ *Identity & Access management,*

✓ *physical security,*

✓ *review of exception reports/audit trails,*

✓ *BCP policy and testing etc.*

- ***Frequency:***
- *Audit shall be carried out* ***for every financial year***
- ***Executing IS Audit***
- *During audit, auditors should :*

❑*obtain evidences,*

❑*perform test procedures,*

❑*appropriately document the findings,*

❑*and conclude a report.*

- ***Reporting and Follow-up actions***
- *a. There should be **proper reporting of the findings of the auditors**.*
- *For this purpose, each Organization should prepare a structured format.*
- *b. **The major deficiencies/aberrations noticed during audit should be highlighted in a special note and given immediately** to IT Department.*
- *c. **Minor irregularities pointed out by the auditors** are to be rectified immediately.*
- *d. **Follow-up action on the audit reports should be given high priority** and **rectification should be done without any loss of time.***
- *e. **Audit reports need to be presented to the Risk Management** Committee of the Board.*
- *f. A copy of **executive summary of the Audit report along with action taken note should be submitted to IRDAI within 30 days** of completion of Audit*

- ***Review***
- *Organization is advised to:*
- *a. **Review the selection and performance** of auditor.*
- *b. Ensure that the **work of auditors is properly documented**.*
- *c. Be responsible for the **follow-up on audit reports** and the presentation of the quarterly review*
- *d. **Rotation of Auditors**: Once in three years*

SBI Muscat – BCP

- **Business Continuity Plan and DR Site**
- *State Bank of India has a Business Continuity Plan (B.C.P.) duly approved.*
  It also has a Disaster Recovery Site at KOM (Knowledge Oasis Muscat) which is activated in case of need.
  The BCP Testing is done on Half Yearly Basis.
  The Last such Testing was done on 31.12.2020.
- **RESOURCE PERSONS:**
  CHIEF MANAGER(CREDIT)
  CHIEF MANAGER(CLIENT SERVICES)
  MANAGER (OPERATIONS)
  DEPUTY MANAGER (IT)

BPCL: Annual ERM Report

- **Infrastructure Risk**

Some of the identified infrastructure risks are:

1. *High Import dependency for LPG (50%) and lack of adequate infrastructure facilities leading to higher costs.*
2. *Lack of facilities at new airport in Navi Mumbai may lead to loss of future business.*
3. *Non Completion of Minimum Work Programme (MWP) for gas business.*
4. ***Inadequate BCP process may lead to organization’s inability to resume normal business operations from DR) site as per SLA.***

Tata Capital Annual Report FY 19-20

- *In order to address the risk associated with COVID 19 and to seamlessly carry out normal operations, the Group immediately **activated its Business Continuity Plan (BCP).***
- *The IT Team had taken the ownership of driving BCP strategy for the Company, **as required by the RBI** and has successfully completed the **BCP annual drill** along with providing support during the country-wide COVID-19 lockdown.*

Arijit Chakraborty