
Business Continuity & Disaster Recovery

(Chapter - 3 : DISSA Course)

Arijit Chakraborty
Feb12 , 2022

Phase I

- **Risk Analysis**

- 1. 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**

- 2. Vital

- Functions can be performed **manually but only for brief** period
 - **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

Phase I

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

Business Continuity Plan

- **Insurance**
 - **Business Interruption**
 - Covers loss of net profit caused by computer media damage
 - **Valuable Paper and Records**
 - Covers actual cash value papers and records
 - **Errors and Omissions**
 - Provides legal liability protection where professional practitioner commits an act, error /omissions results in financial loss to a client
 - **Fidelity Coverage**
 - Covers loss from dishonest/ fraudulent employees
 - **Media Transportation**
 - Provides coverage for potential loss or damage to media in transit to off-premises IPF

Phase III **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**
- **Reciprocal agreement**
 - Contract with hot, warm or cold site
 - Procuring alternative hardware facilities

Phase III- types of Alternate Sites

- **Hot sites**

- Fully configured & ready to operate within several hours
- Equipment & systems software must be compatible with the primary installation being backed up
- Costs associated with use of 3rd-party hot site usually high
- Often cost justifiable for critical applications
- Intended for emergency operations of a limited time period & not for long-term extended use

Phase III

- Warm Sites
 - Partially configured
 - With network connections & selected peripheral equipment, = disk drives, tape drives & controllers, but without main computer
- Cold Sites
 - Basic environment to operate IPF
 - Ready to receive equipment but does not offer any components at site in advance of the need

Internal Audit role in BCP review -IIA Guidelines

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

Business Continuity Management

- 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?

Testing BCP & DRP

- 5 levels of testing
 - Document review
 - Walkthrough
 - Simulation
 - Parallel test
 - Cutover test

ISO 22301 - 2019

- ISO 22301 specifies requirements to implement, maintain and improve a management system to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise.
- The requirements specified are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization.
- The extent of application of these requirements depends on the organization's operating environment and complexity.
- ISO22301 applicable to all types and sizes of organizations that:
 - a) implement, maintain and improve a BCMS;
 - b) seek to ensure conformity with stated business continuity policy;
 - c) need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption;
 - d) seek to enhance their resilience through effective application of BCMS.

Main clauses

- — Clause 4 introduces requirements necessary to establish context of BCMS applicable to the organization, as well as needs, requirements and scope.
- — Clause 5 summarizes requirements specific to top management's role in BCMS, and how leadership articulates its expectations via a policy statement.
- — Clause 6 describes the requirements for establishing strategic objectives and guiding principles for the BCMS as a whole.
- — Clause 7 supports BCMS operations related to establishing competence & communication on a recurring/as-needed basis with interested parties, while documenting, controlling, maintaining & retaining required documentation
- — Clause 8 defines BC needs, determines how to address them and develops procedures to manage the organization during a disruption.
- — Clause 9 summarizes requirements necessary to measure BC performance, BCMS conformity, and to conduct management review.
- — Clause 10 identifies and acts on BCMS nonconformity and continual improvement through corrective action.

Vulnerability Atlas of India (VAI) -

- VAI = comprehensive document provides existing hazard scenario for entire country
- ✓ digitized State/UT- wise hazard,
- ✓ maps with respect to earthquakes,
- ✓ winds and floods for district-wise identification of vulnerable areas
- ✓ additional digitized maps for thunderstorms, cyclone and landslides.
- **Purpose**
 - use for disaster preparedness and mitigation at policy planning & project formulation stage.
 - one of its kind single point source for the various stakeholders - policy makers, administration, municipal commissioners, urban managers, engineers, architects, planners, public etc. to ascertain proneness of any city/location/site to multi-hazard which includes earthquakes, wind, floods, thunderstorms, cyclones and landslides.