# Business Continuity Planning

There are five BCP test types, which are graded according to ease of implementation from easy to difficult:

1. Checklist
2. Structured walk-through
3. Simulation
4. Parallel
5. Full interruption

## Backups

* The archive bit is set when a file is modified, and reset by a full or incremental backup.
* **Full backups**: a complete copy of storage device, clear archive bit
* **incremental backups**: only copy those files that have changed since last full or incremental backup (archive bit=1), clear archive bit
* **differential backups:** incremental backup but do not clear archive bit.

## BCP

* Business continuity planning: assessment of a variety of risks, creation of policies, plans and procedures to minimize the impact of the risks on organization
* BCP: restore normal activity in the event of a minor disaster, business continuity of mission critical service is not lost
* BCP even is less disastrous than a DRP disaster Recovery Planning event

### BCP process has four elements

* 1. Project scope and planning
  2. Business impact assessment (BIA)
  3. Continuity planning
  4. Approval and implementation

### Project scope and planning

* perform business organization analysis to identify depts who have a stake in BCP, e.g. operational depts, critical support services, senior executives
* BCP team selection should include at a minimum
  + reps from each of the org’s depts for core services
  + reps from key support depts
  + IT reps with technical expertise in areas covered by BCP
  + Security reps with knowledge of BCP process
  + Legal reps familiar with legal, contractual, and regulatory responsibilities
  + reps from senior management
* resource requirements required by 3 different BCP stages:
  1. **BCP development** will require resources for the four elements, major one will be manpower by members of the BCP team
  2. **BCP testing, training, and maintenance** will require some hardware and software commitments, and manpower
  3. **BCP implementation**, when a disaster strikes large amounts of manpower and resources will be required
* legal and regulatory requirements – officers and directors of publicly traded firms have a responsibility to exercise due diligence in execution of their business continuity duties
* in many countries, banks and financial institutions are required to provide continued operation to ensure viability of the national economy
* service level agreements (SLA), essential to include legal counsel in BCP process

### Business Impact Assessment

* there are 5 steps in a BIA:

1. **identification of priorities**, identifies the critical resources and threats posed, the likelihood that each will occur, and impact on the business. Quantitative: calculate asset value AV, maximum tolerable downtime MTB, or recovery time objective RTO.
2. **risk identification**, both natural and manmade, this is purely qualitative in nature. At this stage, not interested with calculating rist.
3. **likelihood assessment**, a comprehensive list of threats to the organization, and identify the likelihood that each risk will occur. Calculate the annualized rate of occurrence ARO for each risk in the previous section
4. **impact assessment**, the exposure factor EF is the amount of risk expressed as a % of assets value, single loss expectancy SLE=AV\*EF monetary loss expected each time, and annualized loss expectance ALE = ARO\*SLE. Qualitative: consider loss of goodwill, loss of employees, social / ethical responsibilities to the community, negative publicity
5. **resource prioritization**, take the list of all risks from BIA process and sort in descending order according to ALE computed in impact assessment. Output: a prioritized list of risks to address.

* decision making can be qualitative or quantitative

### Continuity Planning

* **strategy development stage:** take the prioritized list of concerns raised by the quantitative and qualitative analysis, and determine which risks will be addressed
* look at MTD to determine which risks are deemed acceptable and which must be mitigated.
* four responses to risk: reduce, assign, accept, and reject. Ignore is not an acceptable response.
* **provisions and processes**: BCP team designs procedures and mechanisms that will mitigate the risks deemed unacceptable during strategy development stage. 3 categories of assets to be protected

1. **people**: ensure the people in your org are safe
2. **buildings/facilities**: office facilities, manufacturing plants, warehouses, etc. Hardening provisions: patch a leaky roof, install reinforced hurricane shutters. Alternate sites: introduce redundancy, hot / cold / warm sites.
3. **Infrastructure**: a critical part of the infrastructure for many businesses is the IT communication and computer systems. Hardening system: introduce protective measures, computer-safe fire suppression systems and uninterruptible power supplies. Alternative systems: introduce redundancy, redundant components or redundant systems, communications links.

### Approval and Implementation

* have the plan approved by CEO or equivalent top management
* demonstrates importance of plan to the whole organization
* **plan implementation**: develop an implementation schedule, use the resources dedicated to the program.
* supervise a BCP maintenance program so plan is responsive to evolving business needs
* **training and education**: all personnel involved in the plan should receive training on the overall plan and their responsibilities
* at least one backup person for each BCP task.

## BCP Documentation

Commit the BCP to paper

* ensure the BCP personnel have a written continuity document to refer to
* provide a historical record of the BCP process
* force team members to commit thoughts to paper, facilitates fault finding in the BCP

**Documentation should contain**

* Continuity Planning Goals
* Statement Of Importance
* Statement Of Priorities
* Statement Of Organizational Responsibility
* Statement Of Urgency And Timing
* Risk Assessment
* Risk Acceptance / Mitigation
* Vital Records Program
* Emergency Response Guidelines

## Maintenance

* team should meet periodically to discuss the plan, review plan tests to ensure it meets org needs
* older versions of the BCP should be physically destroyed and replaced by most current version

# Disaster Recover Planning

* Natural disasters: earthquakes, floods, storms, fires, other regional events
* Man-Made disasters: fires, bombings / explosions, acts of terrorism, power outages, other utility and infrastructure failures, hardware / software failures, strikes, vandalism / theft,

### Recovery strategy

**Alternate Processing Sites**

**Cold sites**

* standby facilities large enough to handle processing load with electrical and environmental support systems
* no computing facilities, no broadband
* advantage: cheap. disadvantage: long time to activate the site and ready to support business operations

**Hot site**

* backup facility is maintained in constant working order, a facilities mirror
* if data is not instantaneously updated, DR managers may force replication before the transition, hand-carry backup tapes and manually apply the changes, or simply accept the loss of a portion of data
* quick to return to business, but expensive to maintain

**Warm sites**

## RAID

* RAID on an OS is a software implementation, may also be a hardware implementation
* Redundant Array of Independent Disks
* Hot swap: remove faulty disk without stopping system
* Cold swap: server must be fully powered down
* Warm swap: software stop, replace disk, restart SW

|  |  |
| --- | --- |
| 0 | Striping |
| 1 | Mirroring |
| 2 | Hamming code parity |
| 3 | Byte-level parity |
| 4 | Block-level parity |
| 5 | Interleave parity |
| 6 | Second parity data |
| 10 | RAID levels 1 + 0 |
| 15 | RAID levels 1 + 5 |