# Business Continuity Management Guidelines

Business continuity Management (BCM) is a planning and management discipline through which organizations design, implement and maintain measures, plans and strategies which are effective to manage crisis, respond to/ recover from a disaster; This start with an identification of potential threats and vulnerabilities as well as impacts that recognized threats might cause to business operations.


- Introduction
- Business Continuity (BC) And Disaster Recovery (DR)
- Business Continuity Management (BCM) Lifecycle
- Mainly Confronted Disasters in Rwanda and Management
- IT- Disaster Recovery for a Business Continuity
- Guidance for a True IT - Disaster Recovery

# Introduction

**Business continuity Management (BCM)** is a planning and management discipline through which organizations design, implement and maintain measures, plans and strategies which are effective to manage crisis, respond to/ recover from a disaster; This start with an identification of potential threats and vulnerabilities as well as impacts that recognized threats might cause to business operations.

A successful application of Business Continuity plan increases business resilience and efficiency, which, in turn contribute to a higher performance and takes an organization at a level it can control and continue to run its operations during and after a disaster situation.

**INCIDENT AND DISASTER**

Incident is a situation that could lead to an interruption, loss, crisis; while a disaster is a sudden unplanned event that causes significant damage or serious loss to a business. Therefore, BC - DR Plan is more than a just document to be stored aware and never review or consult again, it is a step by step guide to be followed before, during and after a disaster situation which should be reviewed and updated whenever there is a significant change in an organization's operating system.

***BUSINESS CONTINUITY ASKS QUESTIONS***

- Is your business ready to face unplanned disaster situations?
- If there is an interruption to a regular business processes, what is needed to keep a business up and running well? (Look at everything, IT and beyond)

# Business Continuity (BC) And Disaster Recovery (DR)

BC includes DR and DR requires guidance from BC, to direct priorities and set scope.

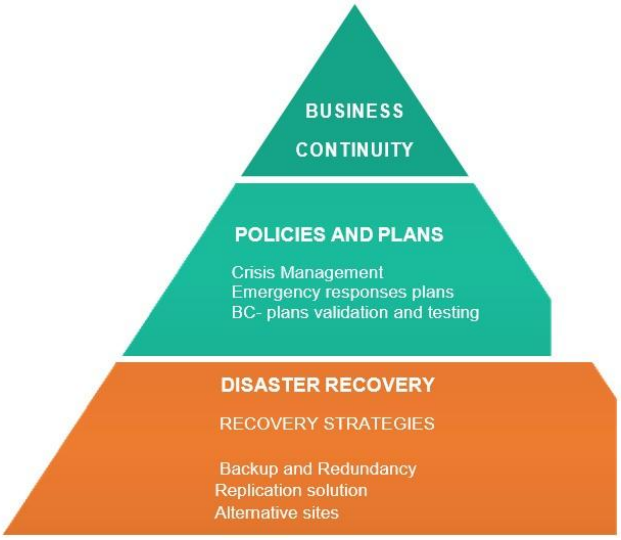



*Figure 1: Business continuity and Disaster recovery*

| BUSINESS CONTINUITY (BC) | DISASTER RECOVERY(DR) |
|---|---|
| **OBJECTIVE:** Build resilience | **OBJECTIVE:** Build technological recovery tactics |
| **FOCUS:** Return business operations at an acceptable predefined level / normal | **FOCUS:** Recover Data/Systems |
| **SOLUTION:** - Planning<br>- Building or rehabilitation | **SOLUTION**: - Active- Active sites<br>- Alternative options |

# Business Continuity Management (BCM) Lifecycle

Business continuity management (BCM) is centred around a BCM lifecycle that consists of following phases:

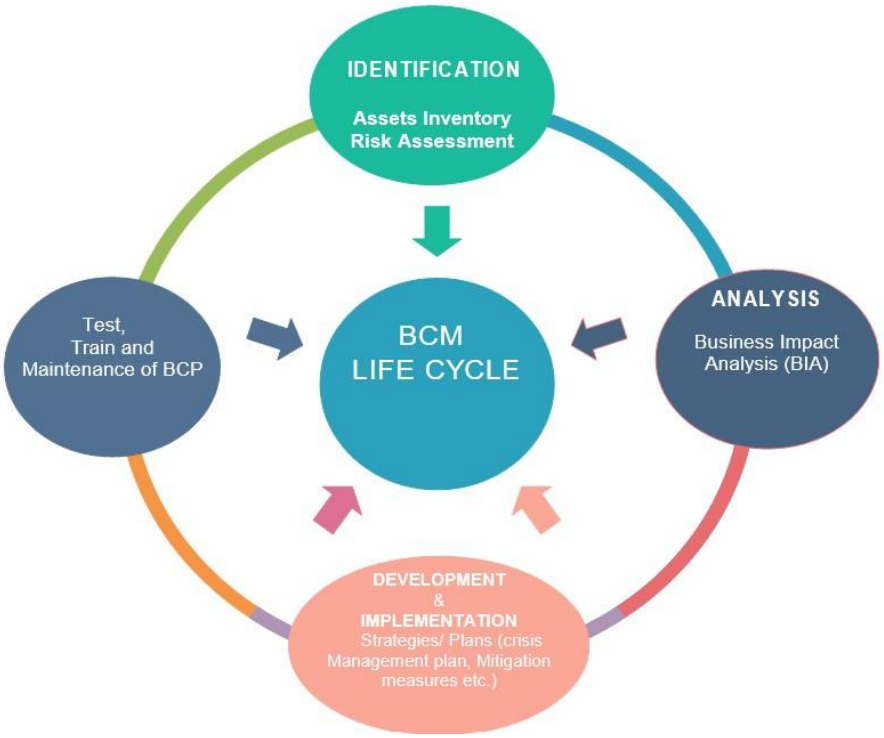



*Figure 2: Business Continuity Management Lifecycle*

## Identification: Assets Inventory And Risk Assessment

This phase is a starting point of BCM which allows an easy recognition of critical assets, categorization and prioritization based on criticality level.

- **Assets inventory**: consists of tracking, recording and managing all assets such as: (Infrastructure, systems, In-house software, Data, licenses, Company- owned equipment etc.).
- **Risk Assessment**: Consists of identifying and evaluating internal and external threats and vulnerabilities (risks), the likelihood, a control methods in place or required as well as the cost for such control.

## Analysis: Business Impact Analysis (BIA)

**BIA**: is a fundamental phase from which a whole BCM process is built on; its central mission is to figure out which functions, systems and processes that are critical to an organization’s ongoing success, for a special management and protection.
BIA should be done as follows:

- **Analyzing damage or outage impact**: We do not only analyze a damage or outage impact and severity, but  also a  chronological sequence, looking at operational level, service level and financial level etc.
- **Prioritizing**: classification of functions/systems based on criticality level.
- **Recovery parameters measurement**: based on system criticality and chronological sequence of damaging events, a maximum tolerable period (**MTP**) of disruption, recovery time objective (**RTO**), and recovery point Objective (**RPO**) for each business function should be specified. For critical systems **RTO** and **RPO** should be minimized to zero.
- **Determining required resources**: Facilities, solutions and technologies that are needed for normal and emergency operation should be well defined.

# Development and Implementation of Strategies - Plans

This phase consists of developing and implementing plans and strategies to follow in an immediate wake of an incident until damaged processes are fully restored.

**Crisis Management Plan**

Crisis management plan should contain:

- Crisis management structure (team with specific responsibilities): comprises of company’s President/CEO, heads of departments, technical team as well as vendors and external entities.
- A call tree to facilitate a quick and secure communication.
- HR and other facilities such as evacuation, alternative options. Etc.

**Crisis Management Steps**

Following crisis management steps are actions to be taken in the face of a major risks or crisis to allow a business to survive any crisis.

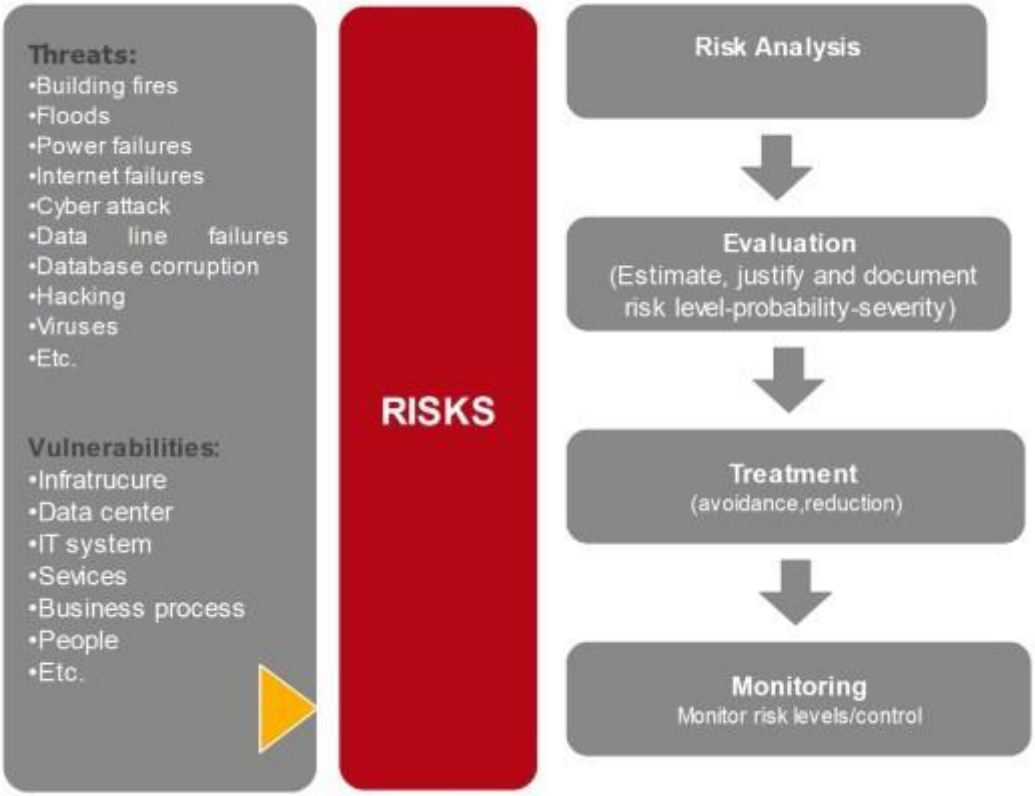



*Figure 3: Crisis Management Steps*

**A. RISK ANALYSIS:** consists of analyzing risk impact, likelihood and the effectiveness of countermeasures or control method in place.

**B. RISK EVALUATION:** This step consist of estimating, justifying, classifying and documenting risk severity level (Major, moderate or minor), risks that are internal - external, Risks with a direct - indirect effect.

**C. RISK TREATMENT** Following risk treatment options could be selected reliant on risk type:

- **Assuming risk:** This simply means that a risk is accepted; this option is selected when a probability of occurrence and potential damage is low or when a cost for an effective countermeasures is greater than a value of the assets to be protected.
- **Risk transfer:** this option consists of transferring risk management to another organization that has those capabilities. This can be done by signing an insurance policy or by outsourcing business process.
- **Risk reduction:** this option is selected for moderate risk, this is achieved by implementing measures, modifying and upgrading the process flow or system.
- **Risk avoidance:** this option is selected for critical functions of a business, where an organization examines well a probability of risk occurrence and reduce to zero a damage resulting from its occurrence.

**D. RISK MONITORING:** is an evaluation of effectiveness of risk management plan; and keep tracking new risks which ensures a control and an execution of a plan. Risk monitoring should be done regularly by performing a risk reassessment, risk registration updates, Technical performance or accomplishment measurement.

# Mainly Confronted Disasters in Rwanda and Management

BCM is a planning that extends well beyond IT function, it looks at everything that might cause interruption or losses in our business in order to provide effectives strategies for protecting our infrastructure, environment on which our business operations and systems are running on.

Natural disasters and other unexpected disruptions occur more frequently and cause greater damage in one way or another, especially in IT function, which is still exposed and uncontrolled as it should be; however it is a function that playing a very important role of carrying and driving our daily activities.

**A. Industrial and Technological Disasters**

A hazard originating from technological or industrial conditions, including accidents, factory explosions, fires, infrastructure failures, electrical hazard, human activities, that may cause stuff and environmental damage or any other loss etc.

**Industrial and Technological Hazards and Their Management**

- For Electrical and fire hazards no inflammable materials should be stored in the proximity, institution should ensure the availability of detection system, alarms, fire extinguishers, fire hydrants system, Emergency escape route, etc.
- To prevent explosion, continuous pressure and Temperature monitoring should carried out, availability of appropriate isolating valves, thermometers and bypass lines for Explosion.
- Regular monitoring and inspection on weakened structures by RHA (buildings), RTDA (Roads, bridges) other essential structures of common interest (RURA / MININFRA).

**B. Water Overflow**

Water overflow in our working building is a disaster if happened may have a great impact on people, infrastructures, and environment.

**PREPAREDNESS AND RESPONSE STRATEGIES**

- Regular maintenance of water piping system in building
- Early warning system for potential failures
- Assess damage and plan provision of required resources
- Construction and repair/ rehabilitation of water points including boreholes, shallow sanitation facilities in affected areas.
- Clearing and desalting of waterways and drainages structures where necessary.

**C. Earthquake**

During an earthquake ground shakes, causing a building to sway and other losses, to withstand this movement building should have a structure system strong enough to carry the earthquake forces yet flexible enough to respond to the ground motion, based on data established by Rwanda Bureau of standard (RBS).
Prevention and Mitigation Non-structural and structural Measures

- Earthquake Early-Warning (EEW): is a system estimate a level of a ground shaking to be expected and issue a warning before; which are valuable to reduce damage, costs and causalities.
- Hazard mapping and Monitoring
- Retrofitting of existing buildings especially in area threatened by earthquake, their structure should be modified to make them more resistant.

# IT- Disaster Recovery for a Business Continuity

IT disaster recovery consists of developing step-by-step procedures for a full recovery, disaster avoidance and business continuity.

When many think about DR, they usually think about Backup, while it is only one piece in BC-DR puzzle and inefficient for a continuity of business operations in an event of a disaster.

**Backup is not disaster recovery (DR) based on following points:**

- Failure of backup software
- Service Levels: backups typically happen twice per day which means that a RTO will be significantly higher and RPO could be ~12 hours data loss which is not acceptable for critical applications in DR concept.
- Reverse Replication: in an event of an outage, once an application has been made available on a target site, you must extend that application's protection to include new data being created. A backup solution can not start taking backups and ship them back to a production site, yet a DR solution will ensure that an application is still protected by replicating back to a source site.
- Application Impact: backups occur at night because, making a copy of an application and its data load a CPU on a server and impacts significantly end-user productivity.

> Every institution large or small should have both a backup mechanism and disaster recovery solution in place; they are complementary pieces to a same puzzle.

## Mitigation Measures For Some IT- Hazards

| POSSIBLE RISK | MITIGATION MEASURE |
|---|---|
| **DOWNTIME**<br>• Hardware<br>• Software | • Redundancy<br>• Maintenance and upgrade of software |

| | |
|---|---|
| **NETWORK**<br><br>• Unreliable network<br>• Loss of connectivity<br>• Traffic<br>• Misconfiguration | • Design and monitor a network for a maximum r eliability<br>• Physical protection, Redundancy or diverse pat hs<br>• Network segmentation<br>• Installation of firewalls to ensure security<br>• Load balancing (Intelligent direction to backup s ite)<br>• Use automation to deploy changes, test all c onfigurations in a lab environment before mak ing changes on your production devices. |
| **DATA AND APPLICATION**<br><br>• File corruption<br>• Application downtime<br>• Malicious software | • Data backup<br>• Mirroring of application, load balancing and replication<br>• Security management and installation of antivir us |
| **EQUIPMENT FAILURES**<br><br>• Server failure<br>• Server Overload<br>• Other Hardware<br>  • Old equipment | • Redundant disks, Backups, SAN / NAS<br>• Load balancer/Monitoring/virtualization<br>• Regular maintenance<br>• Planning for upgrades and replacing out-of-date equipment. |
| **POWER**<br><br>• Power Outage<br>• Equipment failure | • Redundancy and backup power supply (UPS an d Generators)<br>• Monitoring and performing preventative mainte nance regularly. |
| **ATTACKS**<br><br>• DDoS<br>• Viruses<br>• Hackers<br>• Other attacks | • Managed security services/anti-DDoS<br>• Installation of antivirus<br>• Firewall and other security features<br>• Access control system |
| **HUMAN ERROR**<br><br>• File deletion<br>• Unskilled people<br>• Fire | • Regular backup<br>• Access management<br>• Training / Staff certification requirements<br>• Fire detection system, fire extinguisher and fire hydrant |

# Factors Influencing a Successful IT- Disaster Recovery

### A. INFRASTRUCTURE

An infrastructure is a fundamental aspect which impacts and defines an output; an infrastructure condition or state should be well known in terms of network connectivity, quality, performance, processing capability and scalability.

Considerations at infrastructure layer:

- Before any hosting or connectivity, a required infrastructure including additional hardware and software especially needed for recovery and replication should be well defined and avoid single purpose infrastructure.
- Same Infrastructure on both sites(Primary and Alternative site)
- Availability of maintenance facilities

### B. RTO AND RPO MEASUREMENT

RTO and RPO measurement should be based on a business impact analysis (BIA), conducted, that contain a classification and BIA matrix (criticality and priority level) of systems/Assets.

*For critical systems RTO and RPO should be minimized to zero.*

### C. REDUNDANCY AND BACKUP

Backups and redundancy are both infrastructure and data protection methods, but which can not be replaceable and should be applied at every layer.

**Redundancy** is a data and system protection method considered as a real time fail prevention measure.

**Backup** does not provide real-time protection, but by performing restoration for it provides a protection against greater loss.

> Data and system backup should be done regularly and kept offsite.

### D. HIGH AVAILABILITY(HA)

HA is a disaster avoidance, a capability to automatically switch to alternative site without any downtime.

HA is achieved by applying:

- Clustering (mirroring of critical applications)

- Replication of clusters
- Load balancing in network which improves a HA by arranging multiple servers running simultaneously in primary and secondary order.
- Redundancy should be fairly implemented and sufficient at every layer (network, storage, etc.).

### E. LEVEL OF DISASTER RECOVERY SITES

**Active-Active Data centers**

With this solution both primary and secondary systems are active and processing requests in parallel.
This solution doesn't help to recover after a disaster, It helps to avoid a disaster altogether.

- RTO *is minimized to zero.*
- *The risk of losing data is significantly minimized (RPO near to zero).*

**Hot-Standby**

With this solution is a primary system has a master role and there is a backup system that is ready to take over if the primary system fails, which means a software component on a secondary system are up but will not process data or requests.

- It *can provide availability (RTO) within minutes or hours even days.*
- RPO *is significant.*

### F. REPLICATION SOLUTION

Replication for disaster recovery (DR) is no longer a "nice to have" technology, but a necessary part of every disaster recovery solution.

#### Replication Mode

**Asynchronous Mirror**

Asynchronous does not write data in non-real time. It uses snapshots to take a point-in-time copy of data that has been changed and send it to a second storage of site.

**Synchronous Mirror**

Ensures that all data is written in a source and target storage simultaneously, waiting for acknowledgment from both arrays before completing the operation.

### G. Virtualization

Software technique in which a single physical resource appears as multiple logical resources which reduce a data center complexity and improve restoration.
With this solution you have fewer number of machine to manage, also server

including operating systems, applications, patches, are all encapsulated into a single virtual server; hardware is virtual and completely separated from the actual, physical hardware in the host server, this separation and encapsulation allow redundancy and restoration, as a virtual server can be restored on another host if necessary.

**H. Security System**

Physical and cyber security system should be established.

Refer to Directive on cyber security for network and Information

# IT- Disaster Recovery Strategies

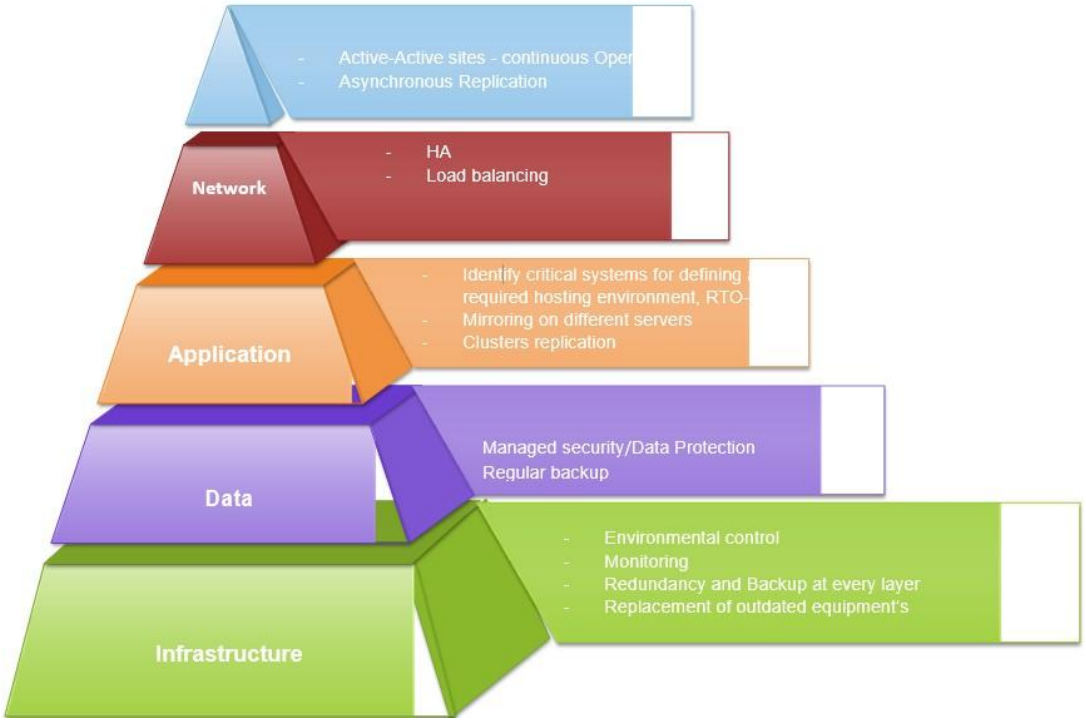



*Figure 4: IT disaster recovery strategies*

> IT disaster recovery strategies encapsulate recovery solution at different layer

# Disaster Recovery Phases

The main phases for responding to a disaster are:

- Deficiency/damage notification

- Analysis and evaluation
- Response and control of disaster (crisis management).
- Site rehabilitation and returning business to operating normal level.
- Documentation / Plan activation/update.

To ensure long-term viability and effectiveness of Business Continuity Plan, organization should maintain, conduct, and document a business continuity testing, training program regularly.

- Conducting a plan review at least quarterly
- Conduct continuity awareness briefings or orientations for entire workforce
- Train personnel on all reconstitution plans and procedures, recovery process.
- Test and validate equipment monthly to ensure internal and external interoperability, test viability of communications, alerts, notifications systems
- Test primary and backup infrastructure systems and services at primary and secondary recovery sites

# Guidance for a True IT - Disaster Recovery

- For a true DR, a recovery site should be outside of a blast radius this means if a primary site locate in Kigali a recovery site should be outside of Kigali
- Distance between sites should not be ≤ 45 km.
- Both Data centers (primary and recovery site) should be Active-Active.
- Based on distance policy for a long distance replication should be asynchronous.
- Maintenance and monitoring of infrastructure should be done regularly and to ensure a good performance, a target system should not be an old.
- Go for cloud.

## Common Mistakes

- Lack of understanding of needs (Compliancy, Due Diligence, “Never Happen to Me”).
- Never Getting Started
- Inadequate planning
- Failure to bring the business into the planning and testing of your recovery efforts