هيئة الإتصالات وتقنية المعلومات
Communications and Information Technology Commission

Guidelines on Disaster Recovery Planning for the ICT Industry

Kingdom of Saudi Arabia

هيئة الإتصالات وتقنية المعلومات
Communications and Information Technology Commission

Table of Contents

GLOSSARY

ATM	Asynchronous Transfer Mode. Packet switching protocol that encodes data into small 53 bytes packets
BC/DR	Business Continuity / Disaster Recovery
BCP	Business Continuity Plan: A clearly defined and documented plan for use at the time of a business continuity emergency, event or disaster and/or crisis.
BIA	Business Impact Analysis
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Stations
CCTV	Closed Circuit Television
Cell Broadcasting (CB)	Cell Broadcasting (CB) is an existing function of most modern digital mobile phone systems, such as GSM (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System) and CDMA (Code Division Multiple Access). It is not the same as the Short Message Service (SMS). It transmits text in a downlink only stream, so that all mobiles in that cell can receive the text at the same time. It causes short text messages in selectable languages to appear on the screen of the mobile phone, and then set off the alert tone. Since it does not use a traffic channel, it is not prone to blocking, and is therefore very useful for mass messaging, for example for warning the public on a mass scale.
Change Management	Process for ensuring that no changes are made to hardware, process software, facilities, or related processes without their impact on production (and hopefully the disaster image) being fully analyzed and evaluated
CITC	Communications and Information Technology Commission
Common Alerting Protocol (CAP)	The Common Alerting Protocol (CAP) is an open, non-proprietary standard data interchange format that can be used to collect all types of hazard warnings and reports locally, regionally and nationally, for input into a wide range of information-management and warning dissemination systems

Disaster	An emergency situation, whether caused by accident, nature or human activity that might be, or could lead to, a business interruption, disruption, loss, incident or crisis that affects a significant number of people
Disaster Management (DM)	A coordinated (and documented) activity to implement procedures to facilitate a business's continued operation during a disaster (Disaster Prevention) or, if that operation is interrupted, to facilitate a restoration of normal operation with minimum loss (Disaster Recovery, DR)
Disaster Preparedness	Disaster Preparedness in the ICT industry means putting in place procedures to increase security and resilience of the telecommunications network and other infrastructure to prevent/mitigate potential disasters
Disaster Recovery	Disaster Recovery (DR) includes putting in place procedures to be undertaken to restore normalcy of operations in the aftermath of disasters. This includes identifying the recovery strategies for all critical business functions and services, establishing recovery management organization and process, and creating recovery plans for various levels of business functions and services
Disaster Recovery Plan (DRP)	A clearly defined and documented plan of action for use at the time of a crisis. Typically a plan will cover all the key personnel, resources, services and actions required to implement and manage the DR process
Diverse Routing	The routing of information using network components that can automatically provide alternative routes to avoid congestion or network failure
DRTET	Disaster Recovery Test Execution Team
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
First Level Responders	Those agencies that are normally immediately involved in rescue and recovery operations at the disaster site(s). The first level responders typically include civil defense, public security and healthcare providers**.** The final list of FLRs will be defined at a later stage in coordination with the Civil Defense
Force Majeure	Any incident that is beyond the reasonable control of the Licensee and which it could not have anticipated when the

	License was issued or cannot be prevented such as an act of fate, wars and unavoidable natural disasters
GPS	Global Positioning System
GSM	Global System for Mobile Communications
Headroom	Surplus network capacity over and above that needed to address peak call volume and planned for growth in demand
Heartbeat Monitoring	Heartbeat monitoring is a cluster resource services function that ensures that each node (typically nodes may be the processors on each unit in a cluster of switches or servers) is active by sending a signal from every node in the cluster to every other node in the cluster to convey that they are still active. When a node fails, the condition is reported so the cluster can automatically begin the failover process to move resilient resources to a backup node
High Availability	Availability is "the percentage uptime achieved per year". High availability refers to a system with a guaranteed level of uptime (operational continuity) to the customer. The best high availability tools can provide a predictive, self-healing telecommunication system, as a component can be fixed or fail-over procedures can begin before an outage or systems failure occurs. It is possible for a system to be 'high availablility' and still be down for maintenance provided that uptime requirements are maintained. Also, redundant parts of a 'high availability' system may be down for maintenance without affecting service.
HLR	Home Location Register. Store of key client data necessary for calls to be made
ICT	Information and Communication Technology
IDR	Intermediate Data Rate equipment
IMS	Incident Management System
Interoperability	The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. The degree of interoperability should be defined when referring to specific cases

ISO 27002	ISO Standard on "Information technology - Security techniques -- Information security management systems"
ITU	International Telecommunication Union
IVR	Interactive Voice Response
Man-made Disasters	The various disasters to be considered as per the Civil Defense in KSA include – huge fires, disruption of normal life (power cut, break down and disruption of communication, transports, water etc); air, land or marine strikes; accidents of chemical, radiation or biological substances; collective displacement as a result of hostilities
MBC	Manager of Business Continuity
MSC	Mobile Switching Centre
MTBF	Mean Time Between Failures. Measure of reliability of equipment. The higher the MTBF the more reliable the equipment
MTTR	Mean Time To Repair. Often used as guideline for decision as to whether to have standby equipment on site or depend on the maintenance contract
N+2 Philosophy	Resilience philosophy whereby the function must be able to continue to support full load capacity although one unit is offline undergoing maintenance and another unit fails
Natural Disasters	A natural disaster is the consequence of a natural hazard (e.g. floods, earthquake, or landslides) which affects human activities
Network Management System (NMS)	A network management system enables effective monitoring and control of the network, and ideally covers the following: - Fault management: for fault management to be effective, there must be evidence of systems and processes being in place for fault detection, fault monitoring, finding the cause of faults, bypassing them to maintain network performance and fault fixing - Configuration management: good configuration management entails keeping a reliable inventory of network resources and having documented robust processes for the allocation of resources - Performance management: effective performance management involves the use of data from the network

	management system and elsewhere to monitor network performance, to gauge performance against specified standards and to manage call carrying capacity to meet specified grades of service - Security management: effective security management in this context involves systems and processes that control access to both the network itself and the network management system. This includes user authentication, encryption, and password protection processes - Traffic management: Real time traffic management involves the ability to gather data from various parts of the network to allow judgements to be made concerning real time call routing options, for example, local, trunk, Intelligent Network (IN) platforms or Virtual Private Network (VPN) platforms. This may also include the gathering of data from signaling links, PSTN/Internet gateways and interconnection with other licensed operators
NSS	Network Switching Subsystem
PABX	A private automatic branch exchange (PABX) is an automatic telephone switching system within an enterprise
PDU	Power Distribution Unit
PPDR	Public Protection and Disaster Relief
PSTN	Public Switched Telephone Network: network of the world's public circuit-switched telephone networks
Recovery	The rebuilding of specific business operations following a disruption to a level sufficient to meet outstanding business obligations
Recovery Point Objective (RPO)	The point in time (prior to an outage) to which data must be restored. This is agreed in advance with the business. For business critical systems it may be the last transaction before the outage occurred. For other less critical systems it could be the close of business the previous day (when, for example, the last tape backup was taken)
Recovery Time Objective (RTO)	The period of time after an outage in which systems and data must be restored to the Recovery Point Objective (RPO). A second definition is 'The maximum downtime that the business will accept before the systems, applications, or functions are

	recovered after an unplanned interruption to service takes place'
Redundancy	Back-up functionality of the systems that is available to take over in the event of failure
Resilience	The ability of an organization, staff, system, network, activity or process to absorb the impact of a business interruption, disruption and/or loss, and ensure continuity of basic services to the end user
Resilient Network	A resilient network ensures continuous operations, with no significant degradation in service, even when a key link has been severed. The equipment and architecture used are inherently reliable, secured against obvious external threats and capable of withstanding some degree of damage. A resilient network provides architectural resilience (Separacy (explained below in Glossary), redundancy, diverse routing), service resilience (example Intelligent Networks) and component resilience
Risk	An unwanted event or exposure with potentially negative consequences
SDH	Synchronous Digital Hierarchy – Technology underpinning self healing rings
Second Level Responders	Utilities (Gas, Water, Power etc), Transport, Telecommunications Providers; Health and Safety Organisations
Self Healing Rings (SHR)	A Self Healing Ring is a telecommunication transmission configuration. It consists of a ring of bidirectional links between a set of stations. In normal use, traffic is dispatched in the direction of the shortest path towards its destination. In the event of the loss of a link, or of an entire station, the two nearest surviving stations "loop back" their ends of the ring. In this way, traffic can still travel to all surviving parts of the ring, even if it has to travel "the long way round". Thus SHR offers high resilience
Separacy	Ensures that specified circuits are physically separated throughout the network so that there are no common exchanges, interconnection points or cable routes. Physical and logical separation of a circuit or system from source to destination
SLA	Service Level Agreement - A formal agreement between a service provider (whether internal or external) and their client

	(whether internal or external) which covers the nature, quality, availability, scope and response of the service provider. The SLA should not only cover day-to-day situations, but also separately cover service during disaster situations
SMPS	Switched-mode power supply
SPoF	Single Point of Failure. SPoF Analysis is fundamental to establishing the potential exposures with any installation, system or organization
STP	Spanning Tree Protocol
Telecommunication Assets	The various types of assets associated with telecommunications organizations including – switching assets, transmission assets (transmission relay systems, network cables), operation assets (telecommunication management systems to operate switching and transmission assets which contain operational information, trouble information, configuration information, customer information etc), and telecommunication service assets (portal information services, credit/prepaid call services, mobile service, roaming service, dialling/directory service etc)
TETRA	Terrestrial Trunked Radio is a modern standard for digital Mobile Radio systems. TETRA is standardized by ETSI and is a more recent standard than TETRAPOL
TETRAPOL	TETRAPOL is a fully digital Public Mobile Radio system for closed user groups, standardizing the whole radio network from data and voice terminal via base stations to switching equipment, including interfaces to the Public switched telephone network and data networks. End-to-end encryption is an integral part of the standard. TETRAPOL currently has 80 networks deployed in 34 countries and claims 70% of the European Digital mobile radio market
Tier IV Data Centre	The Tier IV data center is fault tolerant and has redundant capacity systems and multiple distribution paths simultaneously serving the site's computer equipment. All IT equipment is dual powered. The site availability expectation of Tier IV site is 99.99%
Triangulation	Backup philosophy where 3 diversely located sites are utilised which back each other up through replication and a two phase commit. It is the most secure architectural solution. It avoids the risk of the backup site becoming a single point of failure as

	normally occurs in the "conventional" primary site backup site architecture. However as with all replicated systems there is the risk that software or data corruption could be replicated across all sites
Two Phase Commit	Process whereby the backup sites are updated simultaneously with the production site.
UMTS	Universal Mobile Telecommunications System - a 3G mobile telecommunications system
UPS	Uninterruptible Power Supply/Source
VLR	Visitor Location Register
VPN	Virtual Private Network
VRA	Vital Records Analysis
VSAT	Very Small Aperture Terminal
WDM	Wavelength Division Multiplexing. Technology which multiplexes multiple optical carrier signals on a single optical fiber by using different wavelengths of laser light to carry different signals
WiMAX	Worldwide Interoperability for Microwave Access Technology for providing wireless data over long distances
WLL	Wireless in Local Loop

1 PURPOSE AND SCOPE OF GUIDELINES

1.1 Introduction

Communications infrastructure is critical to a successful Disaster Recovery (DR) process to mitigate the adverse impact on life and property. However, communications infrastructure is among the first to get severely damaged in disasters, making communication very difficult or impossible. It is therefore necessary to implement preparedness measures and establish comprehensive Disaster Recovery plans by the ICT industry, to ensure the continuity of essential facilities as well as to facilitate emergency communication users.

The DR responsibility charts in Annexure 8 clearly outline the roles and responsibilities of the various players with regard to disaster preparedness, recovery planning and emergency communications, and their dependence on other Ministries/agencies for the same. CITC is issuing these guidelines to enable the FBPs in accomplishing their responsibilities, as listed in the Regulatory Framework for Disaster Recovery Planning, through a consistent approach and in line with international best practices.

1.1 The Purpose of the Guidelines

The purpose of the 'Disaster Recovery Planning Guidelines' is:

1.2.1 to supplement the Regulatory Framework for Disaster Recovery Planning for the ICT Industry in the Kingdom of Saudi Arabia

1.2.2 to provide specific guidance for Facilities Based Providers (FBPs)

- to encourage good practices with respect to establishing disaster preparedness/prevention procedures by the FBPs
- to enable a consistent approach towards Disaster Recovery planning by the FBPs
- to facilitate emergency communications during disasters

1.2 The Scope of the Guidelines

In general these guidelines apply to all Facilities Based Providers (FBPs) for improving procedures to counter potential threats (Disaster Preparedness), establishing Disaster Recovery plans to manage restoration of operations in the event of a disaster, and facilitating emergency communications during and in the aftermath of a disaster.

1.3 The Structure of the Guidelines

The guidelines are structured in the following manner:

- Guidelines on Disaster Preparedness
- Guidelines on Disaster Recovery Planning
- Guidelines on Emergency Communications

2 GUIDELINES ON DISASTER PREPAREDNESS

Disaster Preparedness planning for FBPs implies putting in place procedures to increase security and resilience of the network and other infrastructure to prevent/mitigate potential disasters. A resilient network should be able to ensure continuous operations and service, with no significant degradation in service. The equipment and architecture used in a resilient network should inherently reliable, secured against obvious external threats, and capable of withstanding some degree of damage.

- All Facilities Based Providers (FBPs) shall develop and implement Disaster Preparedness procedures for enhancing the security of their telecommunication networks and other infrastructure based on the advisory guidelines identified below.

- The FBPs shall list the Disaster Preparedness procedures (prevention procedures) implemented by them, in the Appendix of their Disaster Recovery (DR) plans.

The guidelines provided below have been structured as:

1) Disaster Preparedness Guidelines for All Facilities Based Providers

2) Disaster Preparedness Guidelines for Fixed Facilities Based Providers

3) Disaster Preparedness Controls for Mobile Facilities Based Providers

Each section (sections 2.1 to 2.3) lists down mandatory preparedness requirements at the beginning of the section, followed by advisory guidelines to meet those requirements. The FBPs are free to choose alternative ways of meeting the mandatory requirements.

2.1 Disaster Preparedness Guidelines for All Facilities Based Providers

The FBPs shall ensure their security and resilience against potential disasters by implementing the following:

1) *Telecommunications Asset Management*: FBPs shall maintain appropriate protection of telecommunications assets.

2) *Physical Security*: FBPs shall prevent unauthorized physical access, damage and interference to business premises.

3) *Communications and Operations Management*: FBPs shall ensure the correct and secure operation of telecommunication facilities.

4) *Information Security*: FBS shall ensure safeguarding of information in networks, and the secure operation of information processing facilities.

To achieve the above requirements, the FBPs **may** use the guidelines listed below:

2.1.1 Telecommunication Asset Management

2.1.1.1 Identify each Telecommunication Asset ("asset"), and maintain an inventory of all important assets

2.1.1.2 Designate an owner for each asset. The term 'owner' identifies an individual or entity that has approved management responsibility for controlling telecommunication services, maintenance, use of, and access to Telecommunications Assets

2.1.1.3 Classify information and outputs from systems handling confidential data, in terms of their value, sensitivity and criticality to the telecommunications organization

2.1.1.4 Develop an appropriate set of procedures for information labeling and handling, in accordance with the classification scheme adopted by the service provider. Procedures for information labeling need to cover information assets in physical and electronic formats.

2.1.2 Physical Security

2.1.2.1 Use security perimeters (barriers such as walls, card-controlled entry gates or manned reception desks) to protect

areas, which contain switching, transmission, operation and information processing facilities

2.1.2.2 Protect secure areas by appropriate entry controls and intrusion detection devices to ensure that only authorized personnel are allowed access

2.1.2.3 Design and apply additional physical security for offices, rooms and facilities against damage from fire, flood, earthquake, and other common environmental threats, as well as against unauthorized access (detailed guidelines are provided in Annexure 5)

- Wherever reasonable, do not concentrate essential equipment, particularly in one building, to the extent that overall network security is jeopardized. If essential equipment is co-located (for example, multiprocessor sites), priority should be given to physical separation, such as a fire break
- Choose underground line plant, buried at a depth where intrusions are unlikely, over an aerial line plant
- Where appropriate, provide diverse cable entry points, example to sites or buildings
- Where appropriate, use diverse duct tracks or routes
- Where appropriate, use suitable detection and extinguishing systems for fire; and detection systems for explosive and asphyxiating gases, and floods
- At sites prone to flooding, utilize the buildings such that the most critical functions are performed in parts of the building with the lowest risk
- Follow relevant standards for earthquake proofing of buildings

2.1.2.4 Protect equipment from power failures and other disruptions caused by supporting utilities

- Provide an uninterruptible power supply (UPS) to all key equipment to ensure service is not interrupted in the event of a mains power supply failure
- Use duplicate mains supplies from separate sub-stations
- Ensure a supply of fuel for back-up generators with contracts for replenishment

- Consider alternate means of power like renewable energy, including some with on-site wind turbines and solar power (which thereby reduce dependency on third party energy suppliers)
- Have enough spares in air conditioning equipment to serve the peak load even if one unit is offline for maintenance and another unit fails.

2.1.2.5 Protect the power and telecommunications cabling carrying data or supporting information services, from interception or damage. It is the FBP's responsibility to use water/contamination resistant cabling of a level compatible to the criticality of the user base served[1].

2.1.2.6 Install technology such as IVR (interactive voice response) at call centers, to take over if staff is unavailable during or in the aftermath of a disaster

2.1.2.7 Implement a range of controls to achieve and maintain security in networks

- Transmission facilities such as transmission cables should be well maintained. In case of emergency situation, the facilities should be repaired as quickly as possible
- Single Point of Failure (SPoF) analysis should be conducted and measures put in place to ensure that no single points of failure exist across the network, as far as practically possible. Where SPoF involves third parties who the FBP has no or minimum influence over, negotiations should be conducted with the third party to agree on mitigation actions, possibly involving sharing the cost. As interconnect and international communications will involve potentially other national and international carriers it is necessary that negotiations start as soon as the SPoF analysis (part of the overall Risk Assessment (*refer to Section 6.3 of Annexure*)) has highlighted the exposure.
- Switching facilities for telecommunication services should be well maintained and their traffic load should

[1] Standards to be considered for critical fiber optic cables include UK-MOD Def-Stan 60- Part 3 or the equivalent American standard MIL-PRF-85045/8A. For lower priority cabling the ability to stand water immersion of at least 2 days or compliance with IEC 60974-1-2-FSB should be considered. For armored underground telecommunications, EEMUA 133 "Specification for Underground Armored Cable Protected against Solvent Penetration and Corrosive Attack" or an equivalent standard can be considered.

be monitored constantly. In case of an emergency situation, the traffic should be promptly switched to back-up facilities or other routes in order to avoid a serious traffic congestion

- In the case of DoS (Denial of Service) attacks, the switching facilities such as routers must process a larger amount of traffic compared to an ordinary situation. The FBP should implement a control to limit the traffic to an allowable level
- Within the data centre, IT equipment serving business critical systems should, where practical, be high availability
- FBPs must endeavor to implement Tier IV Data Centers for their most critical user base.
- An effective Network Management System (NMS) should be deployed, that covers fault management, configuration management, performance management, security management and traffic management.

2.1.3 Communications and Operations Management

2.1.3.1 Establish incident management responsibilities and procedures (including an escalation process) to ensure a quick, effective and orderly response to security incidents and to collect incident related data such as audit trails and logs

2.1.3.2 Implement procedures for faults to be reported and corrective action taken

2.1.3.3 Maintain equipment effectively to ensure its continued availability and integrity

- For cases when normal maintenance access to a site may be jeopardized because of bad weather, make arrangements for use of suitable alternative transport
- Where third party maintenance contractors are used, the FBP should get into Service Level Agreements with maintenance suppliers incorporating low response times (less than 4 hours preferably) from the time of notification of equipment failure. The response time should be related to the Recovery Time Objective (RTO) of systems that are supported by the equipment.

- Make an in-depth spares requirements analysis to determine which spares should be purchased and kept on-site for emergency.
- Prearrangements should also be made with major suppliers to fly in support teams in emergency or disaster situations

2.1.4 Information Security

2.1.4.1 Develop information access control policy.

2.1.4.2 Define and document the telecommunication business requirements for access control, and restrict access to authorized users only

2.1.4.3 Ensure that access to information and application system functions are restricted in accordance with the access control policy

2.1.4.4 Implement detection and prevention controls to protect against malicious software, and appropriate user awareness procedures

2.1.4.5 Establish back-up copies of essential telecommunications information and software, and test the back-up copies regularly by attempting to restore from them

2.1.4.6 Monitor the integrity of databases that store sensitive financial and business information

2.1.4.7 Develop a policy on use of cryptographic controls for protection of sensitive information

2.1.4.8 Strictly control the implementation of changes by the use of a formal change control procedure

2.1.4.9 Review and test the application systems when changes occur

2.2 Disaster Preparedness Guidelines for Fixed Facilities Based Providers

In addition to the 4 requirements listed for all FBPs in the aforementioned section 2.1, the fixed FBPs shall increase their security and resilience against potential disasters by ensuring that no single point of failure exists across their network, as far as practically possible.

To achieve this requirement, the fixed FBPs may use the following guidelines:

2.2.1 Use of diverse routing or dynamic re-routing on failure. The fixed FBPs should ensure, as far as practically possible, that there are no common ducts or switches, and that ideally, except for a very few points (usually close to termination), the routes are several kilometers apart (to ensure that they are not simultaneously taken out by a disaster) Where this is not possible, the FBPs should implement dynamic re-routing to allow affected traffic to be carried over another route.

2.2.2 Use of network physical layer technologies based on Self Healing Rings like SDH (Synchronous Digital Hierarchy)

2.2.3 Use of high availability equipment. All switches and key exchange equipment should be high availability with automated failover/fallback2.

2.2.4 Where there is not a diversely routed backup submarine cable (for example, the Sudan-Saudi cable), the FBP should arrange for backup land routes to redirect traffic if the submarine cable is cut.

2.3 Disaster Preparedness Guidelines for Mobile Facilities Based Providers

In addition to the 4 requirements listed for all FBPs in the aforementioned Section 2.1, the mobile FBPs shall ensure that they are able to provide ICT service access to the disaster struck areas that fall under their service coverage, as far as practically possible.

To achieve this requirement, the mobile FBPs **may** use the following guidelines:

2.3.1 For higher resilience of MSCs:

[2] Automated failover/fallback refers to the process of switching over (failover) to a backup system when the production system fails, and the switching back (fallback) to the production system after restoration/repair

2.3.1.1 Have duplicate MSCs in critical areas like Riyadh, Jeddah and Dammam

2.3.1.2 In non-critical areas, have overlaps in the geographic coverage between MSCs, and keep spare capacity in all MSCs to allow switching of traffic between the MSCs within the network

2.3.2 Establish a backup HLR (Home Location Register) for each production HLR, and locate it at a different site. All updates to the primary HLR should be mirrored at the backup unit

2.3.3 Deploy a hot standby unit containing a backup VLR (Visitor Location Register) at each MSC

2.3.4 Deploy interim mobile network facilities to disaster hit areas as quickly as reasonably possible to allow services to be restored to the most critical areas identified by civil and military authorities

- Deploy transportable (mobile) BSCs to cover for failing fixed BSCs in locations within their networks, where duplicate or overlapping BSCs don't exist

- Deploy mobile BTS for quick provision of mobile services to disaster hit areas. Enough mobile BTS should be maintained to be able to reach, within 4-5 hours, any of the locations that are part of their network coverage

2.3.5 Surplus capacity in excess of that required to cope with peak demand and planned growth should be maintained by the mobile FBPs in their networks to manage unforeseen demand during disasters

3 GUIDELINES ON DISASTER RECOVERY PLANNING

3.1 Requirements for DR Planning for FBPs

3.1.1 Facilities Based Providers (FBPs) are required to create DR plans for their own organizations (An advisory detailed methodology for creation of DR plans is provided in the Annexure 6)

3.1.2 The DR plans are required to be submitted for approval to CITC

3.1.3 The FBPs are required to identify one representative from their Senior Management for overall ownership of DR management for their organization

3.1.4 The FBPs shall notify CITC of any outages as per their Stakeholder Notification Plan, which is part of their DR plans

3.1.5 The FBPs shall establish a regular test and exercise schedule for their DR plans that includes a comprehensive test of their DR plans at least bi-annually, and varying stage tests (See Paragraph (3.2.2)) of their DR plans half-yearly to ensure a state of readiness

3.1.6 The FBPs shall provide CITC with their testing and maintenance program:

- Provide a "Test Calendar" that shows the different test types and their frequency, sequence and dependency to the other tests
- For each test, FBPs should provide objectives of the test, list of participants, scope, schedule, prerequisites and outcomes
- The results have to be documented precisely to facilitate audit by CITC

3.1.7 The FBPs are required to invite CITC to attend the testing of their DR plans, providing a notice of at least one week.

3.1.8 The FBPs shall ensure that the DR plans are based on the generic 'Table of Contents for a DR Plan' provided in Annexure 7.

3.2 Guidelines for DR Plan Maintenance for the FBPs

3.2.1 Undertake a risk analysis and business impact analysis with respect to all their systems at least once every two years

3.2.2 Apply a staged approach to testing of the DR plans to minimize the risk to the production environment

3.2.2.1 Initially undertake a 'Tabletop exercise' to raise the awareness of the business functions involved and highlight any obvious exposures in the plan

3.2.2.2 In the second stage, conduct functional testing for various functions. These should highlight any problems with the DR plan which can be modified accordingly

3.2.2.3 In the last stage, conduct the "production test", i.e, full-scale testing, where the DR plans are fully exercised

3.2.3 Analyze the test results against DR objectives to identify improvement/modifications for the DR plans

3.2.4 Review the DR plans within the FBP's organization, at least once annually, to identify any revisions to the plans based on the changes that might have occurred to the organization's business, structure, systems or personnel

4 GUIDELINES ON EMERGENCY COMMUNICATIONS

These guidelines are for facilitating emergency communications during disasters. The various categories of communications covered under the guidelines are -

- Communication between authorities/organizations (public safety communications)
  - Primary Communication Options
  - Secondary Communication Options
- Communication from users to authorities/organizations (emergency calls)
- Communication from authorities/organizations to users (warning systems)
- Communication among users

4.1 Communication between Authorities/Organizations

4.1.1 Primary Communications

4.1.1.1 For the purpose of facilitating communications between authorities during disasters, CITC shall establish a harmonized narrow band of 5 MHz for all public protection and disaster relief equipment, to allow easy compatibility of equipments of various responder organizations (like Police, Fire agency, Emergency medical services, Relief agencies etc) during disasters.

4.1.1.2 It is suggested that the First Level Responder organizations (like Police, Fire agency, Emergency medical services) deploy equipment based on the same standard, preferably the standard ETSI TETRA, which is becoming the de facto world standard used by most countries

4.1.2 Secondary Communications

Irrespective of the choice of primary method of communication for first level responders it is necessary to have at least two alternative communication mechanisms (Secondary communications) available as backups. The preferred solutions include conventional fixed line networks, conventional mobile networks, and satellite networks.

4.1.2.1 A system of privileged access for emergency communications by authorized users (First Level Responders, relief agencies and designated civil servants etc) shall be implemented by the

Facilities Based Providers (FBPs). CITC shall coordinate with the Civil Defense to identify the list of agencies/persons that shall have access to these priority access services.

4.1.2.2 It is suggested that the Civil Defense stockpiles an appropriate number of satellite communication sets for use by strategic level coordinators in a disaster

4.1.2.3 This satellite equipment shall have access to a dedicated channel that will not get congested during disasters. CITC will coordinate with MCIT and the Civil Defense for allocating specific frequency/bandwidth that could be used by satellite equipment of Civil Defense and FLRs during and in the aftermath of disasters.

4.2 Communication from Users to Authorities/Organizations (Emergency Calls)

Currently in KSA, several emergency numbers exist for the various public protection agencies – Police (999), Medical (997), Fire (998) and Traffic Police (993) (112 is for emergency GSM/UMTS calls and the call is directed to 999, which is police department). Since most of the calls are non-emergency related (by international experience), it is essential to differentiate between emergency and non-emergency calls.

4.2.1 It is recommended to setup a single primary emergency number (for all agencies like police, fire, medical), with the emergency call reception centre having the responsibility to coordinate the contact centre effort where multiple emergency services need to be involved. CITC will coordinate with MCIT and the Civil Defense for assigning a single primary emergency number and establishing the responsibility for that number.

4.2.2 In addition, it is recommended that a dedicated number for non-emergency calls to the emergency services control centre be set up. CITC will coordinate with MCIT and the Civil Defence for assigning a single number for non-emergency calls and establishing responsibility for that number.

4.3 Communication from Authorities/Organizations to Users (Warning Systems)

These guidelines are to ensure that the users are warned of an impending disaster and given instructions on what they should do.

4.3.1 CITC shall liaise with the MCIT (Ministry of Communications and Information Technology) and the Civil Defense to establish a system of receiving disaster warning alert messages

4.3.2 The FBPs shall liaise with CITC and the Civil Defense to establish procedures to receive authorized warning messages and broadcast them to the users using effective methods like Cell Broadcast

4.4 Communication among Users during Emergencies

During and aftermath of disasters, due to the steep rise in voice calls from users trying to get in touch with their loved ones, congestion may occur, leading to failure to connect or dropped calls. This is made worse by common behavior during disaster like “not disconnecting calls for a long time once a call connects”.

4.4.1 All ICT service providers shall implement awareness programs for spreading awareness about correct usage of telecommunications services by users during disasters. The ICT DR Committee shall advise on awareness campaign requirements and content. The service providers shall then implement these programs for their subscribers.

ANNEXURE

5 GUIDELINES FOR GENERIC INFRASTRUCTURE

It is advisable that key buildings within the FBP's organisation be designed to be as resilient as possible to resist/counter threats. This section provides a checklist for the resilience of critical buildings such as data centres, Mobile Switching Centres, Base Station Controllers and major offices.

The checklist is not all encompassing but shall be used as an advisory guideline in relation to new buildings or for retrofitting existing buildings.

5.1 Location

- As all of KSA is vulnerable to seismic activity, it is difficult to eliminate the risk. If possible, the building should not be located in an area with a past history of seismic activity
- The building should not be located in an area:
  - With a history of flooding or landslides
  - Within 1.5 km of the floodplain of a river
  - Below sea level
  - Within 1.5 km of the Red Sea coast (risk of Tsunami)
  - Prone to subsidence or where significant mineral extraction has taken place
  - Under the flight path to a major civilian or military airport
  - Close to a major thoroughfare on which hazardous materials are regularly transported

5.2 Building Surroundings

Consideration shall be given by the FBPs to the landscaping of the area surrounding the building to include:

- High (2 metre+) banks or rows of trees/bushes shall be used as mitigation action with regard to vehicle impact, and/or terrorism

- Internal access roads shall incorporate 90 degree turns to slow up traffic
- Car parks shall be located outside the perimeter fence; or, if within, they shall be several hundred metres from the building.
- Vehicle security/access control functions complete with barriers shall be located at the perimeter at least 60m from the building. All mechanical access control functions shall be resilient with "failsafe" actions if the access control staff or systems are compromised. They shall however have a manual override to allow access by emergency service vehicles.

5.3 Building Infrastructure

Building infrastructure in this context covers:

- Power
- Fire Detection, Warning, and Eradication devices
- Air Handling
- Lightning Protection
- Water detection and protection systems
- Environmental monitoring systems
- Within building access control systems
- Cabling
- Plant room

5.4 Power

5.4.1 Mains Power

Power failures are the major cause of outages in the ICT industry. The key factors to consider by the FBPs are

- Business critical buildings require dual or multiple independent power supplies
- Separate power supplies shall enter the building at different points.
- Separate power feeds shall not share ducts. It is advisable to get the power suppliers to confirm that this is not the case and that they do not sub contract power from a third party supplier
- Dual power supplies should be provided by different mains power suppliers

- Once power has entered the building the design shall ensure that there are no single points of dependency in its distribution to key areas and equipment throughout the building that could cause failure.

Attention shall be given to confirming:

- There is more than one power distribution unit (PDU) in each switch room
- Each PDU is connected to separate mains feeds
- All hardware installed in Computer or Switch room is connected to two separate PDU

5.4.2 Auxiliary Uninterruptible Power Supply (UPS)

Even with the level of resilience suggested in the above section, it is not advisable to depend purely on mains power. The past incidence of mains power failures throughout the world dictates that the FBP requires access to the facilities of an uninterruptible power supply (UPS). What is termed a UPS usually consists of a combination of generators, battery backup, and occasionally power smoothing devices.

- Each business critical building shall be connected to a UPS for emergency lighting, elevators, fire eradication system, and environmental monitoring
- The UPS shall include at least one generator of sufficient capacity to be able to support the full business load.
- To minimize the risk of system crash during the period when power transfers from mains to generator, backup battery systems shall be implemented as an automated system to start the generator as soon as A/C current drops below a threshold. Dependence on a manual start up generator merely adds additional single points of failure.
- The full load capacity of the generator shall be greater than the peak critical business load to allow for growth in business.
- The generator fuel tanks shall normally permit a minimum of N+2 days continuous full load running (where N is equal to the maximum number of contiguous festival days (holidays) in the region). At the very least, fuel for 4 days of continuous full load running capacity should be maintained.
- Irrespective of the N+2 fuel capacity philosophy, a contract shall be signed with a fuel supplier to refill once the bunker fuel supply has fallen to 40% of full capacity or four full days use, whichever is greater.

- A maintenance contract shall be in place to service the generators at least annually, or as recommended by the manufacturer, ideally at a time considered as least risky to mains power historically.
- There shall be a comprehensive monitoring system with regard to the generator to highlight any malfunction immediately.
- The battery backup shall be capable of running the full load of all systems for sufficient time to allow an orderly shutdown. "Sufficient time" shall include time to communicate the need to close down plus a contingency (say 25%) to allow for delays or failures in the closedown process.
- The capacity of the battery backup shall be periodically reviewed in the context of the production workload.
- Although battery backup can be either gel cell or lead acid, the former shall be preferred since it is less prone to leakage
- Spare battery cells shall be carried on site and staff trained in their replacement
- The danger period with regard to battery backup is when it is undergoing recharge (often a considerable period). The generators shall be run when the batteries are being recharged, providing cover in case of a mains power failure

5.5 Fire Detection, Warning and Eradication

5.5.1 Detection

- Each room in the building should be fitted with smoke detectors
- All detectors shall be tested at least twice annually
- Key rooms and common areas shall be fitted with manual pull-alarms for personnel to activate at the earliest detection of a fire or hazardous condition

5.5.2 Warning

- A fire alarm system shall be in place and periodic tests (scheduled and random tests) of the fire alarm system shall be taken.

5.5.3 Eradication

- An inert gas fire eradication system shall be installed and cover all business critical parts of the building.
- The gas based eradication system shall be backed up by a water sprinkler system and/or hand held fire extinguishers to address

situations where the gas does not fully eradicate the fire, except in rooms like switch rooms or computer rooms where water needs to be avoided

- Each gas bottle incorporate a gauge to show gas pressure with a threshold pressure below which it should be replaced
- A maintenance contract should be in place to address the replacement of gas within 24 hours of notification

5.5.4 Fire Detection and Eradication Monitoring System

- Each Building should have a central monitoring system at minimum monitored by security and accessible to first-responders for all smoke detectors, fire alarms and eradication systems
- The central monitoring system should identify the operating status and "alarm" condition of each smoke detector, alarm and eradication system component

5.6 Air Handling/Conditioning Resilience

- The air conditioning plant shall be high availability in design, incorporating component level redundancy
- An N+2 philosophy shall be adopted with respect to air conditioners to allow for maintenance of units to take place without any impact on the business even if one air conditioner fails.
- All air conditioning equipment shall be connected to the UPS
- Where the air conditioners use a coolant gas such as Freon, consideration should be given to carrying a stock of gas on site
- A regular maintenance schedule shall be in place for air conditioners. For any air conditioners with a 'Mean Time to Repair' greater than Recovery Time Objective of the systems that they support, it is essential that a hot standby air handler be available along with a method to switch between units.
- All of the air conditioning units shall be connected to at least two independent mains power supplies.
- The air conditioners shall be connected to an environmental monitoring system which can identify any problems with each unit and highlight hotspots in the switch/computer room.
- A comprehensive Maintenance Schedule shall be established to ensure the regular replacement of air-handling filters, maintenance of refrigerant levels, and proper system operations

5.7 Water Detection and Protection Systems

- It is advisable to ensure that no water or waste pipes are located above the computer room, or switch room
- Water detectors shall be installed in the ceiling space above the business critical rooms, and in the floor below the rooms
- Channelling shall be installed in the floor and ceiling to direct water away from the switch room or computer room
- If the position of the data centre or switch room permits, drains shall be installed to allow any water that enters the room to drain away into a lower level
- All water detection and protection systems shall be connected to an environmental monitoring system to identify the individual operating status and "alarm" condition of each of the system components

5.8 Environmental Monitoring Systems

- All security and environmental protection systems shall be monitored by a comprehensive environmental monitoring system, the operations area of which shall be located significantly away from the business critical room
- There shall be a backup operations area for the monitoring system, located in a different building
- All security or operations area staff shall be trained to recognize the symptoms of potential disaster and act accordingly
- The monitoring system shall be designed to cover both local and remote sites
- The environmental monitoring systems shall be connected to the UPS, and, if standalone, shall feature an internal battery backup

5.9 Within Building Access Control Systems

- There shall be one entry point which is secured via an electronic access control system along with at least two emergency exit points both of which are connected to an audible alarm if opened other than in an evacuation
- Within building access control systems shall feature a combination of electronic access control and human security interfaced with a thorough initial screening of employees through the Human Resources vetting function
- The electronic access control systems implemented shall be appropriate to the level of sensitivity of the building and data contained therein
- Electronic access control systems shall be capable of being manually overridden in an emergency such as a building evacuation.

- Within those rooms housing lots of equipment, CCTV cameras shall be installed. The primary aim is to monitor in case a member of staff in the room has a medical emergency or injures himself. The CCTV tapes could also prove useful in the event of sabotage or theft.

5.10 Plant Room

- The plant room, which usually houses generators and some air conditioning units, shall have hermetically sealed doors to protect the equipment from the effects of dust storms or flash floods.
- It is advisable to ensure that the air intakes of the generators are at least one meter from the ground to eliminate risks from flash floods

6 DETAILED DR PLAN CREATION METHODOLOGY

This section provides the detailed methodology for preparation of Disaster Recovery plans.

6.1 Mission/Strategy and Scope

The primary aim of DR planning within the ICT industry is to ensure that the business processes are restored within agreed recovery time in the event of an unplanned interruption to service or denial of access to staff.

The FBP should ensure that the DR Plan is:

- Written and disseminated so that the staff who are familiar with the organization but not the function can implement the plan in a timely manner
- Specific regarding what conditions should prompt implementation of the plan
- Specific regarding what immediate steps should be taken during a disruption
- Flexible to respond to unanticipated threat scenarios and changing internal conditions
- Focused on how to get the business up and running in the event that a specific facility or function is disrupted, rather than on the precise nature of the disruption
- Effective in minimizing service disruptions

6.1.1 Scope

- The plan should document strategies and procedures to maintain, resume, and recover critical business functions and processes and should include procedures to execute the plan's priorities for critical vs. non-critical functions, services and processes.
- A well-written DR Plan should describe in some detail the types of events/decision points that would lead up to the formal declaration of a disaster and the process for invoking the plan.
- It should put in place planned, coordinated responses which escalate according to the nature of the outage. It should describe the responsibilities and procedures to be followed by each of the continuity teams and contain contact lists of critical personnel.

- The DR plan should describe in detail the procedures to be followed to recover each business function affected by the disruption and should be written in such a way that staff who are familiar with the organization but not the function can implement it in a timely manner.

DR planning is a part of the overall BC process and consists of Recovery Strategies, Developing DR Plans (Crisis Management Process and Organization and documented DR Plans) and DR Plans Testing and Maintenance. Before, the recovery strategies can be developed, DR Accountability has to be defined, and Risk Assessment and Business Impact Analysis need to be carried out by the BC function in the organization, in conjunction with the representatives of the various business functions. The steps that go into the creating of DR plans thus include -

Figure 1: DR Planning is part of Overall BC Management

Business Continuity Management					
			Disaster Recovery Planning		
1 BC/DR Accountability	2 Risk Assessment	3 Business Impact Analysis	4 Developing Recovery Strategies	5 Developing DR Plan	6 Testing and Maintenance
• Define the sponsor of the DR at the highest seniority level in the organization • Define a Business Continuity Function with clear role and scope within the organization	• Review the potential disruptions • Prioritize risks based on severity and likelihood of occurrence • Specify definition of specific scenarios	• Identify potential impact of disaster on business operation • Establish allowable outage time • Prioritize the critical business processes • Establish the recovery objectives for critical business processes	• Identify and document alternate recovery strategies for backup, alternate sites and equipment replacement. • Identify resources required for resumption and recovery • Perform a cost-benefit analysis to identify the optimum recovery strategy	• Crisis management organization structure and process (including stakeholder notification and recovery team notification) • Content of DR plan • Introduction • Notification/Activation Phase • Recovery Phase • Reconstitution Phase • Appendices	• Testing objectives • Testing options •Orientation •Tabletop •Functional testing •Full-scale testing • Text Execution • Result analysis • Plan Maintenance

The following six sections will describe in detail each of these steps.

6.2 Establishing BC/DR Accountability

- It is essential that senior leadership (Board level member(s)) of the organization sponsors and takes responsibility for creating, maintaining, testing, and implementing a comprehensive DRP. This will ensure that management and staff at all levels within the organization understand that BC/DR is a critical top management priority.

- The Board member needs to first establish a Business Continuity Function (if one doesn't exist already in the organization) that will be responsible for carrying out the tasks leading to the creation of DR plans, and setting up of crisis management organization and processes.

6.2.1 Business Continuity Function

A Business Continuity Function should be sponsored and ideally funded at Board level. It is responsible for (apart from general risk management of the business operations) carrying out the steps leading to creation of DR plans, and setting up of crisis management organization and processes.

Scope: Business Continuity Function

- Raise the awareness within the organisation of the need for DR highlighting the responsibilities at both individual and departmental level.
- Periodically audit the organisation to identify the current status of exposures and identify mitigation actions that could be put in place. This would be part of an overall risk analysis.
- Jointly with the business managers, conduct a Business Impact Analysis to identify what would be the impact, over time, of system outages and identify the Recovery Time Objective and Recovery Point Objectives of systems.
- Undertake a service classification analysis in order to establish, from business perspective, the business criticality and desired recovery sequence.
- In conjunction with the business, facilities, network operations and technical functions develop the appropriate recovery strategies.
- Create and champion the business cases to obtain the resources required to implement the recovery strategy.
- Jointly with the business and technical departments develop the DR plans necessary to minimise disruption from events causing unplanned outages to system delivery.
- Assist the DR Test Execution Team in planning the testing of the plans

The Business Continuity Function, in conjunction with business managers, then carries out the steps leading to creation of DRP: Risk assessment using Emergency Cases, Business impact analysis and developing Recovery Strategy.

6.3 Risk Assessment based on Emergency Cases

A Risk Assessment process is designed to identify and analyze the types of risk that may impact the organization. Assessment should be performed by a group representing various organizational functions and support groups, with the aid of the Business Continuity Function. It should include:

- Reviewing types of potential disruptions that could impact the business
- Prioritizing of potential business disruptions based upon severity and likelihood of occurrence;

The risk assessment step is critical and has significant bearing on whether DR efforts will be successful. If the emergency cases developed are unreasonably limited, the resulting DRP may be inadequate.

Specific cases (or scenarios) should include, for example, how the organization would respond if:

- Critical personnel are not available
- Critical buildings, facilities, or geographic regions are not accessible
- Equipment malfunctions (hardware, telecommunications, operational equipment)
- Software and data are not accessible or are corrupted
- Vendor assistance or service provider is not available
- Utilities are not available (power, telecommunications)
- Critical documentation and/or records are not available

6.4 Business Impact Analysis

Once risks have been identified, any organizational impacts that could result, over time, from an interruption of normal operations should be examined in a Business Impact Analysis (BIA). Impacts can be both qualitative or operational and quantitative or financial. The identification of impacts is a critical component required in the cost-benefit analysis, evaluation and selection of viable recovery strategies. BIA should include:

- Identification of the potential impact of unavailability of functions/processes or assets on the organization's business processes and its customers;
- Establishing the maximum allowable outage for business processes, i.e., determine how long process can be non-functional before impacts become unacceptable. (The effects of the outage can be tracked over time as well as across related resources and dependent systems identifying any cascading effects). Cost of system inoperability is weighed against the cost of resources required for restoring the system.
- Determine what and how much is at risk by identifying critical business functions and prioritizing them (also called Service Classification Analysis)

- Establish the Recovery Time Objective RTO (Determining how long process can be nonfunctional before impacts become unacceptable) and Recovery Point Objective RPO (Establishing to what point in time the business needs data restored to) for each critical business process. These are determined by business owner in conjunction with the Business Continuity Function (The RTO/RPO objectives for business processes might differ based on the time of the year).
- It is essential to have a full understanding of the interactions between systems when developing the recovery objectives. A system which, in the view of the business owner, is non-critical may be inputting files into business critical systems. Hence the lowest of the RTO of interfacing systems must apply to all of these systems

6.4.1 Vital Record Analysis

A fundamental part of the Business Impact Analysis and Business Unit Recovery process is Vital Records Analysis. The objective is to identify which records are:

- Essential to allow the business unit to be recovered and continue its work from another location. Typical example of vital records would be - current account receivable and accounts payable, current contracts, un-audited financial records, personnel files, engineering plans, software licenses, data backup media etc
- Required for audit purposes
- Needed to comply with regulatory requirements
- Needed for potential legal reasons, for example HR department case notes

Vital records may be physical hard copy documents or files on magnetic media. In relation to hard copy documentation, at least two copies should be taken, one of which should be stored on-site, in a fire proof safe. One or more additional copies should be stored off-site at safe location(s). The number of copies will be dictated by the recovery strategy.

Most vital records will not be held in hard copy format but will be held on magnetic media such as one of the network drives. Where vital records are stored on magnetic media:

1. It is essential that backup copies are taken at set intervals and when any changes to the record have been made.

2. The location of the record. Type of media it is held on and recovery point objective (RPO) of the data must be identified.

3. All backups must be proven to be readable at the time they are taken (a read after write process for tape copies) or soon afterwards. The records should be restored periodically to ensure that no corruption has taken place.

4. A minimum of two copies should be taken, one of which should be stored a significant distance away from the primary processing centre. This may be at a dedicated storage repository, or replicated on a disaster recovery configuration or a network attached storage.

5. A version control process should be in place to ensure that each member of the team is working, after the business unit has been recovered from records of the appropriate currency.

6. In the worst case scenario where the latest records cannot be recovered, details of how the records will be brought up to the appropriate RPO should be identified.

6.5 Developing Recovery Strategies

Once the BIA has been completed, the next step involves determining the recovery strategy for the various business processes.

The decision regarding the recovery strategy to be followed is critically dependent upon:

- The corporate philosophy as regards resilience to be incorporated in the system design.
- The perceived business criticality of the operators systems as defined by the maximum outage that is tolerable without an unacceptable amount of damage being done to the operator and/or its reputation (as determined by the BIA discussed in the previous section).
- Statutory and regulatory guidelines as regards system resilience

The outage impact(s) and allowable outage times characterized during the BIA, leading to the establishment of recovery objectives (RTO/RPO) enable the development and prioritization of recovery strategies for the various business processes and corresponding resources/facilities. (The time within which a service must be restored has a massive bearing on the potential technical solutions that can be applied to recovery).

A wide variety of recovery approaches may be considered; the appropriate choice depends on the incident, type of system and its operational requirements.

Recovery strategies provide a means to restore operations quickly and effectively following a service disruption. The process of developing recovery strategy includes -

- Identify and document alternate recovery strategies for backup, alternate sites and equipment replacement.
- Identify resources required for resumption and recovery. Such resources can include personnel, technology hardware and software, specialized equipment, general office supplies, facility/office space and critical and vital business records.
- The organization should perform a cost-benefit analysis to identify the optimum recovery strategy
- It should be ensured that the strategy chosen can be implemented effectively with available personnel and financial resources. The cost of each type of alternate site, equipment replacement, and storage option under consideration should be weighed against budget limitations.

Various components of recovery strategies include –

6.5.1 Backup Methods

Relevant system data needs to be backed up regularly. Policies should specify the frequency of backups (e.g., daily or weekly, incremental or full), based on data criticality, the time to restore the data under the worst-case scenario in order to meet the system Recovery Time Objective RTO and Recovery Point Objective RPO, and the frequency with which new information is introduced. When selecting an offsite storage facility, criteria to be considered include the geographic distance from the organization, accessibility, security/confidentiality and costs involved. It should be standard practice to take at least two backups, one to be stored in a fireproof safe on site and a second to be stored at the offsite location

6.5.2 Alternate Sites

The plan must include a strategy to recover and perform system operations at an alternate site for an extended period. In general, two types of alternate sites are available:

- Dedicated site owned or operated by the organization
- Commercially leased facility

Sites may be identified as cold sites, hot sites, mobile sites and mirrored sites based on their operational readiness, with mirror sites providing almost immediate resumption capacity. Some organizations have identified the need to have a third location or a “back-up to the back-up.” This is called tertiary location (Triangulation philosophy). These tertiary locations provide an extra

level of protection in the event neither the primary location nor the secondary location is available. Additionally, a third-location provides a backup site while in disaster recovery mode, and operations can be run at either of the recovery locations until operations can safely return to the primary location.

6.5.3 Equipment Replacement

When primary site is damaged/unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. Two basic strategies exist to prepare for equipment replacement.

Vendor Agreements - As the DR plan is being developed, SLAs with hardware, software, and support vendors may be made for emergency maintenance service. The SLA should specify how quickly the vendor must respond after being notified.

Equipment Inventory - Required equipment may be purchased in advance and stored at a secure off-site location.

6.6 Developing DR Plans

After conducting the Risk assessment, Business Impact Analysis and deciding on the Recovery Strategies for critical business functions, the next step involves actual DR planning in the following 2 steps –

1. Establishing the overall Crisis Management Organization and Process
2. Development of written DR Plans for various levels of business functions

Both these steps are discussed in the two sections below –

6.6.1 Establishing the Crisis Management Organization and Process

Before the actual DRPs are written down for various levels of business functions, it is essential to establish the various teams in the Crisis Management Organization that will be responsible for initiating, coordinating and executing the DR Plans at various levels.

The Crisis Management process describes the procedures that are followed for the invocation of DRPs, notifying the various teams, decision points and escalation procedures during the DR process.

The Crisis Management Organization and Crisis Management Process are described below –

6.6.1.1 Crisis Management Organization

A generic Crisis Management Organisation will consist of the following teams:

Primary Teams (to be activated in all crisis where a disaster is declared)

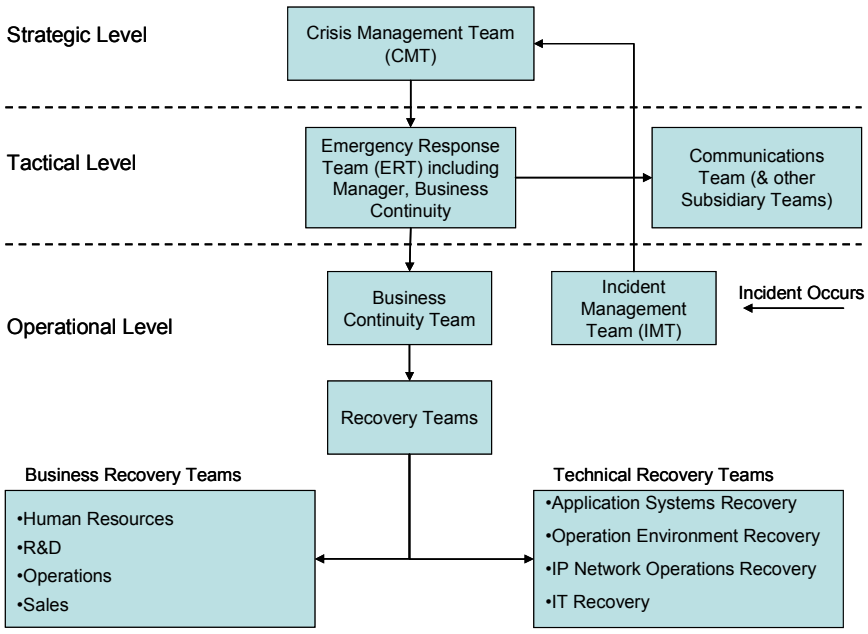
- Crisis Management Team
- Emergency Response Team
- Incident Management Team
- Business and Technical Recovery Teams
- Business Continuity Team (from Business Continuity Function)

Apart from these, certain subsidiary teams can be established that can be activated for specific functions as/when the nature of the disaster dictates. Some of these include

- Damage Assessment and Facilities Restoration Team
- Communications Team
- Administration and Staff Welfare Team

Brief descriptions of the roles and responsibilities of the primary teams are detailed in the next section. Figure 2 below depicts the Crisis Management Structure that should be in place in an organization to enable effective DR.

Figure 2: Crisis Management Structure



6.6.1.1.1 Primary Teams

The following table gives an overview of the various primary teams and their role –

Team	Role
Crisis Management Team	The Crisis Management Team (hereafter, referred to as CMT) is the supreme decision making body with respect to a disaster, although it will usually delegate executive powers to the Emergency Response Team for the initial period (usually 48 hours) of disaster response
Emergency Response Team	The role of the Emergency Response Team is to coordinate the response to a disaster (once it has been declared by the Crisis Management Team) for the critical initial 48 hours (this period may be extended at the discretion of the Crisis Management Team)
Incident Management Team	The identification, reporting, analysis, assignment, resolution and/or escalation of incidents which may lead in the short or long term to a disruption to normal processing of all or part of the business workload
Recovery Teams – Business Recovery Teams and Technical Recovery Teams	The Business Recovery Teams are responsible for conducting recovery of business operations for the critical functions of their respective organization. Each critical business unit will have a designated recovery team to perform the tasks necessary to recover these business functions
	Technical Recovery Teams have responsibility for the restoration of the operational systems and communication functions of the business. In this capacity, the team leaders will provide recovery direction and problem resolution, monitor progress, and report recovery status to the Manager, Business Continuity. There will be several technical recovery teams addressing areas such as application systems recovery, operational environment recovery, IP network operations recovery and IT recovery
Business Continuity	The role of the Business Continuity Team is to coordinate the Recovery Teams' effort and notify

Team	the recovery status to the Manager, Business Continuity

6.6.1.1.2 Subsidiary Teams

The following table gives an overview of the various subsidiary teams and their role –

Team	Role
Communications Team	The Communications team will be the sole source of communication with regard to the transmission of information to all external parties and internally within the organisation
Damage Assessment and Facilities Restoration Team	This team will assess the extent of the damage to the serviceability of premises and the environment infrastructure, secure the protection of all physical infrastructure, co-ordinate with insurance firms and carry out new procurement/replacement if required
Staff Welfare and Administrative Resources Team	The 'Staff Welfare and Administrative Resources Team' is responsible for coordinating/easing the logistics in relation to business unit and recovery team staff with regard to combating a disaster

The next section details the Crisis Management Process, i.e., the procedures that are followed for the invocation of DR Plans, notifying the various teams, decision points and escalation procedures etc during the DR process.

6.6.1.2 Crisis Management Process

A Crisis Management Process addresses incidents which either are causing disruption to service, or have the potential to cause disruption and cannot be addressed by "normal" operational procedures. Allied to the resolution process is a stakeholder management component to ensure that those stakeholders who need to know of the disaster (such as the regulator), or whose resources may be involved in the problem resolution, are appraised of the status from authoritative sources.

The generic process of crisis management is discussed below, following by details of important components of Crisis Management Process –

- Recovery Team Notification
- Stakeholder Notification

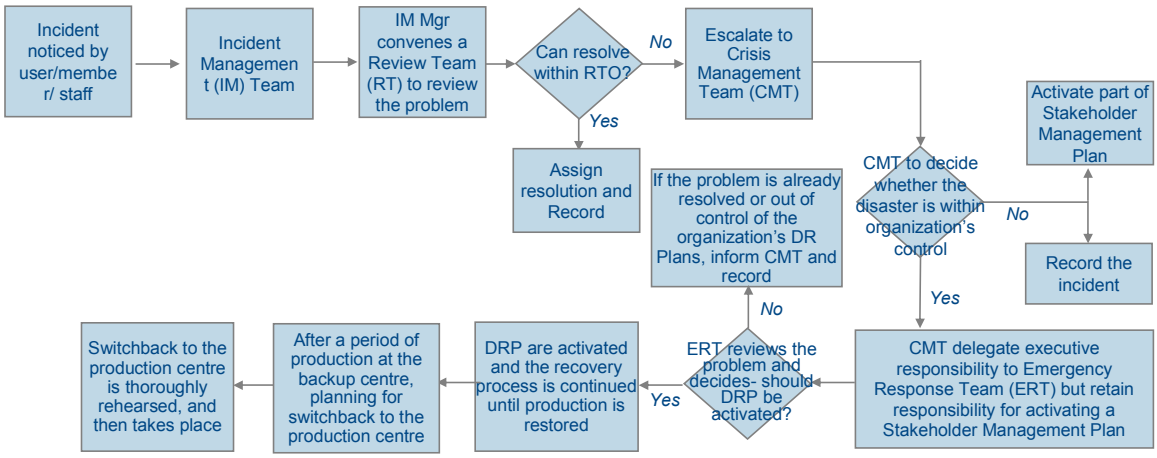
6.6.1.2.1 The Process

A summary of the Crisis Management Process for a type of disaster confined to the operator's sites, networks, or applications is as follows -

1. An incident occurs and is noticed by a user or member of staff who escalates it to the incident management team
2. Incident Management record the problem; conduct an initial assessment of its nature and impact; and assign it for resolution.
3. The Incident Management Manager convenes a review team consisting of the business, technical support and other impacted parties. If the review team decides that the problem cannot be resolved within its RTO, it escalates to the Crisis Management Team (CMT) with a recommendation to declare a disaster.
4. The Crisis Management Team (CMT) is briefed and decides whether to declare a disaster. If it does so it would normally (except in a catastrophic disaster or one of political significance) delegate executive responsibility to the Emergency Response Team, at least for the first 48 hours of the disaster. Although delegating executive power, the CMT would normally retain responsibility for activating a Stakeholder Management Plan. The organization must set a time-limit for making the Disaster Declaration decision following an incident occurring, otherwise recovery strategies will not be able to be carried out within the prescribed RTOs.
5. The Emergency Response Team reviews the problem and decides whether to activate DR Plans.
6. DRP are activated (***Recovery Team Notification and Stakeholder Notification***) and the recovery process is continued until production is restored
7. After a period of production at the backup centre, planning for switchback to the production/primary centre (if it still exists) at an appropriate date takes place
8. Following restoration of the primary location or establishment of a new primary location, switchback from

the backup centre to the restored or primary location is thoroughly rehearsed and then carried out

Figure 3: Crisis Management Process



In the situation where an incident has occurred and it is completely obvious that a disaster has occurred from:

- the extent of the damage to facilities and/or networks,
- the extent of injury or loss of life amongst the operator's staff or elsewhere,
- inability of the systems to continue to meet business objectives or regulatory requirements,
- the impact on the region or country,

then, any surviving member of the CMT, plus the Incident Management Manager, and Business Continuity Manager should have the authority to convene a meeting (whether actual or virtual) of the CMT, and through it declare a disaster, and activate DR plans. Documentation of the incident can be undertaken retrospectively after mitigation actions have been carried out.
Depending on the severity of the disaster the individual operator's recovery plans may need to be modified to conform to industry or national recovery plans.

6.6.1.2.2 Recovery Team Notification

Once a disaster has been declared by the Crisis Management Team, the recovery teams at the operational level, which are

responsible for actually executing the DR plan, need to be promptly notified. This Notification process is described below:

Recovery Team Notification - Generic

It cannot be assumed that all recovery team staff will be on site at the times that a disaster is declared and a decision is taken to activate DR plans.

Notification Actions - Prior to a disaster

1) Ensure that each critical member of the recovery team has a designated deputy.
2) Delegate responsibility for calling out team members to an individual (and deputy) member of the recovery team.
3) Ensure that the security access passwords of each critical recovery team member are held in a file accessible to his deputy (and possibly, via a member of the ERT, to designated third parties).
4) Develop a contact list detailing both on site and offsite contact details of all members of the recovery team and their deputies.
5) It is recognised that in the context of KSA privacy is highly valued and consequently staff may be unwilling to make their offsite numbers available. In these cases the provision of a pager and/or dedicated disaster mobile phone must be considered.
6) Agree with the facilities team at the disaster recovery site(s) what notification procedures will be followed so that they are not taken unawares by the arrival of relocated staff at the DR site.

Once the decision has been taken to activate the DR Plan -

- The Manager, Business Continuity will delegate his staff to activate the Recovery Team Contact List. They will contact the head of each recovery team or his deputy (with the exception of those who are on the ERT) and brief him on the disaster and the decision to activate recovery plans. In the event that both the head of a team and his deputy are incapacitated the Manager, Business Continuity will assign a member of the Business Continuity function to act as temporary recovery team head until the ERT can appoint a permanent replacement.

- The designated recovery team member with responsibility for internal team communications will call out his colleagues.

6.6.1.2.3 Stakeholder Notification

The plan, besides including notification procedures for the technical and business teams, should address notification to the all relevant agencies/people like CITC (i.e., the Stakeholder Notification Plan). Stakeholder notification involves communicating the right message about the disaster to all relevant agencies/people in the right manner and at the right time.

The 'who', 'how', 'what' and 'when' of communicating to key stakeholders is summarized here below.

The 'who' will cover -

- External regulatory or industry disaster management bodies who need to be notified of the nature and impact of the disaster.
- Clients and other organisations who have contractual arrangements which are either financially or politically significant
- Critical business shareholders
- Those Board members who are not directly involved on the Crisis Management Team
- Possibly representatives of the staff, especially if the disaster has resulted in loss of life

The 'how' should identify which members of the Crisis Management Team, Emergency Response Team, or Communications Team will communicate with individual stakeholders and what type of format should be used for communicating with each of the key stakeholders.

The 'what' will, to a very large extent, be determined based on the stakeholder being informed. The regulator for example may wish to know information such as:

- Which locations have been impacted by the disaster?
- Which services are currently unavailable? How long they have been unavailable for and when it is anticipated the services will be restored?

- What, if any, regulations have, or are anticipated to be contravened by the outage?
- Details of any impact on other telecommunications operators?
- What assistance could be required from other operators?
- What it is intended to do to make sure that the disaster is not repeated?

The 'what' will also be influenced by the image that the organisation wishes to project

The when will focus upon how soon after the declaration of a disaster should the Stakeholder Management Plan be invoked? Whilst the answer to this question will be dependent upon the nature of the disaster, the probable answer, at least in relation to operator specific disasters is that it should be involved after the ERT has decided upon a recovery strategy and when a "ball park" estimate of service resumption time is available.
The other aspect of "the when" is the frequency of communication. This again is stakeholder specific.

6.6.2 Development of Written DR Plans

Once the Crisis Management Organization and Process have been established, the next step is the development of written DR Plans.

The plan should document strategies and procedures to maintain, resume, and recover critical business functions and processes and should include procedures to execute the plan's priorities for critical vs. non-critical functions, services and processes.

The provision of comprehensive DR for an operator will necessitate the production of several levels of DR Plan notably:

- Application level DR Plan addressing the failure of an application due to, for example, failures in application specific hardware.
- Facilities level DR Plan addressing facilities level failures which render the infrastructure (buildings, power, air handling etc) that supports the operator's corporate systems unavailable. This plan will include evacuation plans for the buildings.
- Network operation DR Plan addressing failures in the network itself or the facilities underpinning it such as Mobile Switching Centres or Base station Controllers.
- Business Unit Recovery Plans designed to allow each business unit to recover from disasters that may vary in magnitude from the major disasters that impact the whole corporate entity.

- Location Recovery Plans designed for critical locations that may have multiple Business Units from diverse functions. These plans would allow coordination of the restoration of business activities across the various Business Units and facilities at the critical location with minimum confusion, disruption and cost.
- Organisational level DR Plan addressing the unavailability or limited availability of staff or functions as a result for example of quarantine procedures consequent on a re-occurrence of the SARS virus.
- Work area level DR Plan. These are lower level plans that address situations where an individual work area may be rendered unavailable.

The overall plan has to be in line with the guidelines of the Telecommunications industry regulator and National Disaster Plan.

6.6.3 Testing and Maintenance

All DR testing inherently entails risk. Unforeseen problems could occur when switching from the Production Environment to the Disaster Recovery environment. Resources that are involved on the test are not immediately available to assist in resolving production problems; the DR environment may not be stable or may not even come up (especially if 'change management' and 'Disaster Recovery' have nor been de facto integrated).

The following sections will look at the following aspects of DR plan testing –

1. Test Planning
2. Test Execution
3. Analyzing and Reporting Test Results
4. Plan Maintenance

6.6.3.1 Test Planning

6.6.3.1.1 Objectives and Scope

As mentioned above DR tests entail risks.

It is therefore advised that serious consideration be given by operators to the setting up of a dedicated team DRTET (DR Test Execution Team) to exercise the DR Plans in conjunction with the Business, Network and Computer operations.

Crisis Management Team should clearly define, at a strategic level, what functions, systems, or processes are going to be tested and what will constitute a successful test.

The DRTET will refine these down to a lower operational level. The objective of a testing program is to ensure that the

DR Plan remains accurate, relevant, and operable under adverse conditions.

Achieving the following objectives provides progressive levels of assurance and confidence in the plan. At a minimum, a clearly stated testing plan should:

- Be based on a risk minimization philosophy
- The test plan should be developed to allow back out at multiple points in the execution process (go/no-go points). These points will be both formal (incorporated in the plan) and at the discretion of the DRTET Manager
- Gradually increase the complexity, level of participation, functions, and physical locations involved;
- Demonstrate a variety of management and response proficiencies, under simulated crisis conditions, progressively involving more resources and participants;
- Uncover inadequacies, so that configurations and procedures can be corrected;
- Consider deviating from the test script to interject unplanned events, such as the loss of key individuals or services
- Eventually running production for a significant length of time from the DR site

6.6.3.1.2 Types of Testing

Testing methods vary from minimum preparation and resources to the most complex. Each bears its own characteristics, objectives, and benefits. The type of testing employed by an operator should be determined by, among other things, its age and experience with DR planning, size, complexity, and nature of its business.

Examples of testing methods in order of increasing complexity include:

Orientation/Walk-through

An orientation/walk-through is the most basic type of test. Its primary objective is to ensure that critical personnel from all areas are familiar with the DR Plan. It is characterized by:

- Discussion about the DR Plan in a conference room or small group setting;

- Individual and team training; and
- Clarification and highlighting of critical plan elements.

Tabletop/Mini-drill

A tabletop/mini-drill is somewhat more involved than an orientation/walk-through because a specific event scenario is considered and the DR plan applied to it. It includes:

- Practice and validation of specific functional response capability;
- Focus on demonstration of knowledge and skills, as well as team interaction and decision-making capability;
- Role playing with simulated response at alternate locations/facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment;
- Mobilization of all or some of the crisis management/response team to practice proper coordination
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan
- The facilitator introducing complicating factors to ensure that each team is fully capable of adopting a flexible approach to problems that may be encountered in a disaster.

Two types of scenario based tabletop exercise are recommended.

In the first exercise all business units that would be involved in an actual recovery from a real disaster similar to the scenario, send teams to the location of the tabletop exercise which is run by an external facilitator

- The facilitators will outline the circumstances associated with the disaster scenarios. They then cover the planned activities addressed by the DR Plan. The activities will be separated into broad categories like:

  - Procedural aspects of invocation and recovery
  - Logistics of relocation
  - Internal and External Communications
  - System Recovery- Business Critical Applications
  - Transition to full functional operations

- Implications of long term running production from DR centre
- Resumption of services from Head Office

- Each of the resource teams will consider the categories from a business and staffing perspective in the 10 minutes following the facilitators outline.
- They will then provide feedback to the workshop as regards their concerns with the execution of that part of the plan.
- To make the exercise more realistic and interesting, the facilitator will throw in complicating factors such as key technical support staff injured in accident whilst traveling to recovery centre
- The exercise will finish with an overview by each of the teams outlining what they have learnt and what actions they are going to take.
- Post the exercise the facilitators will create a summary report which will be issued to all attendees

The second type of tabletop exercise is again predicated on a disaster scenario –

- A dedicated war room is made available for the exercise. The exercise is coordinated by a facilitator.
- It will commence with a phone call from the disaster site to the incident management team representative (who will be, for the purpose of the exercise, located in the designated war room) reporting the simulated disaster.
- The incident management representative will (theoretically) escalate the issue through the crisis management process until a formal disaster is declared and the DR plans are activated.
- Key staff from business units, facilities, HR and infrastructure will assemble in the “war room” along with observers and a recorder.
- The recovery process will be followed as per the plans except that it will be contained within the war room and each team will outline what it would do as each stage of the process is reached. Some actions such as evacuating buildings will be theoretical to minimize disruption to processing.

- The exercise will continue until completion of the recovery process.
- As with the first type of tabletop exercise, the facilitator will change the scenario "in running", in order to verify the flexibility of the DR execution process and establish the ability of key players to act under pressure.
- After the completion of the exercise a post test review will take place to highlight exposures in the plans

Functional Testing

Functional testing is the first type that involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the DR Plan. It includes:

- Demonstration of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning;
- Actual or simulated response to alternate locations or facilities using actual communications capabilities;
- Mobilization of personnel and resources at varied geographical sites; and
- Varying degrees of actual, as opposed to simulated, notification and resource mobilization.

Functional test should be carried out in relation to plans of business units that use the internal, non customer facing systems such as billing or customer service so as to minimize disruption to the customer base.

- The aim the test is to prove key logistics components of the recovery plan, such as the relocation of staff, connectivity from recovery area to the "production" centre (or if the test scenario dictates, the systems at the disaster recovery centre), security controls etc.
- The test, which may be held over an extended duration, involves business unit or work area sized units and is usually held at off-peak hours or at times of low activity.
- Metrics such as transit times and bottlenecks should be recorded. These can be adjusted to account for increased traffic and volumes of staff to be moved.
- Once at the recovery site, the staff should attempt to log on to the production systems to prove connectivity.

They should also prove that they have connectivity to the disaster recovery centre and that they can undertake work on the DR copy of the applications that they normally use.

- The test should involve infrastructure components such as security at the recovery sites.

Full-scale Testing

Full-scale testing is the most comprehensive type of test. In a full-scale test, the organization implements all or portions of its DR Plan by processing data and transactions using back-up media at the recovery site. It involves:

- Validation of crisis response functions;
- Demonstration of knowledge and skills, as well as management response and decision-making capability;
- On-the-scene execution of coordination and decision-making roles;
- Actual, as opposed to simulated, notifications, mobilization of resources, and communication of decisions;
- A realistic scenario is developed which would cause significant disruption to services.
- All affected business units and third party vendors are fully involved in the test planning process. End user customers may be alerted to the possibility of disruption or degraded performance on the days of the test.
- On the agreed date, DR Plans are activated and the relevant business activity (including affected staff) is transferred to the disaster recovery locations.
- Production service is re-started from these locations and run from them for an agreed period (usually 2 or more days). Production is then switched back to the primary site.
- Depending on the scenario chosen for the exercise some downtime may be incurred. However the exercise is a learning process and this may consequently be reduced in an actual disaster.

In addition to the above tests, the operator should test the resilience of the critical infrastructure on which the systems depend. At very least:

- Twice a year the power should be switched to generators which should be run for at least 24 hours
- The environmental monitoring system should be tested after consultation with the vendor to identify any single points of failure
- The battery components of the UPS should be tested annually in consultation with the vendor
- PDU breakers should be tested/replaced periodically to prove the capabilities of the equipment and staff.

6.6.3.1.3 Test Execution

Testing requires some centralized coordination, often by a dedicated DR Test Execution Team (DRTET). The team or coordinator is responsible for overseeing the accomplishment of targeted objectives and following up with the appropriate areas on the results of the test. Generally, it is advisable to have the maximum number of personnel that will be involved in implementing the DR Plan also participate in the test. This participation increases awareness, buy-in, and ownership in achieving successful DR Plan implementation. It is also advisable to rotate personnel involved in testing in order to prepare for the loss of key individuals, both during or in the aftermath of a disaster, and as a result of retirements, promotions, terminations, resignations, or re-assignment of responsibilities. The involvement and oversight of independent staff such as auditors will help to ensure the validity of the testing process and the accuracy of the reporting.

Tests should be conducted at a frequency appropriate to the size of the network and customer base and number of business units to be exercised. In the long term, at minimum, annual exercises are advised. Some operators may consider more frequent tests appropriate.

6.6.3.1.4 Analyzing and Reporting Test Results

A useful test can only be achieved if the test results are analyzed and compared against stated objectives, and acted upon. The DRTET Manager should report the test results and the resolution of any problems to the participating functions. A summary should be provided to the board level sponsor of

Disaster Recovery management. Management reports should consider all the test results. Test analyses should include:

- An assessment of whether the test objectives were completed;
- An assessment of the validity of test data processed;
- Corrective action plans to address problems encountered;
- A description of any gaps between the DR Plan and actual test results;
- Proposed modifications to the DR Plan; and
- Recommendations for future tests

6.6.3.1.5 Plan Maintenance

6.6.3.1.5.1 Updating the Plan

The plan should be reviewed by the Business Continuity Function and the business unit head periodically. As part of that review process, the assigned Business Continuity Coordinator should contact business unit managers at regular intervals to assess the nature and scope of any changes to the institution's business, structure, systems, or personnel. It is to be expected that some changes will have occurred since the last plan update. All such organizational changes should be analyzed to determine how they may affect the existing DR plan, and what revisions to the plan may be necessary to accommodate these changes. The Business Continuity Function should ensure the revised DR Plan is distributed throughout the organization

6.6.3.1.5.2 Plan Review Process

Procedures need to be put in place to review the DR Plan periodically.
The DR plan review must include representatives of all groupings, whether internal, or third party that are involved in the recovery process. If possible the individuals involved in the review process should be individuals who have been involved in actual plan invocations or in DR tests.

The review must identify any changes in systems, equipment, infrastructure, organizational structure and key personnel that have taken place since the last test or invocation of the plan. It must also identify any significant changes to traffic volumes (peak and average) that have occurred and which may impinge on the ability of the system to be restored.

6.7 Training of Employees for BC/DR

Training of employees should, at the minimum, include –

1. Active program of evacuation drills. This includes:

    - Agree functional responsibility for building evacuation
    - Define roles and responsibilities
    - Appoint evacuation manager, floor evacuation wardens, fire wardens, first aid personnel - train on their roles in an evacuation and brief on basic BC/DR concepts including threat analysis.
    - Ensure procedures are in place for evacuation of disadvantaged (disabled, pregnant, older) employees via personal evacuation plans and visitors
    - Issue pocket sized evacuation plans which can also mention potential threats
    - Train up security staff on how to deal with specific threats such as bomb alerts
    - Undertake program of evacuation drills

2. In depth senior and middle management training on BC/DR, with

    - initial modules addressing risk reporting and corporate governance
    - next modules emphasizing the potential exposures (threat Analysis)to the business that exist from both a practical and financial perspective
    - further modules showing what pro active mitigation actions can be taken.
    - final section on the need for and cost justification of BC/DR planning

3. Training for rest of the organization after prioritizing the business critical functions of the organization

    - Develop and institute BC/DR awareness programs at a business unit level.
    - Ensure that each business unit appoints its own BC/DR representative. They will be needed in the BC/DR planning process and can receive more in depth training so they themselves can provide ongoing refresher training to their unit.
    - Include BC/DR awareness training as part of the company's induction program
    - Place DR manuals for each business unit on its shared network drive/LAN to allow easy reference by all employees

7 TABLE OF CONTENTS FOR DR PLANS

The provision of comprehensive DR for an operator will necessitate the production of several levels of DR Plan notably:

- Application level DR Plan addressing the failure of an application due to, for example, failures in application specific hardware.
- Facilities level DR Plan addressing facilities level failures which render the infrastructure (buildings, power, air handling etc) that supports the operator's corporate systems unavailable. This plan will include evacuation plans for the buildings.
- Network operation DR Plan addressing failures in the network itself or the facilities underpinning it such as Mobile Switching Centres or Base station Controllers.
- Business Unit Recovery Plans designed to allow each business unit to recover from disasters that may vary in magnitude from the major disasters that impact the whole corporate entity.
- Location Recovery Plans designed for critical locations that may have multiple Business Units from diverse functions. These plans would allow coordination of the restoration of business activities across the various Business Units and facilities at the critical location with minimum confusion, disruption and cost.
- Organisational level DR Plan addressing the unavailability or limited availability of staff or functions as a result for example of quarantine procedures consequent on a re-occurrence of the SARS virus.
- Work area level DR Plan. These are lower level plans that address situations where an individual work area may be rendered unavailable.

It is important to note that each DR Plan is different – the mission critical processes, procedures, and functions captured in the DR planning process are specific to each FBP's specific business functions, infrastructure and organization. There may be similarities within same telecommunications service providers like fixed service providers or mobile service providers, but each organization is unique, and as such will have a unique DR Plan.

From a generic perspective the basics of the plans should include**:**

Table of Contents for the DR Plans to be submitted to CITC
1. Introduction, Concept of Operations and Crisis Organization 1.1. **The Introduction** section provides the type and location of information contained in the plan. Generally, the section includes

1.1.1. **Purpose of the specific DR Plan** – this section establishes the reason for developing the plan and defines the plan objectives

1.1.2. **Applicability within the organization** - This subsection documents the parts of the organization impacted by the plan. All related plans that support or are supported by this plan should be identified and their relationship should be described. These related plans should be included as appendices

1.1.3. **Scope** - issues, situations, and conditions addressed and not addressed in the plan, including key assumptions (The scope should address any assumptions made in the plan, such as the assumption that all key personnel would be available in an emergency). The section identifies the target system and the locations covered by the plan. For example, the plan may not address short-term disruptions expected to last fewer than for hours.

1.1.4. **Record of changes** made to the document – the plan is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to the plan should be recorded in this section.

1.1.5. **Definitions** – this section provides definitions for key terminology

1.2. **Concept of Operations (System Description)** – this section includes a general description of the business/IT systems covered in the plan. The description should include the system architecture, location(s), and any other technical consideration.

1.3. **Recovery Organization** (or Crisis Management Organization)

1.3.1. **Overall organization structure of recovery teams** – includes the hierarchy and coordination mechanisms among the teams

1.3.2. **Recovery teams responsibilities** – this section provides an overview of recovery team member roles and responsibilities both pre-disaster and during a disaster. Teams and team members should be designated for specific response and recovery roles during DR plan activation. Roles should be assigned to team positions rather than to a specific individual.

2. **Notification/Activation Process Phase** - defines the initial actions taken once a system disruption or emergency has been detected or appears to be imminent. This phase includes activities to notify recovery personnel, assess system damage, and implement the plan.

2.1. **Notification Procedures** - An event may occur with or without prior notice. Notification procedures should be documented in the plan for both types of situation. The procedures should describe the methods used to notify recovery personnel during business and non-business hours. The notification strategy should define procedures to be followed in the event that specific personnel cannot be contacted. Personnel to be notified should be clearly identified in the contact lists appended to the plan. This list should identify personnel by their

team position, name, and contact information. For all key positions in the notification chain, a fully trained deputy, and emergency resource should be identified. They will be notified in that order should the primary resource be unreachable.

2.2. **Damage Assessment** - To determine how the plan will be implemented following an emergency, it is essential to assess the nature and extent of the damage to the system. The team should look at following areas –

2.2.1. Cause of the emergency or disruption

2.2.2. Potential for additional disruptions/damage

2.2.3. Area affected

2.2.4. Status of physical infrastructure and network connectivity

2.2.5. Inventory status

2.2.6. Type of damage

2.2.7. Items to be replaced

2.2.8. Estimated time to restore services

2.3. **Plan Activation** – Once the damage has been assessed, the decision to activate DR plan and the following recovery activities happen as per the crisis management process of the organization that includes –

2.3.1. **Escalation plan** from the team that first acts on any incident to the team at the top of the recovery teams' hierarchy – including the identification of facilities to be used for communication

2.3.2. **Decision points** to check if the incident needs to be escalated or can be handled within the recovery objectives of the affected systems, decision regarding which recovery plans to activate, decision regarding running production (IT data centre) from the DR site, and decision regarding switching back to original production centre (if it still exists)

2.3.3. **Disaster Declaration** – This section documents the individuals having the authority to declare a disaster, the disaster declaration process and procedures, and guidelines and considerations in reaching the disaster declaration decision

2.3.4. **Evacuation** - Should the buildings be damaged with potential risk to staff, an evacuation plan should be activated with the primary objective of removing staff out of potential harm

Final activation criteria depend on the particular organization, including safety of personnel, extent of damage, criticality of system, anticipated duration of disruption etc. The appropriate teams should be notified of updated information and planned response to the situation. The type of information to be relayed to those being notified should be documented in the plan (example, the information may include the nature of emergency, loss of life or injuries, damage estimates, location details for convening a quick meeting, response and recovery details, instructions for further notification to other teams etc).

2.4. **Stakeholder Notification Plan** also needs to be activated at this stage (refer to Section 6.6.1.2.3 in the Annexure 6 "Detailed DR Plan Creation Methodology"). Points-of-contact of all stakeholders to be notified should be listed in the appendix to the plan

3. **Recovery Process** - Recovery phase activities focus on procedures to execute temporary processing capabilities, repair damage to the original system, and restore operational capabilities at the original or new facility. At the completion of the Recovery Phase, the system will be operational and performing the functions designated in the plan. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site.

3.1. **Recovery Strategy** – this section outlines the recovery strategy for the systems covered under this plan. The outage impact(s) and allowable outage times determined during Business Impact Analysis (BIA), lead to the establishment of recovery objectives (RTO/RPO) that enable the development and prioritization of recovery strategies for the various business processes and corresponding resources/facilities. The components of the recovery strategy include -

3.1.1. **Backup methods** - System data should be backed up regularly. Policies should specify the frequency of backups (e.g., mirroring, daily or weekly, incremental or full), based on data criticality, the time to restore the data under the worst case scenario in order to meet the system Recovery Time Objective (RTO) and Recovery Point Objective (RPO), and the frequency with which new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite

3.1.2. **Alternate sites** - The plan must include a strategy to recover and perform system operations at an alternate facility for an extended period. Sites may be identified as cold sites, hot sites, mobile sites and mirrored sites based on their operational readiness.

3.1.3. **Equipment replacement** - When primary site is damaged/unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. Three basic strategies exist to prepare for equipment replacement – vendor agreements, keeping equipment inventory, and using existing compatible equipment.

3.2. **Sequence of Recovery Activities** - recovery procedures should reflect system priorities identified in the BIA or the corporate priorities at the time of the disaster. The sequence of activities should reflect the system's allowable outage time to avoid significant impacts to related systems and their application. Procedures should be written in a stepwise, sequential format so system components may be restored in a logical manner. Procedures should designate the appropriate team or team members to coordinate shipment of equipment, data, and vital records. References to applicable appendices, such as equipment

lists or vendor contact information, should be made in the plan where necessary.

3.3. **Recovery Procedures** - Procedures should be assigned to the appropriate recovery team and typically address the following actions:

- Obtaining authorization to access damaged facilities and/or geographic area
- Obtaining necessary office supplies and work space
- Obtaining and installing necessary hardware components
- Obtaining and loading backup media
- Restoring critical operating system and application software
- Restoring system data
- Testing system functionality including security controls
- Connecting system to network or other external systems
- Operating alternate equipment successfully

4. **Reconstitution Phase** - recovery activities are terminated and normal operations are transferred back to the organization's facility. If the original facility is unrecoverable, the activities in this phase can also be applied to preparing a new facility to support system processing requirements. Once the original or new site is restored to the level that it can support the business function and its normal processes, the system may be transitioned back to the original or to the new site. Until the primary system is restored and tested, the backup system should continue to be operated. The Reconstitution Phase should specify teams responsible for restoring or replacing both the site and the business system. The following major activities occur in this phase:

- Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies
- Installing system hardware, software, and firmware. This activity should include detailed restoration procedures similar to those followed in the Recovery Phase
- Establishing connectivity and interfaces with network components and external systems
- Testing system operations to ensure full functionality
- Backing up operational data on the DR system and uploading to restored system
- Shutting down the backup system
- Terminating recovery operations
- Securing, removing, and/or relocating all sensitive materials at the backup site

- Arranging for recovery personnel to return to the original facility

5. **Plan Appendices** - DR plan appendices provide key details not contained in the main body of the plan. The appendices should reflect the specific technical, operational, and management DR requirements of the given system. Common DR plan appendices include the following:
    - Distribution list for the DR plan
    - Contact information for DR planning team personnel
    - Disaster Recovery team call list
    - Vendor contact information, including offsite storage and alternate site point-of-contacts
    - Standard operating procedures and checklists for system recovery or processes
    - Equipment and system requirements lists of the hardware, software, firmware, and other resources required to support system operations. Details should be provided for each entry, including model or version number, specifications, and quantity
    - Vendor SLAs and other vital records
    - Description of, and directions to, the alternate site
    - The BIA (Business Impact Analysis), conducted during the planning phases, contains valuable information about the interrelationships, risks, prioritization, and impacts to each element of the system. The BIA should be included as an appendix for reference should the plan be activated
    - Preventive procedures implemented for higher Disaster Preparedness
    - Key customer notification list
    - Description of the audit process for the DR plan

8 DR RESPONSIBILITIES CHART

The following figures outline the responsibilities of the various players involved in Telecommunications disaster management:

- Figure 4 – Overall governance structure
- Figure 5 – Responsibilities chart for disaster preparedness in ICT sector
- Figure 6 – Responsibilities chart for DR planning in ICT sector
- Figure 7 – Responsibilities chart for DR
- Figure 8 – Responsibilities Chart for Emergency Communications Support by ICT Sector
- Figure 9 - Responsibilities of the Various Telecom Players and Interaction with Other Agencies

Figure 4: Governance Structure for DR Management in ICT Sector

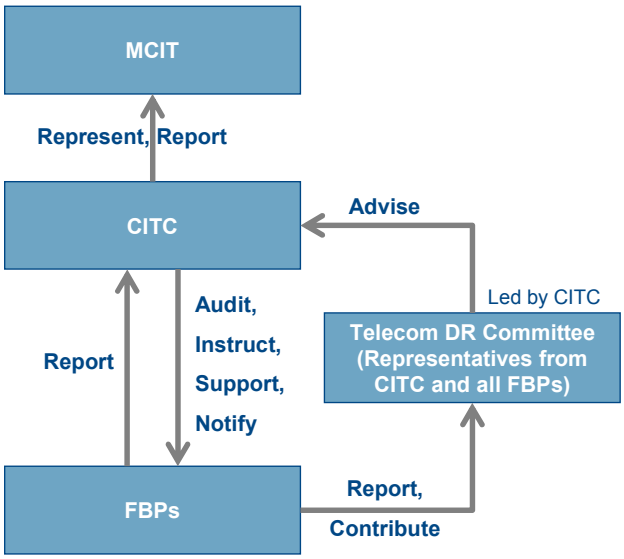


Figure 5: Responsibilities Chart for Disaster Preparedness in ICT Sector

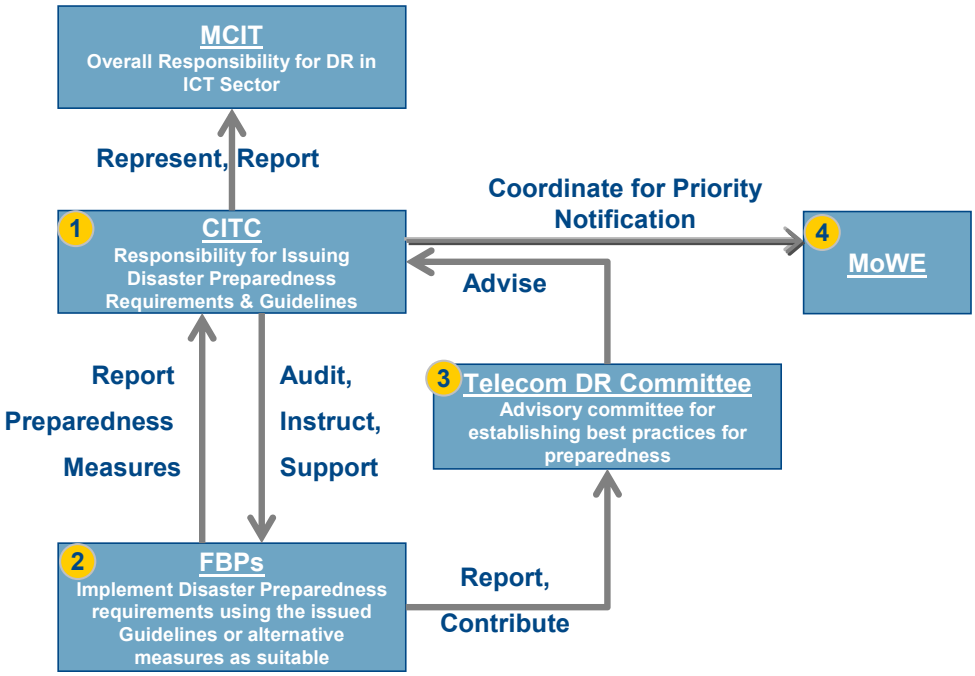


Figure 6: Responsibilities Chart for DR Planning in ICT Sector

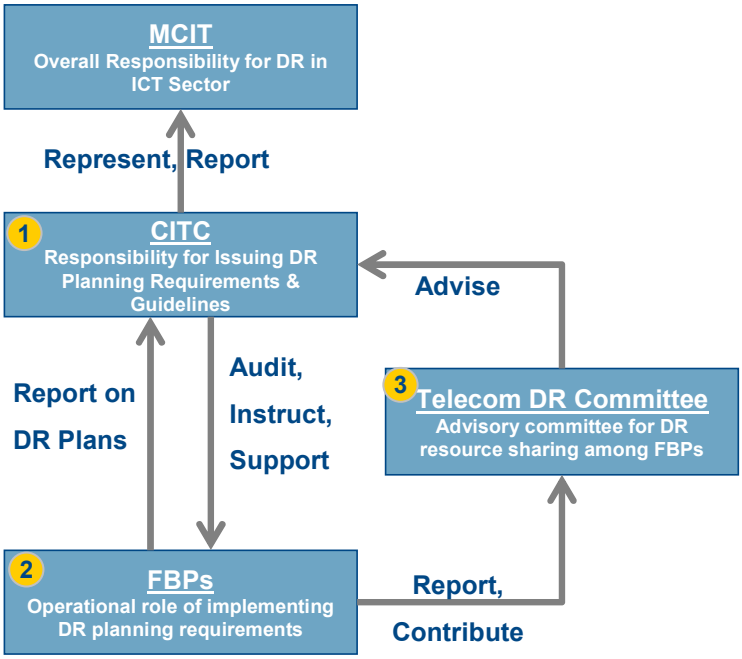


Figure 7: Responsibilities Chart for Emergency Communications Support by ICT Sector

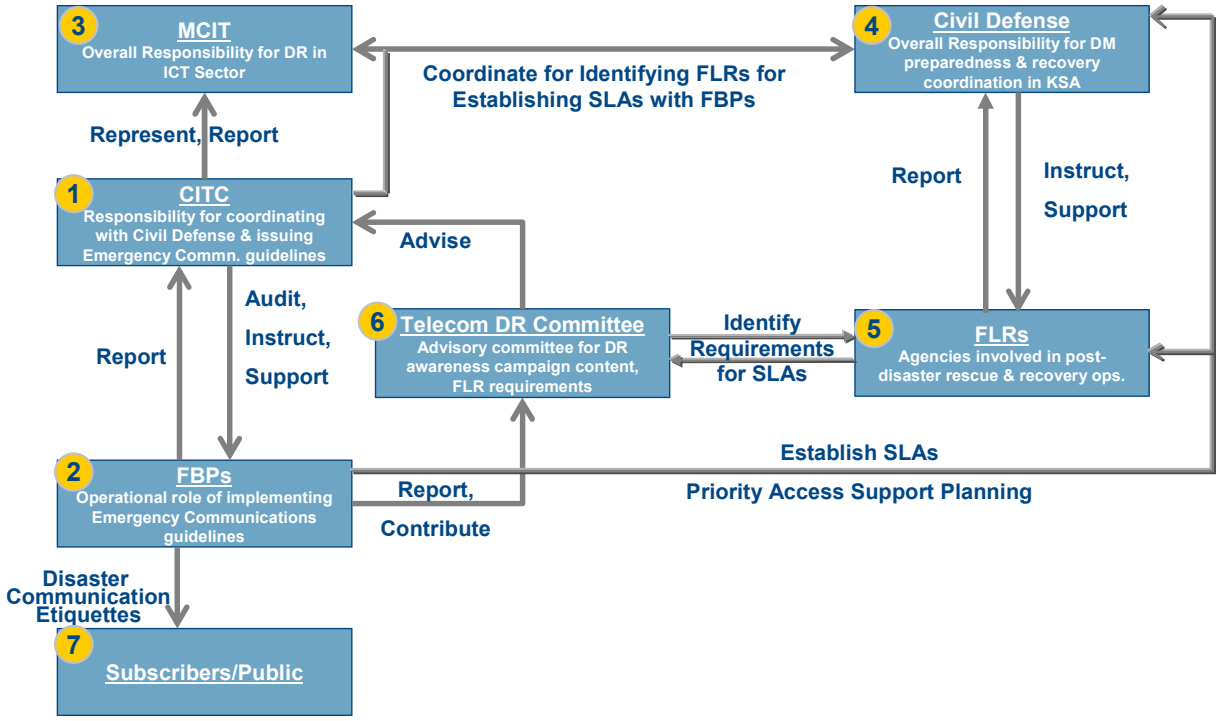


Figure 8: Responsibilities in the Case of a Disaster

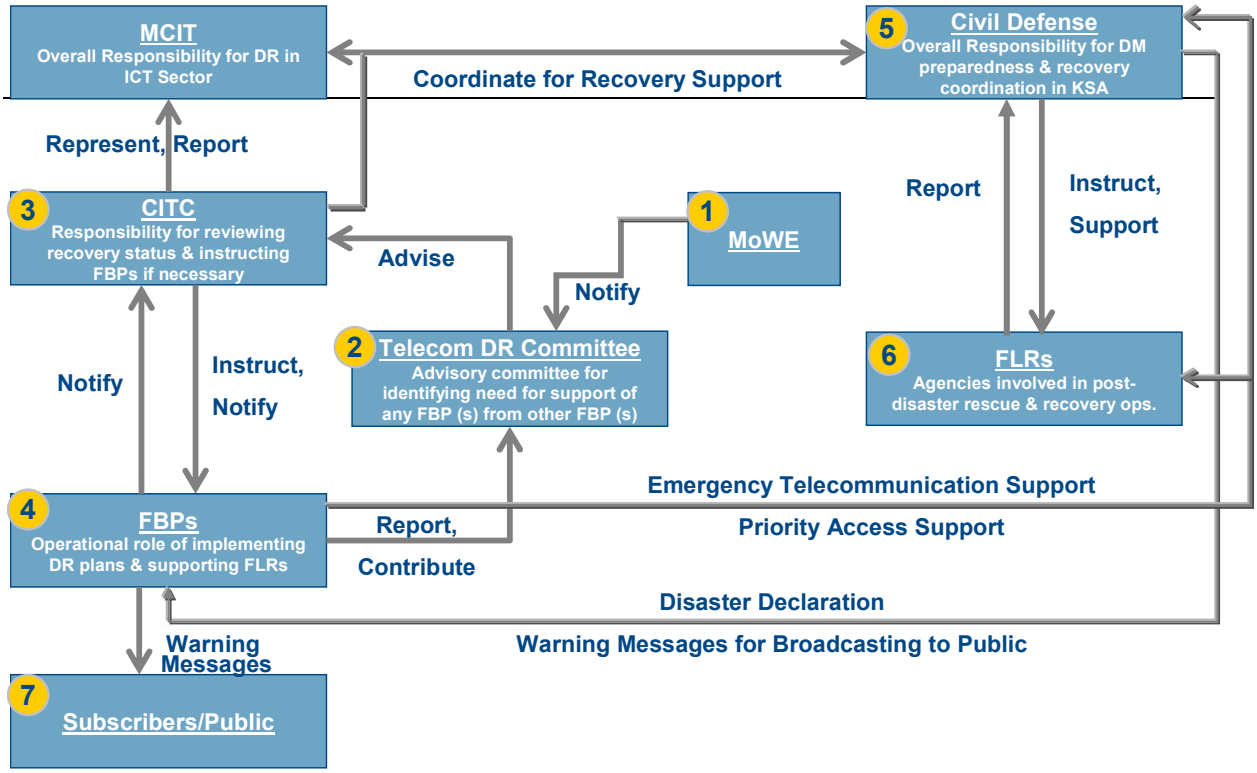


Figure 9: Responsibilities of the Various Telecom Players and Interaction with Other Agencies