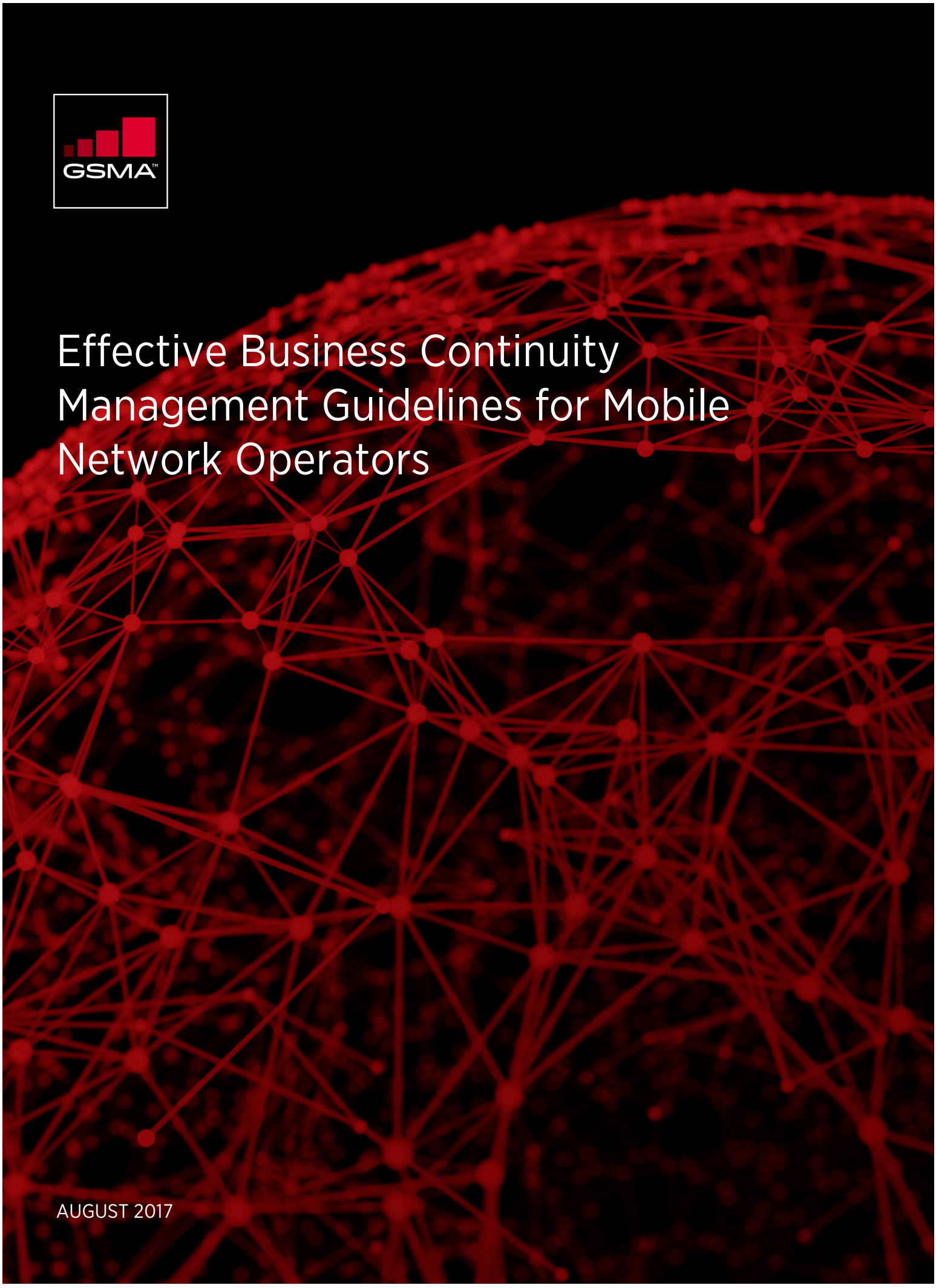


Effective Business Continuity Management Guidelines for Mobile Network Operators

AUGUST 2017

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with almost 300 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai, Mobile World Congress Americas and the Mobile 360 Series of conferences.

For more information, please visit the GSMA corporate website at www.gsma.com
Follow the GSMA on Twitter: @GSMA

The GSMA Disaster Response programme aims to strengthen access to communications and information for those affected by crisis in order to reduce loss of life and positively contribute to humanitarian response. We work to drive the creation and adoption of coordinated, impactful solutions and practices that leverage the ubiquity of the mobile technology under the umbrella of the Humanitarian Connectivity Charter

Learn more at www.gsma.com/disasterresponse
Or contact us at disasterresponse@gsma.com
Follow GSMA Mobile for Development on
Twitter: @GSMAm4d

This document is an output from a project co-funded by UK aid from the UK Government. The views expressed do not necessarily reflect the UK Government's official policies.

Contents

Introduction

In a disaster situation, one of the most important resources is the availability of information (ideally verifiable information) that operators, agencies tasked with response, and the general populace can use to make informed decisions. Information needs to be available, accessible and symmetric in order to be effective; this means that where possible and appropriate, all agencies and organisations should provide critical information so as to ensure that those preparing and responding have appropriate information in a timely way.

As the frequency and magnitude of disasters continues to grow, demand for mobile services in these contexts will only rise. Mobile operators have a critical role to play in facilitating access to information, life-enhancing services, and reconnecting family members. With the need to provide such support to emergency and relief services, building resilience of the mobile network infrastructure and having robust business continuity plans have become key requirements for MNOs.

Preparedness is a corner stone of disaster resilience, yet for every $7 spent in response, only $1 is spent on preparedness activities. It's for this reason that the GSMA, through its Disaster Response Programme, highlights the importance of building comprehensive BCM strategies and capacity, and through the Humanitarian Connectivity Charter advocates that "MNOs work to develop a comprehensive disaster-preparedness and/or business continuity management (BCM) plan". The document below outlines the features of a robust BCM plan and provides practical step-by-step guidance on how to build capacity in this important area.

What is Business Continuity Management?

Business Continuity Management (BCM), as defined by the ISO 22301:2012 standard[1], is the "holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realized, might cause. It is the provision of a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

The primary objective of Business Continuity Management is to allow the Executive of the MNO to continue to manage business operations under adverse conditions, by the

[1] ISO 22301 is a management systems standard for BCM which can be used by organisations of all sizes and types. (www.iso.org)

introduction of appropriate resilience strategies, recovery objectives, business continuity, operational risk management considerations and crisis management plans.

- It is about preparing an organisation to deal with disruptive incidents that might otherwise prevent it from achieving its objectives. Any incident, large or small, natural, accidental or deliberate has the potential to cause major disruption to the organisation's operations and its ability to deliver products and services. However, implementing BCM ahead of time, rather than waiting for this to happen will enable the organisation resume operations before unacceptable levels of impact arise. BCM is not complicated, it involves:
    - Identifying organisations key products and services
    - Identifying the prioritized activities resources required to deliver them;
    - Evaluating the threats to these activities and their dependencies
    - Putting arrangements in place to resume these activities following an incident
    - Making sure that these arrangements will be effective in all circumstances

- It is about identifying and protecting the fundamental components and assets of mobile network operators (such as staff, data, technology infrastructure and premises) and planning for how to retain and recover these elements as quickly as possible if an incident occurs. A mobile operators network has all components interrelated to each other therefore it demands proactive response and best model for Business Continuity. Creating more resilient mobile networks to disaster scenarios does require the development of flexible processes which can adapt to the rapidly changing circumstances, the training of staff in these processes and their ability to respond to disasters.

- It is about working with external agencies to provide both support to key emergency services and to make sure essential resources can be sourced for the rebuilding and running of the network.

Purpose

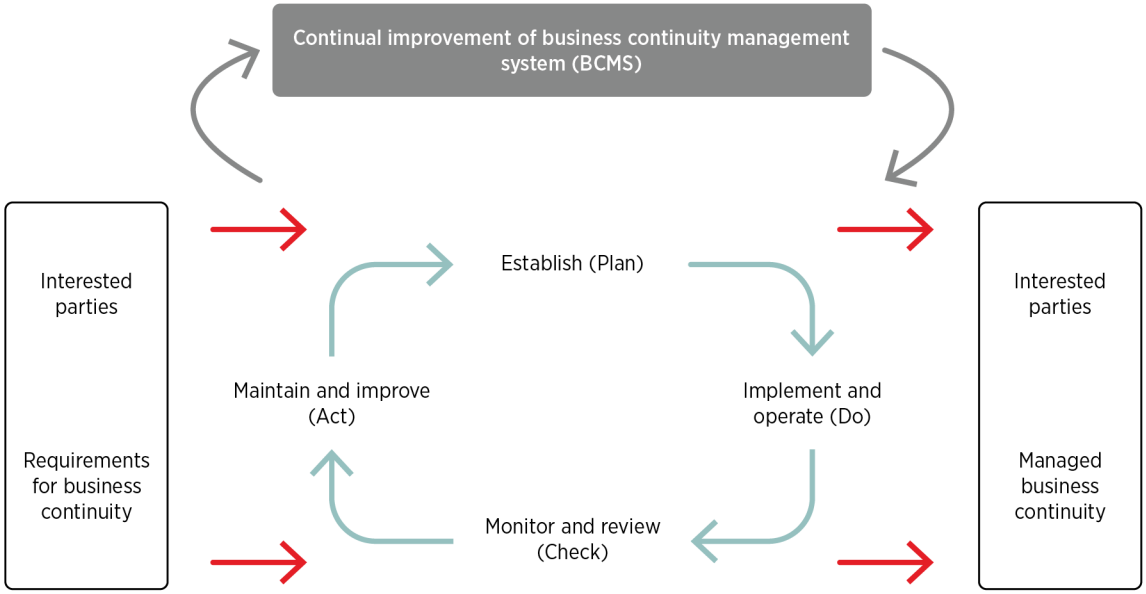
This Business Continuity Management (BCM) guidance document will assist Mobile Network Operators (MNO) in fulfilling their business continuity management obligations. The toolkit is aligned with industry standards and the GSMA Disaster Response - Business Continuity Management Report (2016).

About this document

This guideline document is based on the Plan, Do, Check, Act (PDCA) model for planning, establishing, implementing, operating, monitoring, reviewing, maintaining and continually improving the effectiveness of business continuity preparedness across the operating environment.

FIGURE 1

Plan Do Check Act (PDCA) Model for Business Continuity Management ISO22313[2]



It provides guidance and supporting material that can help in the development of business continuity policy, plans and processes, exercising of those plans as a means of predetermining the course of action for specific mobile operator preparedness levels.

[2] ISO 22313:2012 Societal security - Business continuity management systems - Guidance for business continuity management systems.

Phase 1: Establish (Plan)

1.1 Introduction

For MNOs about to take their first steps in BCM, a good place to start is the Plan phase. Here, they can establish business continuity policy, objectives, scope, processes and procedures that will help deliver results in accordance with the mobile operator's overall business objectives. The information below are designed to support the development of a system suitable for most operating environments irrespective of the location or size.

1.2 Understanding the mobile operator context

Many organisations including MNOs are required to analyse and justify the cost of deploying Business Continuity Plans for both tangible and intangible impacts. Intangible impacts like reputation and consequent loss of customers, market share degradation, negative publicity, staff morale and retention cannot easily be assessed in financial terms in order to build justification for the programme. The Internal and external issues that may affect the business continuity programme can be articulated by determining the context of the mobile operator environment. These issues should then be taken into account when justifying (as part of business case), establishing, implementing and maintaining the mobile operator's BC programme. It should also articulate its objectives, including those concerned with business continuity, defining the external and internal factors that create the uncertainty that gives rise to risk, and define the purpose of the business continuity programme.

Examples of internal issues:

- Connectivity, e.g. internet failure
- High staff turnover
- Fraud
- Single point of failure for vendors/lack of competence
- Process failure
- Human error

Examples of external issues:

- Attacks on base stations and other infrastructure
- Bomb threats (terrorist attack)
- Civil unrest
- Prevalence of natural disasters (flood, earthquake, volcanoes, tsunamis, etc.)
- Expectations of the wider populace and external parties (Humanitarian agencies, fire service, National Emergency agencies) during a widespread disaster
- Political instability
- Suppliers

1.3 Understand the needs of stakeholders

The expectations and interests of all key stakeholders whether internal or external should be taken into account and documented while managing the business continuity programme.

TABLE 1

Typical list of Interested Parties and their Expectations

Steps	Stakeholders/Interested Party relevant to the BCMS	Requirements of Interested Parties
1.	Customers/subscribers	Uninterrupted telecommunication services, especially during a widespread disaster
2.	Regulator	Service availability and Quality of Service
3.	Staff	Job security and uninterrupted service
4.	Board and Management	Protection of continuous revenue/income earning potential
5.	Government	Help inform the Government and the populace about ensuing disasters and provide the means for reaching out to families and friends caught up in disasters
6.	Humanitarian agencies and emergency services	Reliance on communication to fulfil their front line services in disaster relief
7.	Business partners	Recovery capability that aligns with the MNO

1.4 Legal and regulatory requirements

MNOs should identify the legal and regulatory requirements that are applicable to their organisation's operating environment; this is in relation to the continuity of operations, products and services, as well as the interests of relevant interested parties. This information on legal and regulatory requirements should be kept up to date. MNOs can refer to the *Emergency Mobile Telecommunications: Regulatory Best Practice*[3] as a guide where required.

[3] https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/11/GSMA-Industry-Position_Emergency-Telecoms-Regulation.pdf

1.5 Business Impact Analysis (BIA)

Once the issues that affect the MNO's business continuity programme and the legal and regulatory requirements are determined, these will serve as a good foundation upon which to conduct the BIA (and Continuity Requirements Analysis). The BIA should follow a structured format that will ensure the collection of uniform information across the departments/business units (BUs) of the operator.

It should commence with a list of all departments within the organisation and identify the operations, business support systems and network infrastructure that support/enable their processes or key functions. A schedule of interviews should be agreed with key personnel from each department, with group interviews conducted with two to three representatives of each department at a time. Using the BIA questionnaire as a guide during the interviews, the operator should:

- Agree the key business functions (maximum of five) of the department and discuss an overview of each identified function.
- Determine the unavailability impact ratio of the functional area, network infrastructure and technology systems over different time periods across the following three areas:
    - Financial
    - Legal/regulatory
    - Reputational.

The first time-period across the three impact areas with a 'High' impact rating becomes the Recovery Time Objective (RTO) of that function. The following tables present an example of the impact criteria rationale that can be used to assess the RTO for each process/function.

TABLE 2

Impact Criteria Rationale for RTO determination

Impact	Financial	Legal/Regulatory	Reputational
Low	Below 1% of monthly revenues	Doesn't threaten the operating permit/ license or no litigation threat	Significant impact to less than 1% of customers
Medium	1 - 10% of monthly revenues	May threaten the operating permit/ license or may have litigation threat	Significant impact to 1 - 10% of customers
High	Above 10% of monthly revenues	Seriously threatens the operating permit/ license or serious threat of litigation	Significant impact to above 10% of customers

TABLE 3

How RTO is determined

Business Function 1:					
Business Drivers	4 hours	24 hours	72 hours	1 week	More than 1 week
Financial	Low	Low	Medium	High	High
Regulatory/Legal	NA	NA	Medium	Medium	High
Reputation	Low	Low	Medium	Medium	High

Example: RTO for the above function is 1 week

The rest of the interview uses the BIA Questionnaire to capture the resources (technology, suppliers, people) used by the function in a business-as-usual situation and for recovery over time. The operations, business support systems and network infrastructure also need to be further assessed, using the same principle as above in order to determine which of the network and technology infrastructures are the most critical. For example, an MNO could perform some analysis on historic Call Detail Record (CDR) data to help determine critical cell sites that ought to be given priority for engineering updates in order to make them more resilient.

The completed BIA results should be presented to each department or business unit and to senior management for approval and sign-off.

The BIAs should be reviewed every two years or earlier if there are significant changes within the organisation or in its operating environment. The review activity can be staggered over a one-year period commencing one year after the initial BIA was conducted.

1.6 Risk Assessment

Risk Assessment within BCM is the creation and updating of the risk register by following the steps of risk identification, risk estimation and risk evaluation. It looks at the likelihood and impact of a variety of disaster scenarios that could cause business interruptions (see Disaster Scenarios in section seven of the GSMA Disaster Response BCM Report[4]). Further information on disaster scenarios possible in a particular region can be obtained from government emergency agencies; this may be required by an MNO for risk prioritization and or risk reduction activities. The risk assessment should focus on the critical activities with supporting resources identified at the BIA stage, hence the reason why effective risk assessment can only take place once a BIA has been completed.

[4] http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/05/GSMA_Disaster-Response_Business_Continuity_Management_Report.pdf

To undertake Risk Assessment, the MNO could use the steps set out below using the format of the Risk Register included in this guidance document:

1. Identify and document the vulnerabilities that the operator and the critical functions/processes identified in the BIA are exposed to, the threats (or disaster scenarios) that could exploit those vulnerabilities and the eventual risks to the operator should that happen. The risks could result in loss of revenue, loss of systems (IT and telecommunications infrastructure), reputational damage, loss of utilities, e.g. water, gas or electricity, loss of premises, loss of key suppliers, amongst others.
2. Determine the impact and likelihood of each Risk Rate the severity and probability of the risk.
    - Rate the risks in terms of probability of occurrence - the likelihood that the risk could materialize. The ratings are assigned based on a combination of prior experience and estimation
    - Rate the risks in terms of the impact of the risk materializing. Two types of impact are considered, with the rating based on whichever is higher namely financial impact - the potential cost in terms of loss of revenues - and reputation impact - the impact on stakeholders (customers, employees or shareholders) or brand.
3. Calculate the gross risk rating by averaging the probability and the impact. Then rank the identified risks in order of gross risk level.
4. Identify parties responsible for the risk and its management - a Risk Owner should be nominated. The Risk Owner is the person responsible for the asset or area directly impacted.
5. A list of the key controls in place to manage each risk should be added to the Risk Register. Up to five controls should be listed in the Risk Register for each risk. The control information should include some detail regarding the controls, such as the control type (preventative or detective) and whether they have been the subject of independent review. It should be noted that that the controls in place are not necessarily implemented to manage a particular risk - they may be for managing operational risks for example.
6. Put Control assessment in place by:
    - Analysing the processes and producing a high level map of the process workflow.
    - Identifying control points such as signoff, management approval, and any logging, recording or reviewing of information.
    - Compiling process / systems documentation and review it for completeness and accuracy.
    - Performing a ‘walkthrough test’ of the relevant part of the process to determine that the documentation is a true and fair reflection of the process, and that the controls are operated as documented.

7. Rating the controls: Controls should be numerically rated as described below by assessing the control processes against the maturity ratings below. Note that a control score in excess of three is unusual and the reviewer should be cautious about high scores

The risk assessment and treatment actions will need to be reviewed periodically.

1.7 Programme development, policy, scope and objectives

Business continuity programme management is at the heart of the business continuity process. Effective programme management establishes and maintains the organisation's approach to business continuity. In planning the business continuity programme, an MNO should capture and take account of the expectations of its stakeholders, in particular, external organisations (emergency services, humanitarian agencies) can be involved in the development of the programme, its scope and objectives.

The MNO should ensure that any risks to the achievement of the business continuity programme are identified and addressed. It should consider the three aspects of the mobile network resilience namely:

- people and processes;
- critical infrastructure; and
- building/recovery of ecosystems which support the business.

All of these are interdependent and should be considered holistically and at individual levels. For example, providing BTS with backup power generators will help with infrastructure resilience but it needs to be considered within the fuel supply chain ecosystem if it is to be deemed truly resilient. The business continuity policy, scope and objectives should be documented and communicated to all staff. The results of the BIA, Risk Assessment and considerations of the external organisations should be used in shaping he policy, scope and objectives.

1.7.1 Business Continuity policy development

Top management should define the business continuity management policy in terms of the organisation's objectives and its obligations and make sure that it:

- is appropriate to the purpose of the organisation (given its size, nature and complexity and in order to reflect its culture, dependencies and operating environment);
- provides a framework for objective setting;
- includes clear commitments in relation to applicable requirements, including legal and regulatory obligations and continual improvement of the BCMS;

- is communicated and understood within the organisation and available to interested parties;
- is complementary to other relevant policies; and
- is made available to interested parties as approved by management.

Suitable provisions should be made for approving the policy, retaining documented information on it and reviewing it periodically (for example annually), and whenever significant changes to internal or external factors occur (for example change in top management or introduction of new legislation). The suitability of such provisions will depend on the size, complexity, nature and extent of the organisation.

The policy should also provide direction on scope and boundaries of the organisation's business continuity program including limitations and exclusions; It should identify any authorities and delegations required under the BCMS, including person or persons responsible for the organisation's BCM and establish the criteria for type and scale of incidents to be addressed.

On-going maintenance and management activities should include embedding business continuity within the organisation, exercising business continuity procedures regularly, and updating and communicating them, particularly when there is significant change in premises, personnel, process, market, technology or organisational structure.

Phase 1 Activity Summary

Step	What	Why	Who	Input/Output
1.	Articulate the internal and external issues that may affect the business continuity programme	To enable the operator understand and manage all factors that might hinder it from achieving the intended outcomes of its BC programme	• BC Programme Coordinator	List of internal and external issues
2.	Document the expectations and interests of all of the MNO's key stakeholders (external and internal)		• BC Programme Coordinator	Record of stakeholders and their interests
3.	Identify the applicable legal and regulatory requirements to which the operator subscribes		• Company Secretary/Legal Adviser	Legal Register
4.	Conduct the BIA (and Continuity Requirements Analysis)	To identify the critical processes, functions and technology infrastructure to focus protection and recovery efforts on and to gather information needed to develop recovery strategies.	• BC Programme Coordinator • Departmental/ Functional representatives	Business Impact Analysis (BIA) Questionnaire
5.	Conduct the Risk Assessment	To identify key risks and strategies to reduce the likelihood and impact to the delivery of key services	• BC Programme Coordinator	Business Continuity Risk Register
6.	Develop the business continuity policy, scope and objectives	Provides a framework for executing the business continuity programme	• Senior Management • Business Continuity Programme Coordinator	Business Continuity Policy, Scope and Objectives

Phase 2: Implement and Operate (Do)

2.1 Introduction

Once the issues that affect the business continuity programme (including the critical processes, policy, scope and objectives, network infrastructure) and the attached risks are determined, it is then necessary to implement and operate the business continuity programme successfully. This will require MNO personnel being fully aware of their roles on the programme in order to support implementation of the business continuity strategy which may require further be capex or opex investments.

2.2 Determine Business Continuity strategy

As a result of the previous elements, the MNO will be in a position to evaluate the most appropriate continuity strategy to enable it to meet its business objectives and perform critical activities. An assessment of the strategic options for those critical activities and the resources they require will depend on a number of factors. Selected strategies should achieve a balance between the cost of building resilience against the benefits to both the business and to the wider community in the face of a disaster. The following elements are considered:

- Necessary technological infrastructure and costs are determined to provide accepted interruption times
- Necessary technology and costs are determined to work critical systems continuously except major disasters
- Requirements are determined separately for all systems and these requirements are presented to management for approval

This phase involves taking appropriate action to mitigate the loss of resources identified as Continuity Requirements at the BIA stage. Some key actions and considerations for MNOs when developing continuity strategies and plans that are common to all disasters are detailed in Section 6 of the GSMA Disaster Response BCM Report[5]. Key actions and considerations are arranged at varying levels of severity, with pre-disaster, during- and

[5] http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/05/GSMA_Disaster-Response_Business_Continuity_Management_Report.pdf

post-disaster actions, as well as resilience improvement actions for the following categories and sub-categories:

- Operations: Staff, Access & Transportation, Supply Chain.
- Infrastructure: Edge, Network, Core.
  Some identified strategies for Edge infrastructure such as base transceiver stations (BTS) and their masts include Cells on Wheels (COWs), collapsible masts, large radio-zone base stations, and tower sharing.
  Core infrastructure and systems can be protected through strategies such as geo-redundancy, service and BSS duplication, overload handling, and MSC pool.
- Usage: Demand, Subscribers

Other technical considerations for MNOs in building their continuity and recovery plans, especially for supporting both short term and longer term recovery for the wider community within which the MNO operates, include:

- Public early Warning Systems (PWS) - MNOs can work with relevant government agencies, NGOs and international agencies by using the mobile networks as a channel for disseminating impending disaster information that could help in minimising the loss of life and key in initiating BCPs effectively. Mobile networks can also detect the early signs of impending disasters - both directly and indirectly; options for this are in Section 6.4 of the GSMA Disaster Response BCM Report[6].
- Network congestion - This can be addressed in many ways depending on the operating environment and the technical options/capex available to the operator, some of those options for addressing this are outlined in the GSMA Disaster Response BCM Report.
- Mobile apps for information and communications services to staff and the general public.

Key actions and considerations for MNOs tailored to specific disaster scenarios are as follows in table 4:

TABLE 4

Key considerations for specific disaster scenarios (Tsunami)

Disaster Scenario	Operations Considerations	Infrastructure Considerations	Usage Considerations
Tsunami	I. Staff: • Setup early warning feeds for staff, where available	I. Edge: • Avoiding siting edge infrastructure in low	IV. Demand: • Negotiate and configure a national inter-operator

[6] https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/05/GSMA_Disaster-Response_Business_Continuity_Management_Report.pdf

	• Plan damage assessment roster with specific water/flood damage assessment plans. • Water damage rectification • Re-route/site water sensitive equipment II. Access & Transportation: • Transport procurement planning, specific to water and all terrain needs III. Supply Chain: • Identify, test and reinforce critical supply chains • Plan for in-country and import inventory availability	lying coastal areas, where possible • Reinforcement of power backup supply chain II. Network: • Utilise loop or mesh topology design and redundancy to mitigate the effects of transmission path failures III. Core: • Design and deploy flood precautions into the facility hosting the core infrastructure and systems • Careful planning and management of NE monitoring system(s) to avoid overloading	roaming agreement with MNOs and the telecom regulator • Switch compression codecs for OTA interface (beyond the MSC) from FR/EFR to Half-rate (HR) • Use 3GPP standards of 4G/LTE mobile networks for its Self-Optimising Network capabilities I. Subscribers: Plan how to manage the following subscriber issues during a disaster: • Warning notifications • Damage or loss of phone • Power supply for charging phones • Lack of PAYG credit balance • Access to PAYG top-up mechanisms • SIM card registration availability • Account termination • Roaming access (tourists, international agency workers, etc.)

Similar guidance as provided above is available in section seven of the GSMA Disaster Response BCM Report[7] for the following specific disaster scenarios:

- Earthquake
- Volcano
- Hurricane/Typhoon
- Flooding
- Disease

[7] http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/05/GSMA_Disaster-Response_Business_Continuity_Management_Report.pdf

2.3 BCM response

Developing and implementing a BCM response covers development and implementation of the MNO's Incident Management and Business Continuity plans and arrangements to ensure continuity of critical products and services, activities, resources and the management of the emergency/crisis within predefined RTO, RPO. Related departments/divisions should prepare and implement incident management and business continuity plans for their own functions. Incident Management Plans and Business Continuity plans may be combined when needed.

Some aspects of the plans that relate to external parties and joint efforts to support the wider community will need to be jointly developed and shared with these external parties for their reference if, and when, disasters occur.

The acquisition and deployment of resources required for the implementation of business continuity strategies should have started at this point, and can be done simultaneously with the documentation of the plans.

2.3.1 Plan content

Every MNO will have some unique qualities based on its operational environment hence the reason the basics of each plan may differ from location to location. However before developing a plan, the MNO must ensure every procedure and sub-plans would have been identified.

The main part of the plan includes but not limited to the following:

- **The Scope and Purpose of the plan:** The purpose and scope of any plan will need to be clearly stated. Any relationship to other relevant plans or documents within the mobile operator and interactions with external agencies/governmental agencies/humanitarian agencies should also be clearly referenced and the method of obtaining and accessing these described.
- **The Business Continuity organisation:** This will include the relevant teams, the names and contact of the team members and the respective roles and responsibilities. The plan should have a core crisis management team including senior executive representation and department heads with a Crisis Command Centre (possibly mobile), where the relevant personnel can be situated. There should be clear definition of roles e.g. RACI example, points of contact and duties with a level of redundancy to cover staff who may be unavailable.
- **BIA and Critical Services:** As already stated in section 2.5 of this document, It is necessary to undertake a BIA to understand how quickly the organisation needs to respond when a disruption to normal business occurs. The result of the BIA conducted

and the critical services becomes a statement of requirements for the recovery strategy following a disruption and will be included in the plan. By knowing how quickly the delivery of the various products and services needs to be restored in the plan, the MNO is able to work out how quickly the various activities within and outside the business need to be recovered to enable that to happen.

- **Managing Incidents:** The tasks that will be required to manage the initial phase of the incident and the individuals responsible for each task should be documented, including how and when emergency services are to be engaged. This is likely to include:
    - site evacuation;
    - mobilisation to safety;
    - first-aid or evacuation-assistance teams;
    - locating and accounting for those who were on site or in the immediate vicinity;
    - taking temporary measures e.g. deploying COWs (Cells on Wheels) from existing telecoms kit, generators and pickup trucks in order to recover a pre-determined level and quality of service within a time limit (RTO); and
    - ongoing employee/management communications.

  The plan should set out the arrangements for communicating with staff, wider stakeholders and, if necessary, the media. There should be an up-to-date contact list and the location and method of obtaining it described in the plan. The contact details of individuals mapped to the roles specified earlier should be provided, including their addresses, primary and alternate phone numbers and email addresses. Primary and alternate phone numbers for MNO personnel must be from different operators. The mobile operator should identify a robust location, room or space from which an incident can be managed. Once established, this location should be the focal point for the mobile operator's response. An alternative meeting point at a different location should also be nominated in case access to the primary location is denied with each location should have access to appropriate resources.

- **Plan Activation:** The method by which the plan is invoked during a disaster occurrence should be clearly documented, setting out the individuals who have the authority to invoke the plan and under what circumstances. The plan should also set out the process for mobilising and standing down the relevant teams. In doing this, consider putting in place arrangements so that the relevant teams are mobilised as early as possible when an incident occurs. Delay in mobilising these teams could have a major impact on achievement of RTOs, humanitarian support and the effectiveness of the BCM arrangements.
- **Detailed recovery procedures:** There should be detailed recovery procedures for identified MNO services. The procedure should include the resources that will be responsible for executing the procedure and the detailed actions and tasks needed to ensure the continuity and restoration to business-as-usual. The Technology procedures can be individual recovery procedures for services or a general recovery procedure for some disasters e.g. Recovery from Fire Procedure, Procedure for transition to Disaster

Recovery Centre as an example. Outline the resources available at different points in time to deliver those critical activities.

- **Testing the Plan:** As the continuity plan is a living process document, it should be tested periodically. The tests should be done at a time when the processes being tested will minimal impact It should also be noted that testing should be approved by the MNOs management before it is conducted. The main purpose of the test are as follows:
    - To ascertain the efficiency of the business continuity plan (RPO, RTO)
    - To preparing for real disaster situations
    - To measuring the team member's preparation level
    - To capture deficiencies in the business continuity program inclusive of deficiencies of the recovery plan, organisations deficiencies and training deficiencies

- **Maintenance and Update of the Plan:** In specific cases and periodically the plan should be updated. Business Continuity plans should be reviewed at least once a year and determined imperfections should be fixed. The ownership and responsibility for updates should be documented.

- **Training:** A BCM training program should be put in place and could be conducted after testing has been conducted. The MNO personnel and the teams stated in the plan should be informed about the updates in the plan. It is recommended that the training be conducted at least once a year and the steps and methodology of the training should be identified and included in the plan.

2.4 Simulation and exercising

In order to validate the reliability of the Business Continuity programme, it has to exercised and proven to be realistic and workable. Exercising and testing will ensure a controlled, co-ordinated and communicated response to an incident or crisis and provide assurance that confirms appropriate resilience and disaster recovery capability is in place. BCM capability cannot be considered reliable if it is not exercised appropriately. Therefore, exercises shall be performed by MNOs at planned intervals according to the BCM exercise program.

The purpose of exercises is to:

- Evaluate the MNO's current competence in BC
- Identify areas for improvement or missing information
- Highlight assumptions which need to be questioned
- Provide information and instil confidence in exercise participants
- Increase resumption team work efficiency
- Raise awareness of Business Continuity
- Test the effectiveness and timeliness of restoration procedures

The frequency of exercises will depend on two main factors namely continuous improvement based on the output of previous exercises and the rate at which changes occur within the operational environment. It is however recommended that plans follow a schedule to be developed in conjunction with external emergency and humanitarian services at the beginning of the year. A GSMA case study conducted a few years ago of Turkcell's Disaster Management System[8] provides an insight on the how the MNO conducted both informed and uninformed exercises.

The following are the five different types of exercises that the MNOs can leverage as part of a comprehensive exercise program:

- **A discussion based exercise**: this involves participants exploring relevant issues and performing plan walk-throughs in an informal and non-threatening environment. This type of exercise can be particularly useful if targeted at a specific areas of improvement in order to find a solution. It can also be used for training purposes and can provide an important tool for embedding business continuity in the operator's culture. It is probably the easiest and cheapest to organise and can be scaled easily to involve external emergency and humanitarian agencies.

- **Command Post exercises**: this involves stakeholders across the MNO's operation working from their normal positions and location. The aim is to pass information to them and receive response to those information as they would during an actual incident. The information flow and the response can then be reviewed. Some crucial elements like the contact list and the activation process could also be validated during this exercise. A call tree tests emergency communications whereby, someone is designated in the incident response plan to launch the calling tree. That designated person calls two employees (ideally members of the incident response team), and those two call another two, and so on. An alternate call tree lead should be designated as well; in case the lead is not available following the disaster event.

- **A table-top exercise** is a scenario based with all participants expected to not only be knowledgeable in their plans, but also able to demonstrate how to use their plans to respond and recover from a disruptive incident. The effectiveness of this type of exercise will be based on setting a scenario that is time-based, simple and relevant to the MNO's business activities.

- **A live exercise** ranges from a small-scale test of one component through to a full-scale test of all components of the plan, including infrastructure resilience. Live exercises often provide the most effective participant training, executing a live test is time and resource intensive and can result in an actual disruption if not carefully controlled. It is therefore important to consider whether the operator has the necessary capacity to run the exercise without it causing operational disruption. In conducting this exercise, It might be worthwhile inviting other stakeholders, and in particular, suppliers, emergency and humanitarian agencies and suppliers. It is also important to record and evaluate the

[8] https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2014/01/Preparing-for-Disaster_Analysis-of-Turkcells-Disaster-Management-System.pdf

event, by debriefing immediately after the exercise, and then write up a lessons learned report with actions, if required.

- **Testing:** this usually incorporates a procedural walkthrough that involves a pass and fail element which may not be applicable to all aspects of the business continuity plan. This type of exercise is often applied to technology and equipment rather than personnel.

2.5 Awareness and training

For the business continuity programme to be successful, it has to become part of the culture of the operator. This can be achieved through a combination of awareness raising and training programmes.

2.5.1 Awareness

This involves raising and maintaining awareness of business continuity with all staff. The mechanisms for raising awareness includes but not limited to:

- Involving staff in the development of the business continuity strategy;
- Written and oral briefings on the status of the programme;
- Learning from internal and external incidents; and
- Involving staff in various forms of business continuity exercises

Awareness of the operator's business continuity arrangements should be an integral part of the induction process for all new staff. External emergency and humanitarian agencies should be encouraged to create awareness of any joint plans within their organisations.

2.5.2 Training

Training is a key component of the BCM programme that is critical for all stakeholders who have a role to play. The program should not only be targeted at the objectives of the program but most specifically at the roles they play within the whole value chain. It should involve both internal and external resources and have refresher training sessions scheduled periodically following the implementation of any change to the business continuity plans. This training should include both the technical and softer side of training e.g. psychosocial[9] support type training. Implementing and maintaining a training programme for business continuity will involve the following steps:

[9] The psychosocial approach looks at individuals in the context of the combined influence that psychological factors and the surrounding social environment have on their physical and mental wellness and their ability to function

Analyse:

- Perform a training needs analysis based on mobile operator changes (e.g. LTE rollout, recruitment of a new team member into critical functions/departments, restructuring of the key departments, etc.) and changes to the business continuity programme.
- Identify target audience (i.e. individuals to attend each training session), including personnel of external emergency and humanitarian agencies, where possible.
- Identify course trainer

Design:

- Develop training materials and presentation slides (including course evaluation forms)
- Design training schedule

Execute:

- Communicate training schedule to course participants and trainers
- Deliver training courses to participants through classroom training sessions and business continuity simulations

Evaluate:

- Evaluate effectiveness of training covering content, delivery, etc.
- Collate feedback from users and address key issues
- Conduct training assessment

Phase 2 Activity Summary

Step	What	Why	Who	Input/Output
1.	Develop the continuity strategy for meeting functions and infrastructure recovery objectives and for supporting humanitarian efforts during a disaster*	Selection of appropriate continuity and recovery options for achieving BC programme objectives	• BC Programme Coordinator • Infrastructure team	Business Continuity Strategy
2.	Develop business continuity plans for selected strategies*	To provide articulated and rehearsed guidance and capability for ensuring the survival of critical infrastructure, people, services, the populace	• BC Programme Coordinator • Infrastructure team • Process owners	• Incident/Crisis Management Plan • Business Continuity Plan • ICT Disaster Recovery Plan

Step	What	Why	Who	Input/Output
3.	Implement business continuity plans - Acquire and deploy resources (people/teams, suppliers, etc.)	and the business following a catastrophic event	• Senior Management • Infrastructure team • Process owners	Deployed capability to withstand a disruption to infrastructure, processes and services
4.	Deploy redundant/resilient mobile network infrastructure and technology systems		• Infrastructure team	
5.	Exercise and test continuity and recovery capabilities*	To identify deficiencies in documented plans and ensure that the plans work when needed	• BC Programme Coordinator • Infrastructure team • Process owners	• Infrastructure and technology DR test report • Fire Drill Report; • Sample Call Tree Test Report
6.	Plan and embark on training sessions and awareness raising initiatives*	To enhance the probability of success of business survival by equipping personnel with the appropriate knowledge	• BC Programme Coordinator • Infrastructure team • Process owners • All staff	• Training plan • Training slides

* Humanitarian agencies, NGOs and government agencies should be involved in these activities as described in sections 3.1 to 3.5 above.

Phase 3 - Monitor and Review (Check)

3.1 Introduction

The aim of the 'Check' stage is to monitor, review and report the progress and effectiveness of the program against business continuity objectives. This will be subjected to management review with remedial actions ratified and approved for implementation.

3.2 Continuity Assurance Review

Mobile operators should conduct internal audits at planned intervals in order to ensure alignment of the business continuity programme to the operator's overall objectives: The audit should look at such areas as alignment to policy, goals and objectives set at the beginning of the program. It will also check if it complies with the mobile operator's objective of supporting humanitarian efforts for its wider community before, during and after a widespread disaster.

An internal audit programme scope should cover all aspects of the business continuity management system. In line with ISACA[10], a continuity planning audit/assurance review will:

- Provide management with an evaluation on the enterprise's preparedness in the event of a major business disruption
- Identify issues that may limit interim business processing and restoration of same
- Provide management with an independent assessment of the effectiveness of the business continuity plan and its alignment with subordinate continuity plans

The scope of the review will focus on the enterprise business continuity plan, policies, standards, guidelines, procedures, laws and regulations that address maintaining the MNO's continuous business services, including:

- Development, maintenance and testing of the business continuity plan
- Ability to provide interim business services and the effective and timely restoration of same
- Risk management and costs related to the business continuity plan

[10] ISACA is an international professional association focused on IT governance. Previously known as the Information Systems Audit and Control Association

A typical BCM Plan Audit checklist[11] will cover the following areas:

- Business Continuity Planning (Survival)
- Business Resumption Planning (Testing and Simulation)
- Business Resumption Planning (Recovery)

The MNO audit team can either be internal or external resources and should have access to all stakeholders who have participated in the programme. External emergency and humanitarian agencies may also be required to supply information based on their level of involvement.

3.3 Measurement of BCM programme performance

The operator should develop a set of metrics to measure and evaluate the on-going performance of the BCM programme and the processes that support it. These metrics shall be measured as defined and reviewed periodically at management meetings. The defined coverage of the metrics will vary from operator to operator but should typically cover the following:

- Training participation level
- Number of drills conducted
- Programme objectives
- Tests and Exercises
- External or Third Party Involvement
- Security

The targets as agreed by Senior Management should be tracked and reported into the MNO's management team review meetings.

3.4 Senior management review

The ownership of the programme sits with the Senior Management Team and the responsibility for its successful implementation will require that they monitor progress and conduct regular reviews so as to ensure it is meeting its set objectives. The management review should cover the overall progress on the objectives set for the programme, the status of the metrics, progress on risk avoidance, output from a recent or previous

[11] http://www.isaca.org/Groups/Professional-English/business-continuity-disaster-recovery planning/GroupDocuments/DRP%20toolkit_DRP%20and%20BCP%20audit.pdf

conducted audit, the impact on the operating environment and partnership with both governmental and humanitarian agencies. The meeting should also review the debrief notes and agree action plans as and when required. The frequency and agenda of such meeting will depend on each operator but it is recommended that the meetings be formal, actions documented, tracked and the held consistently with all expected participants attending.

Phase 3 Activity Summary

Step	What	Why	Who	Input/Output
1.	Conduct internal audits at planned intervals	To obtain objective feedback on the adequacy of the BC programme for ensuring the survival of critical infrastructure, people, services and the business following a catastrophic event	• Internal auditors	Internal Audit Plan and Checklist
2.	Determine performance metrics and measure programme performance as defined	To track the performance and effectiveness of the BC programme and its value to the operator as part of the continuous improvement process.	• BC Programme Coordinator	BC Programme Measures
3.	Conduct management reviews of the operator's business continuity programme at planned intervals	Management intervention and decision making about improvements to the BC programme	• Senior management • BC Programme Coordinator • BC Programme Team members	Management Review Minutes of Meeting

Phase 4 - Maintain And Improve (Act)

4.1 Introduction

It is important to maintain and improve the business continuity programme by taking corrective action based on the results of management reviews, internal audits and measurement activities, and reappraise the scope of the programme, business continuity policy and objectives. Mobile operators also need to ensure that problems within the programme are corrected, lapse identified are fixed and all changes properly managed with change implemented and tracked.

4.2 Maintaining Business Continuity arrangements

The need to maintain the business continuity arrangement will be critical to any operators BCM program. The importance of keeping it consistent and updated will reduce the number of inconsistences and or non-conformance found either during a periodic audit as well as during exercises. A typical BCM will ensure changes to BCM artefacts are properly managed with required approval levels in place. This is to ensure internal and external changes that may affect the operators BCM program deliverables are regular monitored, impact assessed and planned resolutions are put in place. The expectation is that MNO's implement a typical BCM change[12] management process that will:

- Monitor internal and External Changes
- Review compiled changes, test results and audit results
- Process Business Continuity Plan Change requires

[12] http://www.continuitycentral.com/index.php/news/business-continuity-news/1505-maintenance-of-a-business-continuity-management-system-a-managerial-approach

4.3 Debrief sessions

The expectation is that Incident Managers conduct debrief sessions after every incident has occurred. As with most debriefs, it can either be a feedback session which is conducted immediately after the incident or it could be done some time in the nearest future with the aim of documenting all aspects of the incident for audit and reference purposes. The expectation is that this is conducted in an open, honest and constructive manner.

It is important that debriefing be conducted with all the participants involved with a clear understand of the what, when and where. It will also require that outcomes be frequently reviewed and serves as input into a continuous improvement cycle that brings improvement and or enhancement to the program. It may also require that some key document of the program be updated if required.

Phase 4 Activity Summary

Step	What	Why	Who	Input/Output
1.	Implement programme improvement actions recommended from the management reviews and internal audits	For continuous improvement of the BC programme	• BC Programme Coordinator	Corrective/Improvement Action Report
2.	Update aspects of the programme as a result of technology, organisation, environment and other changes		• BC Programme Coordinator	Updates to the BIA, BC Strategy, BC Plans,
3.	Review the effectiveness of any improvement actions taken	To ensure the action gives the desired improvement effect	• BC Programme Coordinator	Corrective/Improvement Action Report
4.	Following invocation of BC plans, conduct debrief sessions to learn from the incident	To track key learnings that can be used to improve BC plans	• BC Programme Coordinator	Incident Lessons Learned report

Conclusion

The changing role that MNOs play within the disaster management space makes it critical for the operators to implement an effective business continuity management programme. This document provides the basic guideline for implementing such a programme. When critical services and products cannot be delivered, consequences can be severe. An effective Business Continuity Management program allows MNOs to not only moderate risk, but also continuously deliver products and services despite disruption and provide the expected support during disaster periods. The information provided in this document as summarised below will certainly help in developing and enhancing such a programme. The summary is as follows:

- Define the organisational policy relating to Business Continuity (BC) and how that policy will be implemented, controlled and validated through a BCM programme.
- Select appropriate strategies and execute the agreed strategies through the process of developing the Business Continuity Plan.
- Continually seek to integrate BC into day-to-day business activities and organisational culture.
- Review and assess in terms of what the MNO's objectives are, how it functions and the constraints of the environment in which it operates.
- Confirm that the BCM programme meets the objectives set in the BC Policy and that the operator's BCP is fit for purpose.

References

- GSMA Disaster Response Business Continuity Management Report
- ISO 22301 Societal Security - Business Continuity Management Systems - Requirements15
- ISO 22313 Societal Security - Business Continuity Management Systems - Guidance
- BCI Good Practice Guidelines 2013 - A Guide to Global Good Practice in Business Continuity
- Emergency Telecommunications Regulatory Best Practice
- GSMA BCM Training Pack
- http://perspectives.avalution.com/
- http://www.gov.uk/government/
- https://www.isaca.org/
- http://www.continuitycentral.com/index.php/news/business-continuity-news/1505-maintenance-of-a-business-continuity-management-system-a-managerial-approach

Glossary

Abbreviation	Meaning
3GPP	3rd Generation Partnership Project
4G	4th Generation
BC	Business Continuity
BCM	Business Continuity Management
BIA	Business Impact Analysis
BTS	Base Transceiver Station
CDR	Call Detail Record
COWs	Cell on Wheels
DR	Disaster Recovery
FR/EFR	Full Rate/Enhanced Full Rate
GSMA	GSM Association
ISO	Internal Organisation for Standardisation
IT	Information technology
LTE	Long-Term Evolution
MNO	Mobile Network Operator

Abbreviation	Meaning
MSC	Mobile Switching Centre
NGO	Non-Governmental Organisation
OTA	Over-the-air
PAYG	Pay as you go
PWS	Public early Warning System
RACI	Responsible, Accountable, Consulted and Informed
RPO	Recovery Point Objective
RTO	Recovery Time Objective

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601