Contents

1. Introduction 3
2. Glossary 5
3. BCM Requirements 6
4. Telecommunications Infrastructure Resiliency Requirements 14
5. Documents To Be Submitted 18
6. General Provisions 18
7. Annex 19
1. Introduction

Pursuant to the provisions of the Telecommunications Act (Act), the Telecommunications Bylaw (Bylaw) and CITC Ordinance related to safeguarding the public interest and user interest as well, the Regulatory Framework and the Guidelines for Disaster Recovery Planning for the ICT Industry issued with the purpose of improving the preparedness for disasters and emergencies and mitigate the adverse impact on life and property.

The availability of telecommunication services is crucial because of the high level of dependency on communications infrastructure. A critical disruption within a telecommunications network has a potential impact on large numbers of customers and has a broader impact on the kingdom economy. With the rapid technological development in the telecommunications sector and based on the best international practice, there is a necessity to update the Regulatory Framework and the Guidelines on Disaster Recovery Planning for the ICT Sector and establish comprehensive and standardized Regulations on Business Continuity Management for Service Providers. This document is replacing the Regulatory Framework and the Guidelines on Disaster Recovery Planning for the ICT Industry. They define strategic objectives and guiding principles for initiating, implementing, maintaining, monitoring and improving Business Continuity Management in Service Providers.

Effective BCM of Service Providers will support the achievement of the 2030 Vision, particularly the strategic objectives of developing and diversifying the national economy, promoting digital infrastructure, being leader in e-government, promoting investment in emerging technologies and smart cities, and being enabler of e-commerce, e-health and e-learning.

1.1 Purpose

This document define the requirements which the Service Providers shall adopt to enable a consistent and effective approach towards BCM to enhance prevention, preparedness, mitigation, response, and recovery when disrupted.

BCM interacts with other disciplines within the Service Providers, such as risk management, cyber/information security, incident management, safety, governance, and physical security, thus
supporting effective implementation of overall resiliency and ensuring the continuity of services and operations of the Service Providers.

1.2 Scope

1.2.1 This document outlines the minimum BCM requirements and resiliency to be implemented by the Service Providers.

1.2.2 The articles on this document of Regulations and Resiliency Requirements – where applicable – are applied on the Facility Based Providers (FBPs) and the Mobile Virtual Network Operators (MVNOs), and they referred to as Service Providers.

1.2.3 The requirements as set out in this document apply to the full scope of the Service Providers, including, but not limited to, subsidiaries, infrastructure, technical buildings, applications, systems, employees, contractors, customers, suppliers and vendors.

1.3 Compliance and Audit

The Service Providers shall take the necessarily actions for business continuity and shall be completely responsible for ensuring the execution of the BCMS effectively and adhere to the followings:

1.3.1 The relevant legislative and regulatory national requirements.

1.3.2 Ensuring the BCM scope includes all services and activities required to maintain critical business functions.

1.3.3 Developing, implementing and operating BCM to enhance the reliability and availability of their services and infrastructures based on the BCM requirements identified in this document.

1.3.4 Periodic reviews and audits by an independent external party based on CITC request and its approval.

1.3.5 Completely adhere to these Regulations maximum within six (6) months from issuing date.
2. GLOSSARY

The words and expressions outlined herein shall have the same meanings as defined in the Telecommunications Act and its Bylaw as well as CITC statutes. The following words and expressions shall have the meaning assigned to them below unless the context requires otherwise:

**Business Continuity (BC):** Capability of an organization to continue the delivery of products and services within acceptable timeframe at predefined capacity during a disruption.

**Business Continuity Plan (BCP):** Documented procedures that guides an organization to respond to disruption and resume, recover and restore the delivery of products and services consistent with its business continuity objectives.

**Business Continuity Management (BCM):** Process of implementing and maintaining business continuity.

**Business Impact Analysis (BIA):** The process of analyzing the impact over time of a disruption on the organization.

**CITC:** Communications & Information Technology Commission.

**Crisis:** An unstable condition in which the basic activities are disrupted and / or the credibility of the company is damaged and requires urgent action.

**Disruption:** Incident, whether anticipated or unanticipated, that causes an unplanned, negative deviation from the expected delivery of products and services according to an organization’s objectives.

**Exercise:** Process to assess the effectiveness and efficiency of the plans and processes for the BCM through simulation and testing to improve the BCMS.

**Incident:** Event that can be, or could lead to, a disruption, loss, emergency or crisis.

**Maximum Tolerable Period of Disruption (MTPD):** The time for adverse impacts, that might arise because of not providing a product/service or performing an activity, to become unacceptable.

**Policy:** A document whose statements define a general commitment, direction, or intention of an organization as formally expressed by its top management.

**Recovery Point Objective (RPO):** The point to which an activity's information must be restored to enable the activity to operate on resumption.

**Recovery Time Objective (RTO):** The period following an incident within which, products or services must be resumed, the activity must be resumed, or resources must be recovered.
Resilience: The ability of the Service Provider to absorb and adapt in a changing environment.

Test: Unique and particular type of exercise that incorporates an expectation of a pass or fail element within the aim or objectives of the exercise being planned.

3. BCM Requirements

3.1 Context

The Service Providers shall determine:

3.1.1 The relevant internal and external issues that might affect their BCMS or the ability to continue the operation and providing services as intended, issues shall include, where relevant:

   a) Political, legal and regulatory environment whether national or international.

   b) Social, cultural, financial, technological, economic, natural and competitive environment, whether national or international.

   c) Supply chain commitments and relationships with relevant parties.

   d) Services, activities, resources, partnerships, and relationships with interested parties.

3.1.2 Capabilities, in terms of resources and knowledge (e.g., capital, time, people, processes, systems and technologies); interested parties needs and requirements related to the continuity of its operation and providing services.

3.1.3 All applicable legal and regulatory requirements related to its services and business continuity.

3.2 Leadership

3.2.1 The top management of the Service Providers shall sponsor and take responsibility for initiating, implementing, maintaining, monitoring and improving a comprehensive BCM and ensure that management and staff at all levels recognize that BCM is a critical top management priority. The top management shall:
a) Define and implement the relevant BCM organization structure that will have the responsibility and authority for leading the establishment, implementation and operation of business continuity management.

b) Allocate sufficient budget to provide the required resources for the BCM program and to execute the required BCM activities.

c) Define and approve an organization-wide policy appropriate to the purpose of the Service Provider and communicate it within the Service Provider.

d) Establish a BCM Committee with members from senior management of all relevant departments.

3.2.2 The BCM Committee shall:

a) Establish roles relevant to the BCM with clear competences, responsibilities, assigned authorities and resources.

b) Ensure that roles are assigned and communicated internally.

c) Ensure the integration of the BCM requirements into the business processes for the Service Provider.

3.2.3 The business continuity police shall ensure:

a) Top management commitment to satisfy applicable requirements.

b) Providing all the required support and resources for the BCMS effectively.

c) Defined and measurable BCM objectives that will be achieved over a defined period, monitored, updated appropriately, and consistent with the Service Provider’s objectives.

3.3 Resources

3.3.1 The BCM Committee shall identify the resources required to the BCMS.

3.3.2 The resources shall include, but not limited to:

a) People.

b) Facilities, including work locations and buildings.
c) Information and communication technology (ICT) systems.

d) Transportation and logistics.

e) Finance.

f) Partners and suppliers.

3.4 Business Impact Analysis and Risk Assessment

The Service Providers shall:

3.4.1 Comply with Regulations of Communications Infrastructure Risk Management issued by CITC.

3.4.2 Define and document the approach for the Business Impact Analysis (BIA) and Risk Assessment (RA).

3.4.3 Perform and document BIA to priorities activities and to determine:

a) The potential impact over time of business disruptions causing unavailability; for each activity, including but not limited to financial, operational, legal, regulatory and customer related impacts.

b) The Maximum Tolerable Period of Disruption (MTPD) for critical activities.

c) The Recovery Time Objectives (RTOs) for critical services and activities, where the RTO shall be set for each service and activity. The recovery time objective shall be less than the time when the impacts of not resuming the service or activity would become unacceptable (MTPD).

d) The Recovery Point Objectives (RPOs), when applicable, for critical activities.

e) Internal and external interdependencies including but not limited to relevant partners and suppliers.

f) The required resources to support priorities activities.

3.4.4 Perform and document RA for internal and external risks.
3.5 Incident Response

3.5.1 The Service Providers shall establish an incident response team(s) with the necessary responsibility, authority and competence to manage an incident.

3.5.2 The incident response team shall be assigned to manage disruptive incidents, including those which may impact the priorities activities.

3.5.3 The Service Providers shall determine the response level criteria for the incidents.

3.5.4 The incident response team responsibilities shall include, but not limited to:

   a) Assessing the nature and extent of disruption and its potential impact.

   b) Assessing the impact against predefined thresholds.

   c) Activating the appropriate incident response plan, such as DR plan.

   d) Establishing priorities and ensuring prioritizing people safety.

   e) Monitoring the effects of the disruption.

   f) Communicating with relevant interested parties.

3.5.5 The Service Providers shall establish Incident Response Procedures to enable them to prepare for, mitigate, and respond effectively to disruptive incidents.

3.5.6 Incident response procedures shall provide details on how to, but not limited to:

   a) Verify the impact thresholds that justify initiation of formal response.

   b) Detect an incident and alerting response personnel.

   c) Activate, operate, coordinate, and communicate the response.

   d) Ensure sufficient resources being available to support the processes and procedures needed to manage a disruptive incident or work to minimize impact.

   e) Communicate between the various response teams within the Service Providers.

   f) Communicate with relevant interested parties.
3.6 Communication

3.6.1 The Service Providers shall establish a communication plan that includes:

a) Details on the processes, procedures and responsibilities for internal communications with employees and external communications with interested parties including but not limited to governments, partners, vendors, customers as well as media.

b) Different Means of communications during incidents for engaged teams in the BCM including but not limited to SIM cards from different telecom operators and different communication technologies such as satellite communications and Trunked Radio Systems.

c) Testing procedures to ensure the proper functioning of the plan.

3.6.2 The Service Providers shall communicate with CITC on BCM related subjects that include, but not limited to reporting of disruptive incidents according to relevant CITC Instructions on Outage Notifications.

3.7 BCM Strategy

3.7.1 The Service Providers shall establish an appropriate BCM strategy to ensure:

a) Continuity of its activities and services following a business disruption.

b) Recovery of essential services within an acceptable timeframe.

c) Protect critical activities.

d) Reduce the likelihood of disruption.

e) Shorten the period of disruption.

f) Limit the impact of disruption on the business functions, services and processes.

3.7.2 The BCM strategy shall identify the methodology, activities and resources required to achieve the recovery objectives, in response to disruptions scenarios and their impacts as identified in the BIA and RA.

3.7.3 The selection of BCM strategy shall consider setting prioritized timeframes such as the RTO would be less than the MTPD.
3.7.4 The service provider shall have a mutual resource agreement with at least one service provider, to enable service restoration at the event where the solutions and capabilities of the service provider are unable to do so in accordance with the specified recovery objectives.

3.8 Business Continuity Plans

3.8.1 The Service Providers shall establish Business Continuity Plans (BCPs) that provide the required processes to respond to disruption and resume critical activities within recovery objectives.

3.8.2 The Service Providers shall determine BCP invocation criteria and escalation matrix.

3.8.3 The Service Providers shall update BCP annually or when there are significant changes.

3.8.4 BCPs shall include, but not limited to:

a) Purpose and scope, and objectives.

b) Roles and responsibilities of the team that will implement the plan.

c) Activation Criteria and a process for activating the response based on predefined criteria.

d) A process to continue the critical activities within predetermined recovery objectives (RTO, RPO and MTPD).

e) Resources required (e.g., people, equipment, facilities, technologies, logistics, suppliers).

f) Internal and external interdependencies.

g) A process to resume/restore operations to business-as-usual once the disruption is resolved.

h) Requirements for communicating with employees, relevant parties and emergency contacts (see section 3.6 Communication).

3.8.5 The Service Providers shall follow the Table of Content for Business Continuity Plans of Annex A.

3.8.6 BCPs shall be accessible to those with responsibilities defined within them.

3.9 Disaster Recovery Plan
3.9.1 The Service Providers shall develop Disaster Recovery Plan (DRP) for ICT.

3.9.2 The Service Providers shall have technical redundant systems hosted in two alternative locations, as a minimum, to ensure that telecommunications services are not affected in case if any of these systems fail.

3.9.3 The primary site and its alternatives sites shall be in different governance regions, with equivalent technical capabilities.

3.10 Exercising and Testing

3.10.1 The Service Providers shall:

a) Establish an exercising and testing program to confirm the effectiveness of BCPs and strategies.

b) Ensure exercising and testing are carried out periodically and when there are significant changes within the Service Provider.

c) Ensure exercising and testing consider multiple types of disruptions scenarios (e.g., per function, per service, per process, per location, per worst cases scenarios, and scenarios invoking the Crisis Management Team and CITC).

d) Submit to CITC annually BC, Resiliency and DR exercising and testing plan and schedule, before the end of the first month of each year.

e) Amend BC exercising and testing schedule if CITC requests such amendment.

f) Submit to CITC the detailed results within two weeks from the execution date.

g) Conduct BCPs exercises (at least once a year).

h) Conduct Resiliency DR tests for the infrastructure and applications (at least once a year).

i) Conduct DR site tests for all relevant DR sites (at least once every two years).

j) Conduct Crisis Management Plan exercise (at least once a year).

3.10.2 The Service Providers shall follow the Table of Content for the Exercising and Testing Results of Annex C.
3.11 BCM Performance and Monitoring

The Service Providers shall on a regular basis confirm BCMS effectiveness and compliance with this document and the Service Provider’s policy and objectives by:

3.11.1 Review BCMS performance, and update its documentations and plans.

3.11.2 Evaluate the suitability and effectiveness of its BCMS such as BIA, RA, BC strategies, BCPs, and procedures after an incident or exercise, or when significant changes occur (internal or external) that impact the Service Provider context.

3.11.3 Ensure evaluations of the business continuity capabilities of relevant partners and suppliers are conducted.

3.11.4 Report the performance of the BCMS to the top management.

3.12 Awareness and Training

3.12.1 The Service Providers shall:

a) Perform BCMS awareness programs taking into consideration the alignment with target segment, which would support the Service Providers to achieve the goals of the BCMS.

b) Ensure that all people have sufficient business continuity awareness to understand:

- The business continuity policy.
- Their contribution to the effectiveness of the BCMS.
- The implications of non-conformity with the BCMS requirements.
- Their roles and responsibilities before, during and after disruptions.

3.12.2 The Service Providers shall prepare, develop, and implement a Business Continuity Training program.

3.12.3 Review and measure the effectiveness of the awareness and training program and implement the required changes to improve it.
4. Telecommunications Infrastructure Resiliency Requirements

This section demonstrates the minimum requirements that shall be followed by the Service Providers to achieve and improve the resiliency in the network to ultimately ensure the service continuity.

4.1 Core Network Resiliency

The Service Providers shall implement a range of controls to achieve and maintain resiliency in the Core network as described below:

4.1.1 Ensuring availability of Core Network nodes in at least (3) different governance regions, where Core Network nodes are geographically distributed with (N+2) model, and have the capacity to take over the load from other Core Network nodes in (2) different regions once they fail.

4.1.2 Applying the Pooling concept on the Core Network, where applicable, to guarantee the continuity of the services once a node fails.

4.1.3 Ensuring there is no single points of failure (SPoF) in the core network.

4.1.4 All Core Network nodes hardware and software shall be inherently reliable and with automatic failover, that makes the services available despite failures.

4.1.5 Deploying effective Network Management System (NMS), covering resources and service such as fault management, configuration management, performance management and traffic management.

4.1.6 The Core Network nodes for telecommunication services shall be well maintained, and their traffic load shall be continuously monitored and shall not exceed a threshold of 60% in normal circumstances.

4.1.7 Traffic management plans shall be in place in order to avoid severe traffic congestion by:

a) Ensuring the availability of spare capacity/ redundant capacity for the same node to increase traffic handling capability.

b) Providing priority access/ calling for critical users as specified by CITC for priority access/calling.

c) Prioritizing of critical messages, such as early warning disaster alerts or government information Centre messages.
4.2 Transport and Backhaul Network Resiliency

The Service Providers shall implement a range of controls to achieve and maintain resiliency in the transport and backhaul network by:

4.2.1 Using diverse routing and ensuring physical and logical diversity. In addition, implement automatic alternative routing to allow affected traffic to be carried over another route, which shall include, but not limited to, local, national, international routes (terrestrial and submarine routes).

4.2.2 The mobile Service Providers shall ensure that hub site shall be connected to multiple separated core network nodes or a mix of different technologies such as a combination of fiber, microwave and satellite.

4.3 Transportable Network Elements

The Service Providers shall implement a range of controls to achieve and maintain resiliency by deploying transportable network elements as per below:

4.3.1 Deploy interim portable network facilities, including transportable generators and telecom containers with core element node and access network nodes for fixed and mobile access networks. For example, Optical Line Transmission (OLT) containers and Cell on Wheels (COWs) which can be deployed to affected areas to restore the services as quickly as reasonable.

4.3.2 Maintain enough interim portable network facilities to reach, any of the locations that are part of their network coverage within 4 hours.

4.3.3 The dimensioning and the deployment strategy of portable interim network facilities and portable generators shall be based on the overall size, the topology of the networks, RA, and BIA.

4.4 International Connectivity Resiliency

The Service Providers shall implement a range of controls to achieve and maintain resiliency in the international connectivity. These controls include, but are not limited to:

4.4.1 Full geo-redundancy of the cable landing stations in at least (3) cities in the kingdom, connected to at least (3) stations in different countries.
4.4.2 Redundant capacity, and the traffic utilization shall not exceed 60%.

4.4.3 Ensuring diversity in the used cable systems, and to distribute the traffic fairly.

4.4.3 The cable systems shall not use the same landing point, and this landing point shall be connected to the cable landing station through different routes.

4.5 Suppliers and Managing Supply Chains

The Service Providers shall implement a range of controls to achieve suppliers and supply chain management according to the below.

4.5.1 The Service Providers shall identify and periodically update a list of key suppliers, vendors and partners, both domestically and internationally. Communicate with these key suppliers to ensure they have taken appropriate measures and have their BCP in place.

4.5.2 The Service Providers shall establish agreements with vendors and partners to ensure disaster support. The Service Providers and/or their vendors shall have sufficient stock/inventory of (6) months of key spare parts to meet their needs. This stock shall be available in geographically separated warehouses distributed over the Kingdom, and the actual distribution shall be made based on RA and BIA.

4.5.3 The Service Providers shall ensure fuel distribution to critical locations through adequate supply chain plans with relevant stakeholders.

4.6 Physical Infrastructure Standards

The Service Providers shall comply with:

4.6.1 At least TIER (3) requirements for Design, Construction and Operations of their data centers in case of geo-redundant core nodes.

4.6.2 At least TIER (2) requirements for Design, Construction and Operations of their data centers in case of pooling of core nodes.

4.6.3 In case of following different definitions from (4.6.1) and (4.6.2), similar or higher standards must be applied.
4.6.4 Submit to CICT the required certification from an accredited certification body.

4.6.5 At least (3) different connected routes to all the technical buildings.

4.7 Power

The Service Provides shall implement a range of controls to achieve the power resiliency by:

4.7.1 All the technical buildings hosting core nodes and hub sites must have redundant power systems capable of handling the disruption of the main power source following the periods stated in the instructions issued by the related authorities toward providing power sources in their locations.

4.7.2 Mobile towers that are providing coverage shall have redundant power units capable of handling disruption of the main power source with at least 96 hours.
5. Documents to be submitted

5.1 The Service Providers shall submit annually:
   
   a) BCPs based on their BCM approach (by processes, activities, assets, locations, services).
   
   b) Disaster Recovery Plan for ICT.
   
   c) RA and BIA results.
   
   d) BC exercising, Resiliency, DR and DR site testing plan schedules.
   
   e) List of Core Telecommunication Assets and their resiliency concepts.

5.2 The Service Providers shall submit the following supporting plans annually:

   a) Incidents Response Plan.
   
   b) Emergency Response Plan.
   
   c) Crisis Management Plan.


6.1 This document shall be regularly revised by CITC and updated accordingly. Any updates to this document shall be approved by CITC Governor.

6.2 The Service Provider shall incur all the costs required to fulfill the obligations stated herein.

6.3 The Service Provider shall submit any reports or data requested by CITC toward the obligations in this document.

6.4 Any report or data submitted to CITC toward the Service Provider’s obligations would be subject to review and audit, and in case of noncompliance as required the Service Providers shall provide an explanation as to why the obligations were not achieved and what measures would be taken to fulfill those obligations within a period of time determined by CITC at its discretion.

6.5 In case of noncompliance from the Service Providers with the obligations stated herein, CITC is entitled to take any official actions against them, including fines, as stated in the Communications Regulation and the executive regulations thereof.
7. Annex:

Annex A: Table of Content for Business Continuity Plan

The Service Providers shall follow the below Table of Contents in the BCPs:

- BCM Organizational Structure.
- BCM Team, Roles and Responsibilities.
- Approvals (who approves the plan and the date).
- Revision History.
- Objectives.
- Scope.
- RA and BIA Results.
- Resources.
- Incident Management Teams, Roles and Responsibilities.
- BCP Activation Criteria.
- BCP Activation Owner.
- BCP Activation Process.
- Recovery Strategy for all the Scenarios.
- Recovery Process.
- Internal and External Communication Plan.
Annex B: Table of Content for Crisis Management Plan

The Service Providers shall follow the below Table of Contents – as a minimum- in the CMP:

- CMT Team Structure.
- CMT Team Roles and Responsibilities.
- CMT Team Contact Details.
- CMP Activation Criteria.
- Internal and External (Including Media) Communication Plan.
Annex C: Table of Content for Testing Results

The Service Providers should follow the below Table of Contents in their testing results reports:

- Objectives of the test.
- Test scenario.
- Nodes/ system to be tested.
- Success criteria for each node/ system.
- Report on success and issues encountered.
- Actions to be taken if failure.
- Lessons learned.
- Re-testing date, if a total or partial failure was encountered.