ESCCOM

ESWATINI COMMUNICATIONS COMMISSION

DRAFT BUSINESS CONTINUITY (BC) AND DISASTER RECOVERY PLANNING (DRP) GUIDELINES FOR THE ICT (ELECTRONIC COMMUNICATIONS) INDUSTRY

2022

Contents

1.Interpretation

For the purpose of these guidelines, unless the context otherwise requires;

Asset: means a function consisting of a delimited part of a communications network or communications service and which is necessary to provide such a network or service, and which is used to transmit, receive, process or store information;

Business Continuity: means the capability of the organization to continue delivery of products or services at acceptable predefined levels following disruptive incidents;

Business Continuity Plan: means documented procedures that guide Regulated Entity's to respond, recover, resume, and restore to a pre-defined level of operation following disruption;

Business Impact Analysis: means the process of analyzing activities and the effect that a business disruption might have upon them;

Checklist Test: means a process whereby the Disaster Recovery team goes through each step of the plan in order to identify weaknesses or gaps;

Crisis: means a situation with a high level of uncertainty that disrupts the core activities and/or credibility of a Regulated Entity and requires urgent action;

Disaster: means any event that renders a business facility inoperable or unusable such that it interferes with the Regulated Entity's ability to deliver essential business services;

Disaster Recovery: means a set of policies, tools and procedures to enable the continuation of vital technology infrastructure and systems following a natural or human induced disaster;

Disaster Recovery Plan: means a business plan that describes how work can be resumed quickly and effectively after a disaster;

Full Interruption Tests: means a process where the actual production data and equipment are used to test the Disaster Recovery plan;

Incident: means a situation that might be, or could lead to, a disruption, loss, emergency or crisis;

Personnel: means people working for and under the control of the Regulated Entity;

Parallel Test: means a process were the recovery systems are built/set up and tested to see if they can perform actual business transactions to support key processes while the primary systems still carry the full production workload;

Recovery Point Objective: means the point to which information used by an activity must be restored to enable the activity to operate on resumption;

Recovery Time Objective: means the period of time following an incident, within which a product of service must be resumed, or activity must be resumed, or resources must be recovered;

Regulated Entity: means any person or entity that provides Telecommunications, Internet and Information and Communication Technologies, Radio Communications, Broadcasting and Postal Services;

Resources: means all assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that a Regulated Entity has to have available to use, when needed, in order to operate and meet its objective;

Risk: means the effect of uncertainty on objectives (Source ISO/IEC Guide 73);

Risk Assessment: means the overall process of risk identification, risk analysis and risk evaluation;

Services: means beneficial outcomes provided by a Regulated Entity to its customers, recipients and interested parties;

Simulation Test: means a scenario-based test which focuses on a specific type of disasters or business disruptions. It may involve role-playing and actual physical testing of alternate sites and equipment, as well as coordination with vendors and others;

Test: means an exercise whose aim is to obtain an expected, measurable pass or fail outcome; and

Threat: means a potential cause of unwanted incident, which can result in harm to individuals, the environment or the community.

2. Introduction

Advancements in Information and Communication Technologies (ICTs) have profoundly changed society, and will continue to do so in the foreseeable future, as ICTs have permeated virtually every aspect of human life. Not only do ICT solutions and products have the transformative potential to alter (for the better) the socio-economic realities of the people, but they have proven that they can deliver on the promise for improved service delivery, better opportunities for the people and their general well-being. The government and the people of the Kingdom of Eswatini have realized that ICT has become a strategic resource, a commodity and a foundation of most activities that can play major roles in many key sectors of the economy including education, health, commerce, and poverty alleviation. This is achieved through the introduction of efficiencies in service delivery, creation of new businesses and job opportunities as well as transforming the country into a knowledge-based economy.

Moreover, the Communications Sector is an integral component of the Eswatini economy, underlying the operations of all private businesses, public safety organizations and government. The Communications Sector is critical because it provides an enabling function across all critical economic sectors. The sector is also critically important among the members of the public as it offers an opportunity to connect, source information and even for use of social services. In this regard, Eswatini has seen an increasing usage of ICT services by the country's citizens. This has made the provision and continued availability, quality and reliability of such services to be of critical importance. With the increased usage of communications services, tolerance for downtime and unavailability of services decreases, business continuity and disaster recovery gain importance. This understanding has made the Commission to, in line with the mandate outlined in the founding legislation, come up with these regulatory guidelines on disaster recovery planning aimed at ensuring that electronic communications services are always available within the country.

Specifically, the Commission is required to provide information and issue guidelines or codes to the public and to commercial entities with respect to the matters which the Commission regulates, as well as promoting the delivery of quality communications services. These practices enable a Regulated Entity to get back on its feet after problems occur, reduce the risk of business disruption, data loss and reputational harm, and improve operations while decreasing the chance of service disruption.

2.1. Purpose

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

a. To ensure continued availability of electronic communications services within the Kingdom of Eswatini;
b. to supplement the Regulatory Framework for Quality of Service for the ICT Industry in the Kingdom of Eswatini
c. to provide specific guidance for Regulated Entities:
    i. to encourage good practices with respect to establishing disaster preparedness/prevention procedures by the licensees
    ii. to enable a consistent approach towards Disaster Recovery planning by the licensees.

3. Disaster Recovery Planning Guidelines

3.1. General Principles

a) The Regulated Entity shall develop business continuity plans which must always include a disaster recovery plan in order to assure continuous or uninterrupted service provision. The business continuity plans shall comprise both normal operating conditions and extraordinary events or incidents. Such incidents shall include,

among others, power outage, cable theft, high traffic, equipment and software failure, changes on equipment and software, cyber-attacks and natural disasters.

b) The Business Continuity Plans must include preventative controls, for example, maintaining and checking systems, scheduled software updates, network upgrades and documented processes of daily business operations.

c) The Regulated Entity shall also develop disaster recovery plans which shall detail all the steps that they must follow and take to resume business operations following a disaster.

d) The Business Continuity and Disaster Recovery plans shall have a clear division of roles with specifically designated personnel responsible for Business Continuity and Disaster Recovery.

e) The Regulated Entity shall adopt any relevant standard(s) in the development of business continuity and disaster recovery plans.

f) The Regulated Entity shall file the Business Continuity and Disaster recovery plans with the Commission and any updates thereafter. The Commission will ensure the confidentiality of these plans.

3.2. Scope of Business Continuity and Disaster Recovery Plans

a) The Regulated Entity shall clearly define which areas of the organization the business continuity and disaster recovery shall be applied to. This shall be in accordance with the entity's identified business requirements and objectives. The entity shall outline the objectives of the business continuity and disaster recovery and how it will control the same.

3.3. Records Management

b) The Regulated Entity shall document all relevant information that have a direct impact and relation to the Regulated Entity's business continuity plan. This shall include both internal and external documents. Internal documents shall include, amongst others, licences, company policies, contractual agreements, business processes, project documentation, business continuity and disaster recovery documents. External documents shall include, amongst others, different types of correspondence with relevant stakeholders or parties.

3.4. Documentation of Assets

1) The Regulated Entity shall document all its assets and network links where applicable in its asset register.
2) The Regulated Entity shall document, amongst others, the following:
   i. A unique description (example, make or model);
   ii. The functionality of the asset or network link;
   iii. The geographical location of the asset or network link; and
   iv. A reference to the current risk analysis for the asset or network link.

3.5. Risk and Impact Analysis

1. The Regulated Entity shall, at least once a year assess the business risks that cause disturbances or interruption of its services and identify the strategies to mitigate the risk the business is exposed to.
2. The Regulated Entity shall conduct risk analysis before the development of business continuity and disaster recovery plans of such incidents that could affect service availability of the communications services. The Regulated Entity shall record and update the risk assessment report after every incident. The Regulated Entity shall also report such service disruptions or

interruptions to the Commission in accordance with the Quality of Service Regulations, License Conditions, and/or any other relevant regulatory instruments.

3. The risk analysis shall include, but not limited to the following:
    i. Identification of critical business functions and assets essential for continued service delivery;
    ii. Identification of all potential threats and relevant incidents against the business functions and assets. Threats related to weather and intrusion and other external impact must always be analyzed;
    iii. Assessment of the consequences in the event of identified threats occurring;
    iv. Assessment of the probability of identified threats occurring; and
    v. Consolidated assessment of the probability of identified threats occurring and the consequences they may bring about if they occur (risk assessment).
4. In performing the risk analysis, the Regulated Entity shall consider the history of incidents that occurred in specific areas and apply relevant measures.
5. The Regulated Entity shall have a plan regarding the times and situations the entity will conduct risk analysis. For areas that experience consistent disruptions or interruptions, the Regulated Entity shall conduct a risk and impact analysis and come up with mitigation measures.
6. The Regulated Entity shall document the conducted risk and impact analysis.

3.6. Business Continuity Management

1. Business Continuity Management must include the following plans;
    a. incident response

b. business continuity
c. disaster recovery
d. communication
e. training and awareness
f. testing plans

1.1. Incident Response plan

a. The Regulated Entity shall update its plans whenever there are changes in the business, industry or the location it operates in.
b. An incident response plan should define the procedures of responding to different types of incidents or crisis. These procedures should address all the major risks an organization might face. It should outline the actions that need to be taken to limit the disruption of service and loss of infrastructure during and after an incident.
c. An incident response plan shall include but not be limited to the following:
    i. Plan activation details, including a clear statement of the circumstances when the plan will be activated and the person authorized to do so;
    ii. Incident response team details, including key roles and responsibilities;
    iii. A communication plan, including key communication methods and timings needed to keep everyone safe;
    iv. Contact lists of Interested Parties which the Regulated Entity will need to communicate with during a crisis, including staff and emergency services; and an event log to record information, decisions and actions that should be taken during a crisis, including staff and emergency services;
    v. Event log to record information, decisions and actions that should be taken during a crisis.

1.2. Business Continuity Plans

a. A Business Continuity Plan shall outline procedures on responding to incidents that might disrupt services with an objective to resume service provision timely and minimize losses. It shall also outline the time frame in which the Regulated Entity can realistically expect to resume to usual business operations.

b. The Business Continuity Plan should include but not be limited to the following:
   i. Strategies to recover business activities in the quickest possible time;
   ii. Priority services to be restored, indicating order of recovery;
   iii. A description of key resources, equipment and staff required to recover business operations;
   iv. Clear Recovery Point Objective (RPO) and Recovery Time Objective (RTO);
   v. Backup procedures of critical software, data, power and any other critical resources; and
   vi. Key processes and technologies that need to be resuscitated and important infrastructure and assets.

1.3. Disaster Recovery Plans

a. The Disaster Recovery Plan shall capture all the information that describes the business ability to withstand disaster as well as the processes that must be followed to recover from disaster and/or unexpected event and resume business operations. The plans shall be developed in such a way that priority or emergency services are fully accessible during the event of a disaster.
b. The disaster recovery plan should include but not limited to the following:

i. A statement of goals that will outline what the entity wants to achieve during or after a disaster, including the recovery time objective (RTO) and the recovery point objective (RPO). The recovery point objective refers to how much data (in terms of the most recent changes) the company is willing to lose after a disaster occurs and Recovery time objective or RTO refers to the acceptable downtime after an outage before business processes and systems must be restored to operation.
ii. The plan must detail the personnel who are responsible for the execution of the DR plan, and make provisions for individual people becoming unavailable.
iii. An updated IT inventory must list the details about all hardware and software assets, as well as any cloud services necessary for the entity's operation, including whether or not they are business critical, and whether they are owned, leased, or used as a service.
iv. The plan must set forth how each data resource is backed up – with exact location, on which devices and in which folders, and how the team should recover each resource from backup.
v. Disaster recovery procedures - these specific procedures, distinct from backup procedures, should detail all emergency responses, including last-minute backups, mitigation procedures, limitation of damages, and eradication of cybersecurity threats.
vi. Disaster recovery site – the plan should designate a hot disaster recovery site. Located remotely, all data can be frequently backed up to or replicated at a hot disaster recovery site — an alternative data center holding all critical systems. This way, when disaster strikes, operations can be instantly switched over to the hot site.

vii. Restoration procedures - The disaster recovery plan should include restoration procedures for recovering from a loss of full systems operations. In other words, every detail to get each aspect of the business back online should be in the plan.

1.4. Testing Plans

a. Testing is crucial for the improvement of the Business Continuity Plans. Procedures to test the business continuity plans should be documented, but only accessible by the Commission. It is essential that the plan be thoroughly tested and evaluated on a regular basis, at least annually to ensure that they are still effective.

b. The plan should be updated to correct any problems identified during the test.

Types of tests shall include:

i. Checklist;
ii. Simulation
iii. Parallel; and
iv. Full recovery or interruption tests.

c. The tests will provide the company with the assurance that all necessary steps are included in the plan. Other reasons for testing include:

1. Determining the feasibility and compatibility of backup facilities and procedures;
2. Determine the plan's effectiveness, identify gaps, bottlenecks and weaknesses;
3. Identifying areas in the plan that need modification;
4. Providing training to the team managers and team members;
5. Demonstrating the ability of the company to recover; and
6. Providing motivation for maintaining and updating the business continuity plan.

d. Where certain functions within the company are outsourced or processed by a third-party (i.e. maintenance, signal distribution, power) the Regulate Entity shall:

    i. Evaluate the adequacy of the third party's business continuity plan and its compatibility with the plan of the Regulated Entity.

1.5. Communication Plans

a. These procedures must cover decisions as to whether the risks and impacts are to be communicated externally, and how to communicate with interested parties, particularly with the Commission.
b. The objective is to clearly define the responsible personnel for conveying relevant information to the internal staff, relevant Authorities, public, and media. Templates may be developed for communicating with media, which will help the Regulated Entity to issue press releases quickly, if needed. These will also be helpful in the event the person responsible for communications is not available.
c. Communication to the Commission
d. In the event of a disaster, the Regulated Entity shall notify the Commission detailing the following:
    1. Nature of the disaster;
    2. Location of the affected area or site and services;
    3. Magnitude of the disaster;
        i. Damaged infrastructure or resources,
        ii. Affected customers or network coverage,
    4. Impact of the disaster;
    5. Planned measures to overcome the disaster; and
    6. Anticipated timelines for service restoration.
e. During service disruption, the Regulated Entity shall provide regular updates to the Commission and other affected stakeholders, including customers.

f. After normalizing the situation, the Regulated Entity shall provide a detailed root cause analysis report to the Commission within 5 working days.

1.6. Training and Awareness Plans

b. Training and awareness plans are a vital component for the successful execution of critical procedures to be followed during the event of a disaster. A detailed plan shall be developed and subject to regular reviews and updates. The Regulated Entity shall identify a Business Continuity and Disaster Recovery team that shall be responsible for the specific roles and functions. Frequent training is critical, so the team can do its assigned roles safely and respond appropriately when there is an incident.

4. Submissions to the Commission

1. The Regulated Entity shall submit the following to the Commission:
    a. Business Continuity and Disaster Recovery Plans every five (5) years, or such other shorter period as the Regulated Entity or Commission may decide from time to time;
    b. Risk and Impact Analysis Reports at least annually; and
    c. Reports of occurring incidents and updates every quarter as part of the quarterly compliance report.