Notice Number: SECZ SS-ICT13/11/17

Business Continuity Management Guidelines

Table of Contents

1. Introduction

The adoption of technologies enabling interoperability and straight through processing exposes the Zimbabwe Capital Markets to a wide array of both planned and unplanned events that may cause operational disruptions. Implementation of robust Business Continuity Management (BCM) practices becomes imperative.

Business Continuity Management ensures Investors receive a continuous service that is not interrupted by unplanned events thus cultivating confidence in the Zimbabwe Capital Markets. Securities Market Intermediaries (SMI) must ensure that mission critical applications and information are highly available in the event of any form of operational interruptions.

In issuing these guidelines, the Securities and Exchange Commission (SECZ) recognizes the need for SMIs to implement effective BCM that will ensure their ability to operate on an ongoing basis and limit losses in the event of an operational disruption.

Effective Business Continuity Management typically incorporates:

i. A thorough Business Impact Analysis and Risk Assessment
ii. Identification of key products and services, and critical business functions
iii. Identification of potential risks that may cause disruptions
iv. Identification of financial and non-financial impact of potential disruptions
v. Formulation and implementation of viable recovery strategies and plans
vi. Awareness, Training, Exercising and Testing of these plans
vii. Independent audit of the BCM plan and BCM test results and
viii. Review by the senior management and board of directors.

ix. Regular maintenance, review and updating of the analysis, strategies and plans, to have the assurance and peace of mind that the plans continue at all points in time to support the changing needs of the organization.

2. Objectives of the Guidelines

The guidelines set minimum requirements for establishing effective Business Continuity Management (BCM) practices in the Zimbabwe Capital Markets. The guidelines shall apply to all market participants registered or licensed by the Securities and Exchange Commission of Zimbabwe (SECZ).

3. BCM Policy Establishment

3.1. Business Continuity Management Policy

Securities Market Intermediaries shall establish a Business Continuity Management high level policy statement that sets out

i. Scope, aims and objectives of BCM in the organisation; and
ii. The activities that will be required to deliver these.

The policy should stipulate deliverables, key roles and responsibilities and how the BCM will be governed.

The objectives of BCM are the expression of the intent of the organization to treat the risks identified and/or to comply with requirements of organizational needs. The business continuity objectives must:

i. Be consistent with the business continuity policy;
ii. Take into account the minimum level of products and services that is acceptable to the organization to achieve its objectives;
iii. Be measurable;
iv. Take into account applicable requirements;

v. Be monitored and updated as appropriate.

3.2. Board and Senior Management Responsibility

Board of directors and senior management are responsible for the organisation's Business Continuity Management.

The board of directors is responsible for:

i. Approving BCM policies, standards and principles developed by senior management;
ii. Ensuring compliance with regulatory and legal requirements for BCM

Senior management is responsible for:

i. Ensuring the BCM is compatible with the strategic direction of the organization;
ii. Integrating the BCM requirements into the organization's business processes;
iii. Providing the necessary resources for the BCM;
iv. Communicating the importance of effective business continuity management;
v. Ensuring that the BCM achieves its expected outcomes;
vi. Directing and supporting continual improvement;
vii. Establish and communicate a business continuity policy;
viii. Ensuring that BCM objectives and plans are established;
ix. Ensuring an organisational culture that places a high priority on business continuity
x. Ensuring that the responsibilities and authorities for relevant roles are assigned.
xi. Ensuring testing and review of business continuity plans at least once per annum

4. BCM Program Operations

4.1. Business Impact Analysis (BIA)

Securities Market Intermediaries shall conduct organisation-wide Business Impact Analysis (BIA) to identify business functions that are mission critical and potential losses (financial and non-financial) in case of any disruptions.

The purpose of the business impact analysis (BIA) is to:

i. Identify which business units/departments and processes are essential to the survival of the organisation
ii. Identify how quickly essential business units and/or processes have to return to full operation following a disaster situation.
iii. Identify the resources required to resume business operations.

A BIA should generally gather information that includes the following as a minimum:

i. Complete list of services (prioritised in terms of direct/indirect revenue and other key factors).
ii. Critical processes to support the most important services (with time-critical details).
iii. Financial impacts of loss of service i.e. loss of revenue, regulatory fines, breach of contract claims.
iv. Intangible impacts of loss of service i.e. company reputation, customer service, public image, shareholder relations, market share
v. List business process Recovery Time Objectives (RTOs), business process Recovery Point Objectives (RPOs) and business process Maximum Tolerable Downtime (MTD).
vi. List recovery options for each mission critical business process.
vii. Key staff to support the critical processes.

viii. Key systems, records and equipment to support the critical processes.

ix. Reliance on internal departments to carry out the critical processes.

x. Reliance on specific premises to carry out critical processes.

xi. Reliance on suppliers/partners whom you depend on to undertake critical processes.

xii. Key customers and stakeholders who would be impacted by the loss of products/services.

BIA information gathering techniques may include one-on-one interviews, workshops and questionnaires.

4.3. Risk Assessment

SMIs need to identify what risks could disrupt the key functions and services that have been identified within the BIA. The Risk Assessment conducted at least once a year looks at the likelihood and impact of a variety of risks that could cause a disruption to an organisation.

Identified risks could include:

- Loss of staff
- Loss of systems (IT and telecommunications)
- Loss of utilities e.g. water, or electricity
- Loss of, or access to, premises
- Loss of key suppliers
- Disruption to transport

The risk assessment should focus on the critical activities and supporting resources identified in the BIA stage. For this reason a risk assessment can only take place once a BIA has been completed.

Risk assessment is at minimum expected to achieve the following:

i. Identify unacceptable concentrations of risk and 'single points of failure'
ii. Identify internal and external threats that could cause a disruption and assess their probability and impact;
iii. Prioritize threats according to the institution;
iv. Provide information for a risk control management strategy and an action plan for risks to be addressed;
v. Mitigation of risks through a documented remedial plan;
vi. Ensure BCPs are updated regularly to reflect the changes in the institution's operational risk profile;
vii. Specify events that should prompt implementation of the plans;

Using a risk assessment matrix similar to the one below (figure1), a plot of risk likelihood identified against the impact as previously identified in the **BIA** can be created.

Likelihood	Impact				
	Insignificant	Minor	Moderate	Major	Severe
Almost certain	Moderate	High	High	Extreme	Extreme
Likely	Moderate	Moderate	High	High	Extreme
Possible	Low	Moderate	Moderate	High	Extreme
Unlikely	Low	Moderate	Moderate	Moderate	High
Rare	Low	Low	Moderate	Moderate	High

Figure1 – Example of a Risk Assessment Matrix

The plot enables ranking the risks and making an informed decision about what action to take. The options of action to take are:

i. **Treat** – use of **BCM** to reduce disruption by ensuring the activity continues at, or is recovered to, an acceptable minimum level (**RTO**) and timeframe stipulated in the **BIA**.

ii. **Tolerate** – you may decide that you are willing to accept the risk as the cost of implementing any risk reduction strategies outweigh the benefits.

iii. **Transfer** – for some risks the best response may be to transfer them. This might be done by conventional insurance or contractual arrangements, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets.

iv. **Terminate** – in some circumstances it might be appropriate to change, suspend or terminate the service, product, activity, function or process. This option ought only to be considered where there is no conflict with the organisation's objectives, statutory compliance and stakeholder expectation. This approach is most likely to be considered where a service, product, activity, function or process has a limited lifespan.

4.4. Business Continuity Strategy

After requirements have been established through the BIA and the risk assessment, strategies should be developed to identify arrangements that will enable the organization to protect and recover critical activities based on organizational risk tolerance and within defined recovery time objectives.

SMIs shall set up and maintain appropriate strategies in respect of people, premises, technology, information, suppliers/partners and stakeholders. Find below some of the tactics that you could adopt to protect your resources but should not be seen as an exhaustive list:

a) People

Managing people's core skills and knowledge by:

i. Keeping inventory of staff skills not utilised within their existing roles - to enable redeployment
ii. Process mapping and documentation - to allow staff to undertake roles with which they are unfamiliar
iii. Multi-skill training of each individual
iv. Cross-training of skills across a number of individuals
v. Succession planning and staff retention policies
vi. Use of third party support, backed by contractual agreements i.e. outsourcing skill
vii. Geographical separation of individuals or groups with core skills can reduce the likelihood of losing all those capable of undertaking a specific role

b) Premises

Reducing the impact of unavailability of the primary site by:

i. Relocation of staff to other premises owned by your organisation such as training facilities.
ii. Displacement of staff performing less urgent business processes with staff performing a higher priority activity. Care must be taken when using this option that backlogs of the less urgent work do not become unmanageable.
iii. Enable remote access by staff – this can be working from home or working from other locations.
iv. Use alternative premises provided by other organisations, including those provided by third-party specialists

c) Technology

Establishing technology strategies which may include:

i. Investing in highly resilient technology infrastructure i.e. recovery site automatic failover, redundant backup telecommunications links, backup Internet and Telephony services, cloud computing.
ii. ICT application recovery options based on defined priority e.g. automated fail-over, manual fail-over, hot-site, warm-site, cold-site, acquisition at time of disaster
iii. Identify and minimise risks posed by single points of failure e.g. Trading System, Depository System, network switch, network storage
iv. Escrow software agreements with proprietary software vendors, to ensure access to source code in the event vendor shuts down operations.
v. Entering infrastructure sharing arrangements.
vi. Making additional arrangements for specialized or not readily available ICT equipment i.e. multiple sources.
vii. Maintaining the same technology at different locations that will not be affected by the same business disruption.
viii. Holding older equipment as emergency replacement or spares.

d) Information

Establishing strategies to ensure information protection and recoverability by:

i. Ensuring data is backed-up and it is kept off site.
ii. Storing essential documentation securely (e.g. fire proof safe)
iii. Ensuring copies of essential documentation are kept by multiple custodians at different locations.
iv. Storage of information in both physical and electronic format
v. Outsourcing of information custody and archiving e.g. online data hosting services

e) Suppliers and Partners

Instituting strategies for supplies needed for critical operations, which may include:

i. Facilitating storage of additional supplies at another location
ii. Establishing multiple sources of supplies
iii. Identification of alternative suppliers and substitute goods/services
iv. Encouraging or requiring suppliers/partners to have a validated business continuity capability
v. Implementing significant penalty clauses on supply contracts
vi. Arranging with suppliers to deliver stock at short notice

f) Stakeholders

Instituting strategies for managing relationships with key stakeholders i.e. employees, regulators, auditors and media by:

i. Putting in place mechanisms to provide stakeholders with accurate information in a timely manner
ii. Making arrangements to ensure vulnerable groups are accommodated

4.5. Business Continuity Plan and Procedures

All SMIs shall develop and maintain a comprehensive business continuity plan (BCP) based on their business impact analysis, recovery objectives and risk assessment.

The organization shall document procedures to ensure continuity of activities and management of disruptive incidents. The Business Continuity Plan has to:

i. Define an institution-wide BCP awareness program

ii. Establish an appropriate internal and external communications protocol ;

iii. List the critical processes in priority order for recovery;

iv. Establish staff roles and allocate responsibilities for managing operational disruptions;

v. Contact details of team members and other parties i.e. contractors, service providers and suppliers;

vi. Provide clear guidance regarding the succession of authority in the event of a disruption that disables key personnel;

vii. Define the triggers for invoking the organisation's business continuity plan and provide detailed activation procedure;

viii. Be detailed and specific regarding the response actions that are to be taken following a disruption (Incident Response Plan);

ix. Prioritise safety of employees through adequate emergency evacuation procedures and accounting for all staff during an incident.

x. Be flexible to respond to unanticipated threats and changing internal and external conditions;

xi. Focus on the impact of events that could potentially disrupt operations;

xii. Address relocation to an alternate site in the event of a major disruption;

xiii. Define data backup and recovery processes (hard copy and electronic)

xiv. Define processes to deal with loss of data not available from data backup i.e. recapturing transactions

xv. Define processes enabling switching to backup telecommunications systems (telephony and data)

xvi. Be developed based on stated assumptions and an analysis of interdependencies; and;

xvii. Be effective in minimizing consequences through implementation of appropriate mitigation strategies.

xviii. Determine what types of insurance are available and put in place the insurance your business needs.

xix. Specify a review process to ensure that the BCP is feasible and up-to-date

4.6. Communication Protocols

SMIs should include in their BCM comprehensive protocols and procedures for communicating within their institutions and with relevant external parties in the event of an operational disruption.

The organization should draft in advance the message templates, scripts, and statements it may need to communicate with regulators, investors, customers, counterparties, business partners, staff, the media and other stakeholder groups regarding the disruptive incident. The organization should designate key and substitute official spokespersons especially those trained to interact with media and communicating with internal and external stakeholders.

External means of communications include:

- News or press releases
- Media
- Social media channels
- Financial reports
- Newsletters
- Websites
- Phone calls, emails and text messages (manually delivered and/or via automated emergency notification systems)

The organization's communications protocols should provide instructions and guidance to Senior Management, Executives, and Staff and Public Relations personnel on how to communicate approved messages with internal and external stakeholders before, during and after a disruptive event.

This plan should include a predefined structure of the process of gathering and publishing information on the emergencies, crises and disasters to internal and external stakeholders.

The plan should provide for regular updating and testing of call tree and other contact information at least quarterly.

4.7. BCM Exercising and Testing

Annual exercising and testing should be conducted for assessing the readiness, usability and appropriateness of the tools, technology, facilities, and infrastructure required for the implementation of the BC plans of the organization. Post-Test reports should be developed, revised and remedial measures taken, when required.

Exercising and testing are the processes of validating business continuity plans and procedures to ensure the selected strategies are capable of providing response and recovery results within the timeframes agreed to by management. An exercise and testing program is necessary to ensure all staff has a good understanding of their responsibilities as defined in the Business Continuity Plan. The Exercise and test plans typically consist of:

i. Training for managers, team members and external parties
ii. Roles and responsibilities for all personnel during an interruption event
iii. Internal and External communications plan exercising,
iv. Testing all procedure and processes included in exiting plans
v. Testing new processes and plans.

Exercising and test programs can be a combination of the following exercises:

Type of Exercise	Objectives of the exercise
Walkthrough Exercise (workshops or	To check the structure and elements of the plan and verifying if a BC plan is current, accurate and complete.
Tabletop Exercise (desktop)	To test the BCM plan against different scenarios i.e. single or multiple events/incidents.
Live Exercise	Verifying how BC plans are implemented on the ground using real resources. Confirm full recovery of a complete set of activities within
Test Exercise	Benchmarking responses against key performance indicators e.g. testing RTOs and RPOs. Test exercises normally focus on ICT systems.

Exercises should be evaluated to determine whether exercise objectives were met and to identify opportunities for program improvement. A facilitated discussion held at the end of an exercise is a great way to solicit feedback and identify suggestions for improvement. Evaluation forms are another way for participants to provide comments and suggestions. An after-action report that documents suggestions for improvement should be compiled following the exercise and copies should be distributed to management and other interested parties.

4.8. BCM Awareness and Training

SMIs shall embed BCM in their organisational culture through raising awareness and continuous training of staff.

All new staff should be made aware of the organisation's BCM arrangements on joining and this should form an integral part of the induction process. Mechanisms for raising awareness include:

- involving staff in the development of the organisation's BCM strategy;
- written and oral briefings;
- learning from internal and external incidents; and
- discussion based exercises i.e. Walkthrough and Desktop/Tabletop

It is good practice to ensure that all staff members who have business continuity responsibilities receive training on BCM.

5. BCM Program Review and Maintenance

5.1. BCM Audit

A formal Business Continuity Audit process should ensure the entity has an effective Business Continuity capability program. The purpose of a Business Continuity audit is to:

i. Ensure compliance with the entity's BCM policies and procedures;
ii. Review the entity's BCM solutions;
iii. Verify the entity's BCM plans;
iv. Verify that appropriate exercise and maintenance activities are available;
v. Highlight deficiencies and compliance gaps;
vi. Ensure the remedy of such gaps.
vii. Audits should be conducted on a regular basis, as defined in the entity's audit and governance policies.

5.2. BCM Annual Review and Continual Improvement

On a regular basis, at least annually, each market participant is required to perform a review of it's:

i. Business Impact Analysis,
ii. Risk Assessment,
iii. Business Continuity Strategy,
iv. Business Continuity Plans, and
v. BCM Testing and Exercise.

This review is designed to ensure all Business Continuity capability documents are valid and consistent with the entity's strategic objectives. Reviews and updates are necessary when a change occurs in the entity or when a change occurs within Senior Management.

The review should be formally conducted by an auditor or Business Continuity resource and a Business Continuity capability report presented to Senior Management. The report should also address any non-conformities and risks requiring treatment that either carry over from or have been identified since the previous report.

Appendices

Appendix 1 - Glossary

Term	Definition
Alternate Site	A site held for readiness for use during a Business Continuity event to maintain the business continuity of an organization. The term applies equally to office or technology requirements. Alternate sites may be cold, warm or hot. This type of site is also known as a Recovery Site.
Activity	A process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products or services
Audit	A systematic examination to determine whether activities and related results conform to planned arrangements and whether these arrangements are implemented effectively and are suitable for achieving the organization's policy and objectives.
Backup	A process, by which data, electronic or paper based, is copied in some form so as to be available and used if the original data from which it originated is lost, destroyed or corrupted.
Business continuity	Strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level
Business continuity management (BCM)	A holistic management process that identifies potential threats to an organization and the impacts to business

Term	Definition
	operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business continuity plan (BCP)	A documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident to enable an organization to continue to deliver its critical activities at an acceptable pre-defined level
Business Continuity Strategy	An approach by an organization that will ensure its recovery and continuity in the face of a disaster or other major incident or business disruption
Business Impact Analysis (BIA)	The process of analysing business functions and the effect that a business disruption might have upon them
Cold Site	Office or datacenter space without any server equipment installed. Servers and equipment have to be migrated to cold site in the event of a significant outage at the main datacenter.
Critical activities	Those activities which have to be performed in order to deliver the key products and services which enable an organization to meet its most important and time-sensitive objectives
Disruption	Event, whether anticipated (e.g. a labour strike or hurricane) or unanticipated (e.g. a blackout or earthquake), which causes an unplanned, negative deviation from the expected delivery of products or services according to the organization's objectives
Escrow Agreement	A legal document that outlines the terms and conditions between parties involved in an escrow arrangement. An escrow agreement defines the arrangement by which one party deposits an asset with a third person (called an escrow agent), who, in turn, makes a delivery to another party if and when the specified conditions of the contract are met
Exercise	Activity in which the business continuity plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result

Term	Definition
	when put into effect
Hot Site	A mirror of existing datacenter operations where production environment runs concurrently with main datacenter. Hot site enables immediate change over in the event of a disaster with minimum impact and downtime.
Impact	Evaluated consequence of a particular outcome
Incident	Situation that might be, or could lead to, a business disruption, loss, emergency or crisis
Market Participant	Individual or entity licensed/registered by the Securities and Exchange Commission of Zimbabwe
Maximum Tolerable Downtime (MTD)	Duration after which an organization's viability will be irrevocably threatened if product and service delivery cannot be resumed
Non-conformity	Non-fulfillment of a requirement organization group of people and facilities with an arrangement of responsibilities, authorities and relationships
Process	A set of interrelated or interacting activities which transforms inputs into outputs
Recovery Point Objective (RPO)	The maximum targeted period in which data might be lost from an IT service due to a major incident. Simplified, the RPO gives a target for maximum data loss
Recovery Time Objective (RTO)	The targeted duration of time within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity. The RTO sets a goal for maximum downtime in case of a disaster.
Resilience	Ability of an organization to resist being affected by an incident
Resources	All assets, people, skills, information, technology (including plant and equipment), premises, and supplies and information (whether electronic or not) that an organization has to have available to use, when needed, in order to operate and meet its objectives

Term	Definition
Risk	Something that might happen and its effect(s) on the achievement of objectives
Risk Assessment	Overall process of risk identification, analysis and evaluation
Senior management	Person or group of people who direct and control an organization at the highest level
Single point of failure	A unique source of service, activity and/or process where there is no alternative and whose loss could lead to the failure of a critical function
Stakeholders	Those with a vested interest in an organization's achievements
Warm Site	Offers office or datacenter space with pre-installed server hardware. Servers are ready for the installation of production environments.

For and On Behalf of Securities and Exchange Commission of Zimbabwe

T. Chinamo

Chief Executive Officer **13.11.2017**