BUSINESS CONTINUITY PLAN GUIDELINES

FINANCIAL SERVICES AUTHORITY

Bois De Rose Avenue
P.O. Box 991
Victoria
Mahé
Seychelles

Tel: +248 4380800
Fax: +248 4380888
Website: www.fsaseychelles.sc
Email: enquiries@fsaseychelles.sc

Version: 01st September 2022

Table of contents

DRAFT

DRAFT

1. INTRODUCTION

1.1 The Financial Services Authority ("the Authority/FSA") is issuing the Business Continuity Plan ("BCP") guidelines to provide guidance to regulated entities and licensees ("licensees") in creating and submitting their BCP to the Authority as and when required. The BCP will assist the Authority in evaluating the licensees' ability to continue to provide services through an effective standard of operation in the event that unforeseen situations occur.

1.2 Operating disruptions can occur with or without warning, and the results may be predictable or unknown. As the licensees contributes and plays a crucial role in the Seychelles economy, it is important that their business operations are and remain resilient to the effects of disruptions in services in order to maintain the public trust and confidence in our financial system. Effective business continuity planning establishes the basis for businesses to maintain and recover business processes when operations have been disrupted unexpectedly.

1.3 Business Continuity Planning is the process whereby it requires the licensees to ensure the maintenance or recovery of operations, including services to customers, when confronted with adverse events such as natural disasters, technological failures, human error, or terrorism. The objectives of a business continuity plan are to: -

(a) minimize the financial loss to the business;

(b) continue to serve customers and financial market participants;

(c) minimize the negative effects disruptions can have on the business' strategic plans, reputation, operations, liquidity, credit quality, market position, and ability to remain in compliance with applicable laws and regulations; and

(d) aid in all other matters which regard to business disruptions.

1.4 Change in business processes (internally in the business and externally amongst interdependent financial services companies) and new threat scenarios require that the licensee maintains updated and viable BCPs.

1.5 As such, licensees should incorporate business continuity considerations into their business process development to proactively mitigate the risk of service disruptions. In creating an effective BCP, the licensees should assume a reduced demand for services during the disruption and identify means to counteract the identified items or any other situations that may arise.

2. SCOPE

2.1 These guidelines aim to describe the "sound practice' that the FSA's licensees should have in place through a BCP, especially taking into consideration the recent technologies, change in business practices and increased concerns of the public, specifically in relation to services being offered.

DRAFT

2.2 In light of, the significant differences that exist in the organizational and legal structures of licensees and the nature and scope of the business activities conducted, the FSA recognizes that there exists no single set of universally applicable BCP framework that would be adequate for all licensees. As a result, the guidelines provided in this document serves as the minimum standards expected to be in place within licensees, to enable them to comply with relevant laws.

2.3 The Authority notes that the licensees might be impacted differently depending on their location and nature of their business, hence there could be various approaches to business continuity planning. Furthermore, the implementation and practical aspect may evolve over time depending on various situations that may arise.

2.4 **Appendix 1** provides a list of the possible threats that a business may encounter. Therefore, it is desirable for the licensees to design their own management framework that addresses their own particular risk profile, and to review such framework on an ongoing basis.

2.5 The BCP guidelines is applicable to all licensees listed below and as per their respective legislation:

(a) All licensees under the International Corporate Service Providers Act, 2003
(b) Insurance Companies – Insurance Act, 2008
(c) Insurance Brokers – Insurance Act, 2008
(d) All licensees under the Securities Act, 2007
(e) Fund Administrator - ~~All licensees under the~~ Mutual Fund and Hedge Fund Act, 2008

2.6 The BCP format will differ from one business to another, however, the general principle shall be applicable and incorporated to fit the nature and size of the business.

2.7 The FSA emphasizes that the contents of this Guidelines are neither intended to, nor should be construed as, an exhaustive treatment of the subject.

3. THE AUTHORITY'S VIEW OF THE BUSINESS CONTINUITY PLAN

3.1 *Significance of Business Continuity Plan*

Business continuity planning may be deemed essential for the following three reasons but not limited to:

(a) Maintaining the economic activity in the affected area

Business continuity planning enables the continuation of services during and after disasters, thereby contributing to sustaining economic activity in the affected area. Therefore, the BCP will assist licensees to function without any delays and supports the achievement of objectives.

(b) Preventing widespread payment and settlement disorder

Business continuity planning could prevent and identify possible defaults within the business, thereby serving to restrain widespread payment and settlement disorder. Payment and settlement services are at the foundation of economic activity and forms a linked chain throughout the society. Business continuity planning for the licensee helps in the continuation of transactions and payments, subsequently mitigating such systemic risks.

(c) Reducing managerial risks

The prolonged suspension of operations in a disaster situation makes it difficult for the licensee to take or make profit-wise decisions. As a result of such, it may lower their reputation among customers that may have detrimental impact on their management and the business survival. Therefore, business continuity planning is necessary in terms of mitigating these risks.

3.2 *Key points in business continuity planning*

The below points are for the consideration of the licensee:~~-~~

(a) Planning, testing, and reviewing

A robust risk management framework should be formulated so that licensees can continue to operate smoothly in the event of a disruption. It is more effective to start with plans specific to key business functions or priority locations, and then to gradually expand to cover other operations.

BCPs should be maintained and kept in ~~a~~ the licensees respective register, which shall be readily ~~made~~ available for the Authority to have sight of it during on-site compliance inspection or upon request by the Authority. Additionally, the licensee shall communicate and notify the Authority of any alteration within the BCP. Furthermore, the BCP shall be regularly tested and reviewed to ensure that they are practical and counteractive to the specific risks being targeted and identified and the information needs to kept on the licensees records.

For assurance on the functionality and effectiveness of its BCP, a licensee should design and carry out regular, complete and meaningful BCP testing that commensurate with the nature, scope and complexity of the licensee. For the tests to be complete and meaningful, the licensee should involve the service provider[1] in the validation of its BCP and assess the awareness and preparedness of its own staff. Similarly, the licensee may take part in its service providers' BCP and disaster recovery exercise in order to determine its effectiveness. Such testing evidence should be available at the FSA's request if and when requested.

[1] Means an individual or entity that provides services to the licensee. The provision of services between a service provider and a company is typically governed by a service agreement. Such may include but not limited to telecommunication providers, banks, individual consultants etc…

(b) Focusing on critical operations

Disasters result in limited access to managerial resources, especially under severe time constraints. Business continuity planning must therefore prioritize critical operations which are deemed essential for the business to continue in the event of a disruption.

(c) Considering special circumstances under large scale disruptions

Licensees have many options for responding to disruptions and providing for business continuity. Such includes switching over to back-up facilities, moving to manual processing, or entrusting operations to another business (which will ~~require the necessary approval with relevant authorities, agreements and written procedures for the hand-over of documents~~they will need to inform the Authority in such case and should be in line with the licensee's BCP). Assuming the possibility of large scale disruptions, the business should take into consideration the following, the list not being exhaustive:

(i) Avoid geographical concentration of main operational offices, information centers, and back-up facilities so as to reduce risk of simultaneous damage.

(ii) Be aware of the possibility that traffic suspension and other disruptions could prevent necessary staff from moving to back-up facilities on-time. Therefore, licensees with alternate operational offices should have procedures in place so that substitute staff may take up any necessary action or task instead of, or whilst, the affected staff relocate.

(iii) The possibility of staff fatigue and ensuring that there are adequate supplies as emergency conditions or unprecedented circumstances could continue or persist for a prolonged period of time, amongst other things.

(iv) Diversifying communication methods because ordinary and everyday means of telecommunications may be restricted.

(d) Coordinating business continuity planning with outside parties

The operations of the licensees are intertwined. It is desirable that the business coordinates with other similar market participants and outside service providers such as telecommunication service providers or insurance companies in order to increase the effectiveness of their own business continuity planning. Such coordination ultimately strengthens the resilience of the entire non-bank financial system. It is important in this context to mutually disclose information regarding the BCP and contact points in an emergency within predefined limits and with adequate information security.

(e) Exerting strong leadership

Business continuity planning is a major project that requires substantial investment of managerial resources and an enterprise-wide awareness by encouraging all level of the

organisation to provide their inputs. The board and senior management of the licensee/entity needs to exert strong leadership and be involved in the planning, reviewing and implementation of the BCP.

It is essential for licensees to provide adequate and efficient training and awareness of the BCP to its employees. Hence, the BCP should be a requirement for the senior management to impart the business continuity awareness and make it part of the organisation's culture.

4. BUILDING A BUSINESS CONTINUITY PLAN

Irrespective of the size and nature of the business, similar principles shall apply for an effective BCP:

(a) A senior person or a designated officer at managerial level within the business should take responsibility of the BCP. The BCP should be allocated the same importance in business planning as to other business plans and procedures, for example those related to quality management, cash flow or health and safety.

(b) The responsibility of managing the BCP must be clearly established within the business and everyone should know the importance of the BCP and who has overall responsibility.

(c) A team of suitability qualified and/or experienced people should be assembled to review the business operations and itemize the key features and areas of operations.

(d) The scope of the work must be established.

(e) It is imperative that a business is able to respond to any type of emergency. A disaster or emergency situation is unexpected. The BCP should be prepared along the following principles:

(i) The BCP should have a broad scope if it is to effectively address the many disaster scenarios that could affect the company.

(ii) It should distinguish between partial loss of services and complete loss of services and facilities.

5. COMPONENTS OF A BUSINESS PLAN CONTINUITY PROCESS

5.1 The licensee should conduct business continuity planning on an enterprise-wide basis. That is, to consider every critical aspect of its business in creating a plan for how it will respond to disruptions. It should not be limited to the restoration of information technology systems and services, or information maintained in electronic form, since such actions, by themselves, cannot always put a business back in operation. The BCP should consider every critical business unit, including personnel, physical workspace, and similar issues, as a business may not be able to resume from serving its customers at an acceptable level. Licensees that outsource the majority of their information processing, or other information technology systems or services,

DRAFT

are still expected to implement an appropriate BCP addressing the equipment and processes that remain under their control.

5.2 A BCP is a working document that reflects the licensee as is, and should be regularly updated and maintained to reflect any changes within the licensee's business. It should be concise and easy to use. The procedures state what tasks should be done, but not necessarily how to carry them out, taking into account that the process on how the BCP will be operated will be dependent on the nature, size and complexity of the business. The reason such specifics are avoided is that a successful BCP requires the flexibility to be creative, within a given situation, and not be encumbered by strict compliance and detailed procedures. The BCP should identify decisions (including options) to be made during a disaster.

5.3 The management should update the BCPs as the licensee's process changes. For example, businesses of all size are increasingly relying on distributed network solutions to support business processes. This may be observed by the increased reliance of desktop computers to maintain essential information (for example, client's information, confidential agreements, KYC & CDD document, etc.). While distributed networking provides flexibility in allowing licensees to deliver operations to where employees and customers are located, it also means that end-users should be made aware by the licensee that they have a BCP ~~be made aware by the licensee that they have a BCP~~ procedure in place and on what constitutes the current business processes and the significant changes. Technological advancements are allowing faster and more efficient processing, thereby reducing acceptable business process recovery periods. In response to competitiveness and customer demands, many businesses are moving towards shorter recovery periods and designing technology recovery solutions into business processes. These technological advancements increase the importance of business continuity planning.

5.4 There are three stages to creating a BCP:

(a) Conduct a risk assessment of the potential impact that the arising situation may have on the business operation in order to determine the magnitude of the exposure to threats;

(b) Develop and document the Business Impact Analysis (BIA) and the BCP;

(c) Test, identify corrective measure, approve and implement the BCP. This stage includes updating and maintaining the BCP on an ongoing basis to meet the changing demands of the business.

Stages	**Objective**
I. Risk Assessment	
1. Risk Evaluation	➢ Identify critical business functions essential for continued service or production. ➢ Determine the events that can adversely affect the company, the damage that such events can cause and the controls needed

	to prevent or minimize the effects of a loss potential.
2. Business Impact Analysis	➢ Identify the impacts that result from disruption that can affect the company and the techniques that can be used to quantify and qualify such impacts. ➢ Prioritise critical business functions.
II. Develop and Document Business Continuity Plan	
1. Develop Recovery Strategy	➢ Determine and guide the selection of recovery operating strategies to be used to maintain the critical functions
2. Documented Plan	➢ Organise and document a written BCP plan. Senior management should review and approve the proposed plan.
III. Test, Corrective Measures, Approve and Implement Business Continuity Plan	
1. Test Plan	➢ Develop testing criteria and procedures. Coordinate, test, and evaluate the plan. Document all results.
2. Corrective Measures	➢ Rectify and identify factors that may have produced during the testing or while implementing the BCP ➢ Finds measures to improve the BCP to eliminate the undesirable effects
3. Approve and Implement Plan	➢ Obtain senior management endorsement of plan
4. Maintain Plan	➢ Develop processes to keep the plan up-to-date with reviews and tests completed at a maximum of 12-month intervals. ➢ Ensure the plan is in-line with the strategic direction of the company.

6. BOARD AND SENIOR MANAGEMENT RESPONSIBILITIES

6.1 It is the ultimate responsibility of the Board of Directors to establish the Business Continuity Arrangement of the licensee. The Board is responsible for approving Business Continuity Plan policies, standards and principles developed by Senior Management and ensuring that sufficient resources are devoted to implementing the plan. The Board would provide oversight, approve the BCP, review test results of the BCP and ensure maintenance of the current plan.

6.2 The Senior Management of the licensee has the responsibility for developing the policies, standards and principles of the Business Continuity Plan. They must ensure that the necessary administrative support functions such as human resources, insurance, legal, security and any other necessary arrangement are in place. They should also ensure that all levels of staff are aware of the importance of the Business Continuity Plan. The senior management level should fulfil its business continuity planning responsibilities by setting policy, prioritizing critical business functions, allocating sufficient resources and personnel.

DRAFT

6.3 Senior management will be responsible for identifying, assessing, prioritizing, managing, and controlling risks. The effectiveness of business continuity planning depends on the management's commitment and ability to clearly identify what makes existing business processes work. Each licensee must evaluate its own unique circumstances and environment to develop a comprehensive BCP.

6.4 Both the board and senior management should designate personnel to participate in the BCP development. Properly allocating resources will facilitate a business throughout the development and maintenance of a BCP. A large and complex business may need a business continuity planning department or a team with departmental liaisons throughout the business. A smaller and less complex business may only need an individual business continuity planning coordinator. While the planning personnel may recommend certain prioritization, ultimately the board and senior management are responsible for understanding critical business processes and subsequently establishing plans to meet business process requirements in a safe and sound manner.

6.5 The Authority shall also recognise its role in supporting the systemic market business processes and that the service disruption of the business may significantly affect the integrity of key markets.

7. RISK ASSESSMENT

7.1 The risk assessment step is critical and has significant bearing on whether business continuity planning efforts will be successful. If limited threat scenarios are identified, the resulting BCP may be inadequate. During the risk assessment step, business processes and the business impact analysis ("BIA") assumptions should be stress tested with various threat scenarios.

7.2 Regulated entities and licensees should identify realistic threat scenarios that may potentially disrupt their business process and ability to meet their client's expectations (internal, business partners, or customers). Threats can take many forms, including malicious activity as well as natural and technical disasters. Where possible the licensee should analyse the threat by focusing the impact on the business and the nature of the threat, in order to increase chances of prevention in the future or to mitigate it completely. For example, the effects of certain threat scenarios can be reduced to business disruptions that affect only specific work areas, systems, facilities or geographical areas. Additionally, consideration should be taken based on the magnitude of the business disruption as well as the variety of threat scenarios based upon practical experiences and potential circumstances and events. If the threat scenarios are not comprehensive, BCPs may be too basic and omit reasonable steps that could improve business processes' resiliency to disruptions.

7.3 Threat scenarios need to consider the impact of a disruption and probability of the threat occurring. Threats range from those with a high probability of occurrence and low impact to the business (e.g. brief power interruptions), to those with a low probability of occurrence and high impact on the business. High probability threats are often supported by very specific BCPs. However, the most difficult threats to address are those that have a high impact on the business but a low probability of occurrence. Using a risk assessment, BCPs may be more flexible and adaptable to specific types of disruptions that may not be initially considered.

DRAFT

~~7.4 It is at this point in the business continuity planning process that a "gap analysis" should be performed. In this context, a gap analysis will be considered as a methodical comparison of what types of plans the licensee (or business line) needs to maintain in order to resume or recover normal business operations in the event of a disruption, in comparison to what the existing BCP provides. The difference between the two highlights additional risk exposure that management and the board need to address in BCP development.~~

~~7.5~~7.4 The risk assessment may consider the following, but should not be limited to:

(a) The impact of various business disruption scenarios on both the business and its customers;

(b) The probability of occurrence based, for example, on a rating system of high, medium, and low;

(c) Measures to consider for each probability;

(d) The loss impact of information services, technology, personnel, facilities and service providers from both internal and external sources;

(e) The safety of critical processing documents and vital records; and

(f) A broad range of possible business disruptions, including natural, technical, and human threats.

~~7.6~~7.5 When assessing the probability of a specific event occurring, the business should consider the geographic location of their facilities, their susceptibility to natural threats and the proximity to critical infrastructures such as power sources or airports. The worst case scenarios such as destruction of the workplace and/or its facilities may be included. At the conclusion of this phase, the business will have to prioritize its business processes and estimate how they may be disrupted under various threat scenarios.

8. BUSINESS IMPACT ANALYSIS AND RECOVERY

8.1 Following the risk assessment, the business will have to document the result of the risks identifies. Therefore, the business will need to perform a Business Impact Analysis ("BIA"). The amount of time and resources necessary to complete the BIA will depend on the risk identified, size and complexity of the business. The business should include all business functions and departments in this process. The BIA phase identifies the potential impact of uncontrolled, non-specified events on the business processes from the risk assessment. The BIA phase should determine what and how much is at risk by identifying critical business functions and prioritizing them. It should estimate the maximum allowable downtime for critical business processes, recovery point objectives and backlogged transactions, and the costs associated with downtime. Management should establish recovery priorities for business processes that identify essential personnel, technologies, facilities, communication systems, vital records, and

DRAFT

information. The BIA should also consider the impact of legal and regulatory requirements such as the privacy and availability of customer information.

8.2 Uniformity can improve the consistency of responses following the threats and help personnel involved in the BIA phase compare and evaluate the business process requirements. This phase may initially priorities business processes based on their importance to the business achievement of strategic goals and maintenance of safe and sound practices.

8.3 The BIA is also used to prioritize treatment of the risks, to have a consensus on the likelihood, impact of the risk materializing and based on these results the business will decide on priority basis with risk to treat, tolerate, transfer or terminate.

8.4 After conducting the BIA and risk assessment, management should prepare a written BCP. The plan should document strategies and procedures to maintain, resume, and recover critical business functions and processes. The BCP should also include procedures to execute the plan's priorities for critical and non-critical functions, services and processes. A well-written BCP should describe in detail the types of events that would lead up to the formal declaration of a disruption and the process for invoking the BCP. It should describe the responsibilities and procedures to be followed by each continuity team and contain the contact lists of the critical personnel. The BCP should describe in detail the procedures to be followed to recover each business function affected by the disruption and should be written in such a way that various groups of personnel can implement it in a timely manner. The BCP should be flexible to respond to changing internal and external conditions as well as new threat scenarios. Rather than being developed around specific events, the plan will be more effective if it is written to adequately address specific types of scenarios and the desired outcomes. A BCP should describe the immediate steps to be taken during an event in order to prevent or minimize the damage from a disruption, as well as the action necessary to recover. Thus, business continuity planning should be focused on maintaining, resuming, and recovering the business' operations when a disruption occurs. For specific scenarios, the BCP should include how the business would respond if:

(a) Critical personnel are not available;

(b) Critical buildings, facilities, or geographic regions are not accessible;

(c) Remote working arrangements for the staff located within Seychelles;

(d) Equipment malfunctions (hardware, telecommunications, operational equipment);

(e) Software and information are not accessible or corrupted;

(f) Utilities are not available, such includes power; and

(g) Critical documentations and/or records are not available.

8.5 A BCP consists of many components that are both internal and external to a business. The activation of a BCP and restoration of businesses in the event of an emergency is dependent on the successful interaction of various components, which includes the involvement of all the

employees in the actual implementation of the business continuity measures, having a robust back-up information system, procurement of managerial resources, communication arrangement and a practical operational manual. An effective BCP coordinates across its many components, identifies potential process or system dependencies, and mitigates the risks from interdependencies.

8.6 The risk management team should identify the risk and the development of risk mitigation strategies across business areas. Internal causes of interdependencies can include line of business dependencies, telecommunication links, and/or shared resources (i.e. email systems). External sources of interdependencies that can negatively impact a BCP may include telecommunication providers, service providers, customers, business partners and suppliers.

DRAFT

Chart: Sample of Process of Business Continuity Planning

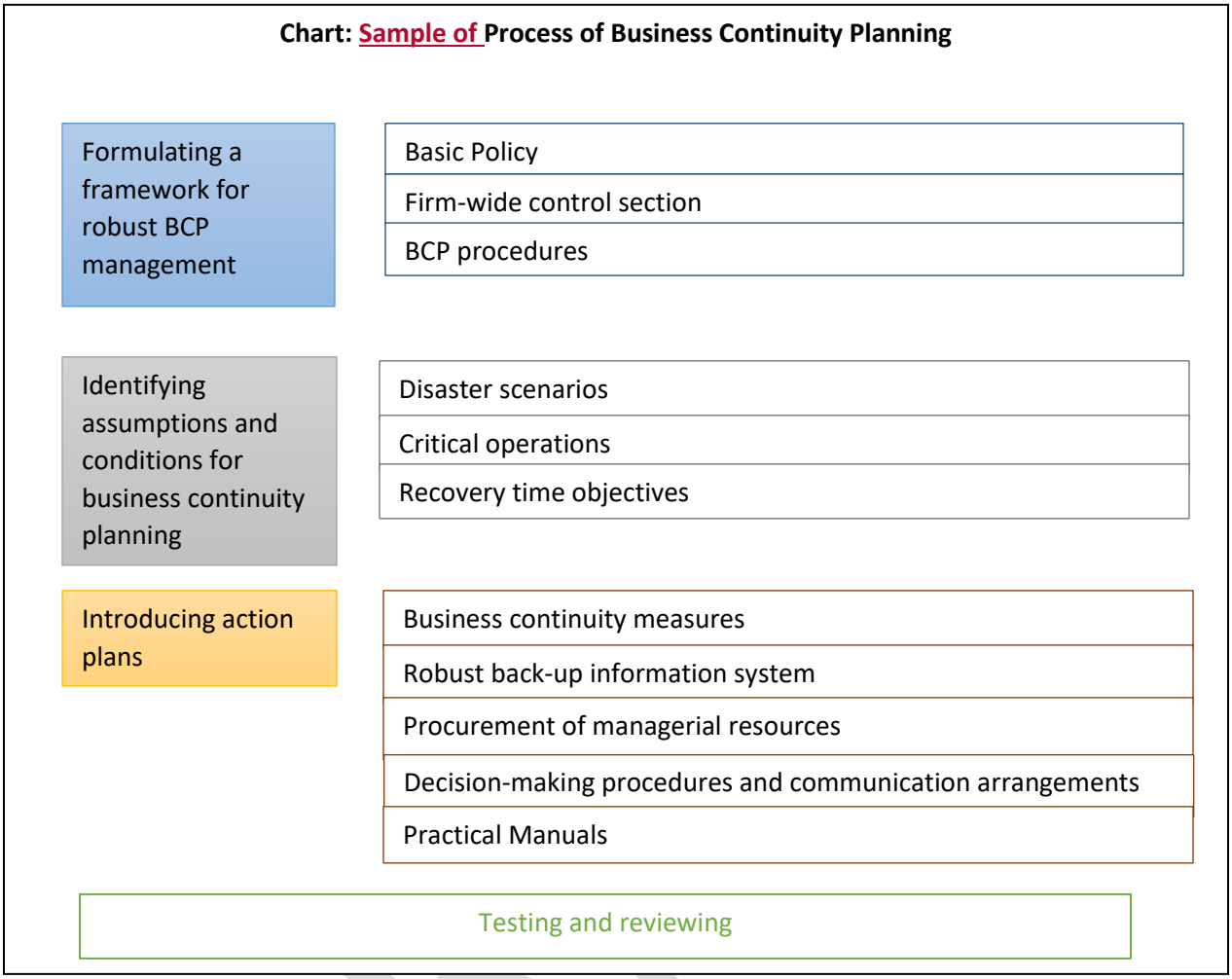

Figure 1 - Procedures in creating an effective BCP

9. OTHER POLICIES, STANDARDS AND PROCESSES

In addition to the BCP, other policies, standards and practices should be implemented to address the continuity of the business operations and services. These may include, but are not limited to, emergency contacts, change control and restoration of information, which will need to relate with the internal control procedures and policies. This will allow work continuity, specifically in regards to information synchronization within the business. The licensee should apply these policies, standards and practices according to their structure, complexity and nature of organization. Although the operation for each business differs, in practice, similar components should be included for the effective operation and restoration of the business activity. The BCP information should be reviewed occasionally for accuracy and to remain up-to-date.

10. CHANGE OF CONTROL

Change in management and control policies and procedures should appropriately address changes to the operating environment. Hence, whenever a change is made to an application, operating system, or utility that resides in the production environment, a methodology should exist to ensure all back-up copies of those systems are updated to reflect the new environment. In addition, if a new or changed system is implemented and results in new hardware, capacity requirements, or other technology changes, management should ensure the BCP is updated and the recovery site can support the new production environment.

11. INFORMATION SYNCHRONISATION

11.1 Information synchronization can become a challenge when dealing with an active/back-up environment. The larger and more complex a business is (i.e., shorter acceptable operational outage period, greater volume of information, greater distance between primary and back-up location), the more difficult synchronization can become. If back-up copies are produced as of the close of a business day and a disruption occurs relatively late the next business day, all the transactions that took place after the back-up copies were made would have to be recreated, perhaps manually, in order to synchronize the recovery site with the primary site.

11.2 Managing and testing of contingency arrangements are critical to ensure the recovery environment is synchronized with the primary work environment. This testing includes ensuring software versions are up-to-date and communication equipment are compatible. Proper change control, information back-up, and adequate testing can help avoid total loss of information. Additionally, back-ups should be considered as essential and the management should ensure that the back-up facility has adequate capacity to process transactions in a timely manner in the event of a disruption at the primary location.

12. INSURANCE

12.1 Insurance is commonly used to recoup losses from risks that cannot be completely prevented. Generally, insurance coverage is obtained for risks that cannot be entirely controlled, yet it

could represent a significant potential for financial loss or other disastrous consequences. The decision on which type of insurance cover to obtain should be based on the probability and degree of loss identified during the BIA.

12.2 Nonetheless, the Authority takes into account that insurance is ~~a choice, in order to reduce risk. The insurance cover that a licensee opt for would be dependent on the risks that the insurer and reinsurer has identified in relation to their size, nature of business and operations~~ mandatory, notably the Professional Indemnity Insurance Cover, which a copy is requested to be submitted to the Authority upon the annual license renewal.

12.3 The business should determine potential exposure for various types of disasters, unforeseen circumstances and review the insurance options available to ensure appropriate insurance coverage is provided. The management should know the limits and coverage detailed in insurance policies to ascertain such coverage is appropriately given to the necessary risk profile of the business. Businesses should perform at least an annual insurance review to ensure the level and types of coverage are reasonable, up-to-date and consistent with any legal, management and board requirements.

12.4 The business may create and retain a comprehensive hardware and software inventory list in a secure off-site location in order to facilitate the claims process.

12.5 However, businesses should be aware of the limitations of insurance. Insurance can reimburse a business for some or all of the financial losses incurred as the result of a disaster or other significant event as specified in the policy wording. It is good to note that insurance is by no means a substitute for an effective BCP, since its primary objective is not the recovery of the business. For example, insurance cannot reimburse a business for damage to its reputation.

13. AUDIT OR INDPENDENT REVIEWS

The audit department or a qualified independent party should review the adequacy of the business continuity process to ensure that the BCP meets the required standards that the business should have in place in the eventuality that the BCP shall come into operation. The review should include assessing the adequacy of business process identification, threat scenario development, communication and recommendations. The audit review should be provided to the Board and the senior management of the business to review the effectiveness of the business's process that identifies any areas of weakness. Following the audit or the qualified independent party report, the board and the senior management must ensure that the weaknesses and/or recommendations identified are addressed, recorded, updated and implemented accordingly.

14. COMMUNICATION

14.1 Communication is a critical aspect of a BCP and should include communication with emergency personnel, employees, directors, regulators, customers (notification procedures), and the media (designated media spokesperson). Alternate communication channels should be considered.

14.2 The licensee should communicate and engage all employees vis-à-vis the BCP importance and its implementation. Members of the organization should understand and recognize their role to be part of the BCP process, notably when the BCP is activated. Hence, the organization, should ensure that all employees are aware and have adequate training on how the BCP operates.

15. UPDATING THE BUSINESS CONTINUITY PLAN

15.1 The BCP should be reviewed by the senior management, the planning team members or coordinator, internal audit (where applicable) and the board of directors at least annually. As part of the review process, the team or coordinator responsible for the BCP update should contact the head, directors and managers throughout the business at regular intervals to assess the nature and scope of any changes to the business structure, systems, personnel or facilities. It is to be expected that some changes will have occurred since the last plan update.

15.2 Any organizational changes should be analyzed to determine how they may affect the existing BCP and what revisions to the plan may be necessary to accommodate these changes. The business should ensure that the existing and revised BCP is distributed throughout the business.

15.3 Additionally, depending on the nature, size and complexity of the business there should be a "gap analysis" should be performed. In this context, a gap analysis will be considered as a methodical comparison of what types of plans the licensee (or business line) needs to maintain in order to resume or recover normal business operations in the event of a disruption, in comparison to what the existing BCP provides. The difference between the two highlights additional risk exposure that management and the board need to address in BCP development.

15.4 Any changes relating to the BCP, the licensee should notify the Authority and the document need to be readily available for inspection.

15.5 The BCP should reflect the component as established per **Appendix 2**.

16. CHECKLIST FOR BUSINESS CONTINUITY PLAN

Appendix 3 provides for a checklist, advising of the key elements that should be contained within the BCP.

DRAFT

Appendix 1

INTERNAL AND EXTERNAL THREATS

While a BCP should be focused on ensuring minimal interruption in the day-to-day business of a company, regardless of the nature of the disruption, different types of disruptions may require a variety of responses in order to resume business. Many types of disasters impact not only the business but also the surrounding community. The human element can be unpredictable in a crisis situation, and should not be overlooked when developing the BCP. Employees and their families could be affected as significantly as, or more significantly than the business. Therefore, the senior management of the business should consider the impact that such disruption would have on the personnel or the business. Additionally, cross-training of personnel and succession planning may be just as essential as back-up procedures addressing equipment, information, operating systems, and application software.

Malicious Activity

FRAUD, THEFT, OR BLACKMAIL

These may be perpetrated more easily by insiders, as such, implementation of employee awareness programs and computer security policies is essential. These threats can cause the loss, corruption, or unavailability of information, resulting in a disruption of service to customers. Restricting access to information that may be altered or misappropriated reduces exposure. The business may be held liable for release of sensitive or confidential information pertaining to its customers; therefore, appropriate procedures to safeguard information are warranted.

Natural Disasters

FIRE

A fire can result in loss of life, equipment, and information. The human resources department or the staff responsible for health and safety must know what to do in the event of a fire in order to minimize these risks. Instructions and evacuation plans should be posted in prominent locations, and should include the designation of an outside meeting place so personnel can be accounted for in an emergency. Guidelines for securing or removing media should also be accounted for if time permits. Fire drills should be periodically conducted to ensure personnel understand their responsibilities. Fire alarm boxes and emergency power switches should be clearly visible and unobstructed.

All primary and back-up facilities should be equipped with fire extinguishers, heat or smoke detectors. Ideally, these detectors should be located in the ceiling, in exhaust ducts, and under raised flooring. Detectors situated near air conditioning or intake ducts that hinder the buildup of smoke may not trigger the alarm.

Technical Disasters

COMMUNICATIONS FAILURE

The distributed processing environment has resulted in an increased reliance on telecommunications

networks for communications to customers, third parties, and back-up sites. Business that lacks diversity in their telecommunications infrastructures may be susceptible to single points of failure in the event that a disaster affects one or more of these critical systems.

Regulated entities/licensees should make efforts to identify and document potential single points of failure within their internal and external communications systems. In addition to restoring communication lines with affiliates and vendors, restoration of communications with employees will be critical to any BCP. As an alternative to voice landlines, businesses should consider cell phones, corporate and public e-mail systems, and Internet-based instant messaging.

Unprecedented events (for example pandemics)

These are situations that is not known, experienced, encountered, done before or dealt with by the licensee. In such circumstances, the business may opt the option of having the employees working remotely until a favorable decision and determination had been deduced by the board and the senior management.

DRAFT

Appendix 2

BCP COMPONENTS

Personnel

Based on the BIA, the BCP should assign responsibilities to management, specific personnel, teams, and service providers. The plan should identify integral personnel that are needed for successful implementation of the plan and develop contingencies to be implemented should those employees not be available. The BCP should address:

(a) How will decision making succession be determined in the event of the loss of management personnel?
(b) Who will be responsible for leading the various BCP Teams (e.g., Crisis/Emergency, Recovery, Technology, Communications, Facilities, Human Resources, Business Units, Customer Service)?
(c) Who will primarily be contacted?
(d) Who will be responsible for security (information and physical)?

Planning should also consider personnel resources necessary for decision making and staffing at alternate facilities under various scenarios. Key personnel should be identified to make decisions regarding efforts to provide for renovating or rebuilding the primary facility. This could require personnel beyond what is necessary for ongoing business continuity efforts.

Finally, the business continuity planning coordinator and/or planning committee should be given responsibility for regularly updating the BCP on at least an annual basis, and after significant changes to the operations and environment. The BCP should also be circulated for employees' awareness as and when necessary, notably when there is an update to the document.

BACK-UP RECOVERY FACILITIES

The recovery site should be tested at least annually and when equipment or application software is changed to ensure continued compatibility. Additionally, the recovery facility should exhibit a greater level of security protection than the primary operations site since the people and systems controlling access to the recovery site will not be as familiar with the relocated personnel using it. This security should include physical and logical access controls to the site as well as the computer systems. Furthermore, the BCP and recovery procedures should be maintained at the alternative and off-site storage locations.

Regardless of which recovery strategy is used, the recovery plan should address how any backlog of activity and/or lost transactions will be recovered. The plan should identify how transaction records will be brought current from the time of the disaster and the expected recovery timeframes.

Alternative workspace capacity is just as important as alternative information processing capabilities. Management should arrange for workspace facilities and equipment for employees to conduct ongoing business functions.

DRAFT

FACILITIES

The BCP should address site relocation for short-, medium- and long-term disaster and disruption scenarios. Continuity planning for recovery facilities should consider location, size, capacity (computer and telecommunications), and required amenities necessary to recover the level of service required by the critical business functions. This includes planning for workspace, telephones, workstations, network connectivity, etc. When determining an alternate processing site, management should consider scalability, in the event a long-term disaster becomes a reality. Additionally, during the recovery period, the BCP should be reassessed to determine if tertiary plans are warranted. Procedures to utilize at the recovery location should be developed. In addition, any files, input work, or specific forms, etc., needed at the back-up site should be specified in the written plan.

The plan should include logistical procedures for moving personnel to the recovery location, in addition to steps to obtain the materials (media, documentation, supplies, etc.) from the off-site storage location.

DRAFT

Appendix 3

	Check
A business continuity plan awareness program	☐
A risk management program that includes clearly defined roles and responsibilities for resumption of business processes, including support organization functions	☐
Continuity plans for each core business process	☐
Procedures for mitigating interdependency risks between departments within the business and with other organisations	☐
Trigger points and/or dates to activate the continuity plan	☐
Data back-up and recovery (hard copy and electronic)	☐
Processes to deal with the loss of information that are not available from backup data	☐
Manual processes for continuing operations until technology is restored	☐
Accessible recovery locations and emergency operations centers	☐
A process for automatically switching telephone and data lines	☐
Testing of the business continuity plans on an end-to-end basis	☐
A review process to ensure that the business continuity plan is feasible and up-to-date	☐
Specific incident/emergency management responses that identify assembly areas at a safe distance from the site of the incident	☐
Annual statement by Senior Management on whether the recovery strategies adopted are still valid and whether the documented business continuity plan is properly tested and maintained	☐
Does the document indicate the objectives of the plan?	☐
Does the document indicate the various risks associated with the business activity?	☐
Does the document provide for the measures to be taken to mitigate the risks identified?	☐
Does the document provide for data protection measures to be taken?	☐

DRAFT

Does the document provide for the procedure to be put in place for cybersecurity?	☐
Does the document provide for an off-site alternative location in relevant circumstances as identified? (If applicable)	☐
Does the document provide for amount of contingency fund to be maintained?	☐
Have procedures been set out in cases where the business cannot continue as a going concern?	☐

DRAFT

Appendix 3

Checklist

Below is a checklist, advising of the key elements that should be contained within the BCP and to be submitted to the FSA. Please insert a page reference within your proposal to each information item listed below.

	Check	Official Use
A business continuity plan awareness program	☐	
A risk management program that includes clearly defined roles and responsibilities for resumption of business processes, including support organization functions	☐	
Continuity plans for each core business process	☐	
Procedures for mitigating interdependency risks between departments within the business and with other organisations	☐	
Trigger points and/or dates to activate the continuity plan	☐	
Data back-up and recovery (hard copy and electronic)	☐	
Processes to deal with the loss of information that are not available from backup data	☐	
Manual processes for continuing operations until technology is restored	☐	
Accessible recovery locations and emergency operations centers	☐	
A process for automatically switching telephone and data lines	☐	
Testing of the business continuity plans on an end-to-end basis	☐	
A review process to ensure that the business continuity plan is feasible and up-to-date	☐	
Specific incident/emergency management responses that identify assembly areas at a safe distance from the site of the incident	☐	
Annual statement by Senior Management on whether the recovery strategies adopted are still valid and whether the documented business continuity plan is properly tested and maintained	☐	
Does the document indicate the objectives of the plan?	☐	

DRAFT

~~Does the document indicate the various risks associated with the business activity?~~	☐	
~~Does the document provide for the measures to be taken to mitigate the risks identified?~~	☐	
~~Does the document provide for data protection measures to be taken?~~	☐	
~~Does the document provide for the procedure to be put in place for cybersecurity?~~	☐	
~~Does the document provide for an off-site alternative location in relevant circumstances as identified? (If applicable)~~	☐	
~~Does the document provide for amount of contingency fund to be maintained?~~	☐	
~~Have procedures been set out in cases where the business cannot continue as a going concern?~~	☐	
~~Regulatory approval~~		☐

DRAFT