POLICY PAPER ON BUSINESS CONTINUITY MANAGEMENT

Relevant financial sectors: **Credit institutions, Insurance companies, Captives, Insurance brokers, Pension funds, Money transfer companies, Trust companies, Finance companies, Pawnshops, and Institutional Investors**

Guidelines issued pursuant articles 15 and 15a of the State Ordinance on the Supervision of the Credit System (AB 1998 no.16) (SOSCS); articles 2, paragraph 4, 10 and 10a of the State Ordinance on the Supervision of the Insurance Business (AB 2000 no.82) (SOSIB) in conjunction with the State Decree on Captive Insurance Companies (AB 2002 no. 50) (SDCIC); article 4, paragraph 3, of the State Decree on the Supervision of Insurance Brokers (AB 2014 no. 6) (SDSIB); article 11a of the State Ordinance on Company Pension Funds (AB 1998 no. GT 17) (SOCPF); article 6 of the State Ordinance on the Supervision of Money Transfer Companies (AB 2003 no. 60) (SOSMTC); article 6 of the State Ordinance on the Supervision of Trust Service Providers (AB 2009 no. 13) (SOSTSP); and articles 21 and 28 of the State Ordinance on the Supervision of the Securities Business (AB 2016 no 53) (SOSSB).

I. Introduction

The "Guidelines for Business Continuity Management" (hereafter "BCM Guidelines") are issued to promote and ensure safe and sound practices among the Financial Institutions (hereafter "FI") subject to the supervision of the Centrale Bank van Aruba (hereafter "CBA").

Business Continuity Management (hereafter "BCM") is a holistic management process that aims to minimize the impact to business due to operational disruptions. It not only addresses the restoration of information technology ("IT") infrastructure, but also focuses on the rapid recovery and resumption of critical business functions for the fulfillment of business obligations. BCM provides a framework for building resilience and the capability for an effective response after such an operating disruption. Its objective is to safeguard the interest of the key stakeholders, reputation, brand and value creating activities.

Operating disruptions can occur with or without warning, and the results may be predictable or unknown. As FI form part of the Aruban financial sector and the economy as a whole, it is important that the effects of disruptions, regarding services to the public, are mitigated to an acceptable level. This contributes in maintaining public trust and confidence in Aruba's financial sector.

II. Implementation of the Guidelines

A key challenge is to establish and maintain a comprehensive BCM that is commensurate with the institutions' nature, scale, and complexity of business activities. This is a continuous process. As changes in technology, business focus, and staff affect the state of preparedness, increasingly institutions recognize the need to incorporate BCM as an ongoing discipline into its business-as-usual operations and thereby improve its readiness to respond to and recover from operating disruptions.

FI should have Business Continuity Plans ("BCP") in place to allow the continuation of critical business operations and fulfillment of business obligations, including compliance with regulatory requirements, in the event of disruptions.

The manner in which the FI implements the BCM Guidelines and to which extent risks are mitigated is the primary responsibility of the senior management of the FI. The FI must verify on an ongoing basis that the principles provided in the BCM Guidelines are met and that controls are in place to ensure that risks are managed adequately. The Supervisory Board ("SB") should see to it that Senior Management complies with the principles set forth in this guidance paper. These Principles apply to all FI irrespective of their size. This Guideline is therefore based on the "comply or explain" principle.

This policy paper enters into force on July 1, 2022, with a transition period of six (6) months. This means that no enforcement actions will be undertaken prior to January 1, 2023 in case of non- compliance.

III. BCM principles

Principle 1.

Senior Management is responsible for BCM of its institution.

Senior Management should establish effective management oversight by:

1.1 Establishing BCM policies, standards and procedures

Senior Management is responsible for identifying, assessing, prioritizing, managing, and controlling risks. By establishing business continuity policies, management sets out:

- The organization's aims, principles, and approach to BCM;
- Key roles and responsibilities in the BCM process; and
- How BCM will be governed and reported upon.

The effectiveness of BCM depends on management's commitment and ability to clearly identify what makes existing business processes work. Each FI should evaluate its own unique circumstances and environment to develop appropriate BCM policies, standards and procedures in accordance to the risk profile of the organization.

1.2 Allocating sufficient resources and knowledgeable personnel to accomplish the BCM principles

Senior Management should allocate sufficient time and resources to accomplish the BCM principles mentioned in this document. The appointed BCM team or coordinator can recommend certain prioritization. However, Senior Management is ultimately responsible for understanding critical business processes and, subsequently establishing plans to meet business process requirements in a safe and sound manner.

1.3 Providing adequate training to its personnel and testing of the BCP

Testing the ability to recover critical business operations is an essential component of effective BCM. Senior Management should verify on a regular basis that business continuity testing is scheduled and personnel is sufficiently trained to perform its tasks should an interruption occur. Senior Management should review test plans to ensure all business critical elements are included. Senior Management should review the test results and also inform the SB on the outcome of the tests performed.

1.4 Formally approving the updated BCP

New technology, new personnel, and new business products require BCP to be updated on a continuous basis. By embedding the update of the BCP into policies, standards and procedures, the FI ensures operational update of its BCP. Senior management should formally approve the (updated) BCP.

Principle 2.

Financial Institutions should prepare BCP to recover from disruptive events in a timely fashion.

The purpose for creating BCP is to recover in a timely and controlled fashion in the event of a disruption, in order to minimize the operational, financial, legal, reputational and other material consequences arising from the disruption. The BCP is a comprehensive set of plans for the FI, including all business processes, business units, branches and subsidiaries. It covers the recovery of technical and non-technical infrastructures.

2.1 Financial institutions should plan for disruptive events

FI should plan for the recovery from at least the following disruptive events:

- Natural events such as hurricanes, floods, other severe weather conditions;
- Technical events such as power outage and fluctuations, communication failure, equipment and software failure;
- Malicious activities including but not limited to network security attacks, internal fraud and abuse, assaults and public riots;
- Pandemic; and
- Fires.

2.2 Financial institutions should perform a risk assessment and a business impact analysis

A risk assessment and business impact analysis is the starting point for identifying critical operations and services, key internal and external dependencies and appropriate resilience levels. IT together with the business process owners assess the risk of likelihood and potential impact of disruptive events and establishes appropriate recovery objectives for the organization. The outcomes of the risk assessment and business impact analysis should regularly be reviewed.

The risk assessment and business impact analysis process should determine what and how much is at risk by identifying critical business functions and prioritizing them.

The process should at least identify:

- The maximum allowable unavailability per business process[1];
- The acceptable quantity of data loss[2];
- The acceptable recovery time per business process; and
- The acceptable recovery time per business application.

[1] Also known as Recovery Time Objective "RTO"

[2] Also known as Recovery Point Objective "RPO"

Senior Management should establish recovery priorities for critical business functions and identify essential personnel, technologies, facilities, communications systems, vital records and data. The relationship/dependencies between critical business functions and critical information sources, systems, processes, internal and external parties should be documented.

Critical business functions differ among FI largely due to the different business focus and customers' expectations.

When planning for the business continuity of critical business functions, FI should take into account the interdependencies of their business functions, and the extent to which they depend on other parties. FI should also understand the business processes of these parties that support their critical functions, including their business continuity preparedness and recovery priorities.

2.3 Financial Institutions should review single points of failure

Each FI is unique and has different concentrations of risks and single point of failures. Single points of failures represent a unique source of a service, activity, and/or process, where there is no alternative and which loss could lead to a failure of a critical function. FI should at least take into account the following single points of failure (but not limited to):

- **Organizational spread:** FI that operate from a single physical location.
- **Data Center:** Operating a single Data Center bears a concentration of risk.
- **Paper files:** Critical data that is only available on paper/hardcopy files.
- **Tacit knowledge and specific expertise of personnel:** FI that rely on key personnel with specific expertise.
- **Hardware equipment:** Critical IT components and infrastructure.
- **Power sources:** Power supply interruptions and fluctuations.
- **Telecommunication and Internet Providers:** Failure in (internet) communication with branches, the head office, internally or clients.
- **Service providers or other outsourced services:** Dependency on service providers, vendors, and third parties[3].

2.4 Financial Institutions should create BCP as a recovery strategy to address disruptive events

BCP should provide detailed guidance on how to react after a disruptive event occurs. A principal plan should be established to address the objects for the FI's BCM. For each line of business, office or building a specific action plan may be required.

[3] Reference is made to the CBA's policy paper on Outsourcing arrangements

The FI should ensure that the BCP is:

- Written and disseminated to the relevant personnel, command center(s), and recovery site(s);
- Specific on when to implement the plan;
- Detailed with respect to immediate steps to be taken after a disruption;
- Flexible to respond to unanticipated threat scenarios and changing internal conditions;
- Focused on how to get the business up and running in the event that a specific facility or function is disrupted;
- Explicit in what order to recover the different lines of business;
- Effective in minimizing service disruptions and financial loss; and
- Addressing the return to normal operations and original business locations once the situation has been resolved and permanent facilities are again available, or return to an alternative long term solution that is able to meet the business requirements.

FI should include in their BCP procedures on communication within their institution and with relevant external parties. The communication procedures should at least include:

- A protocol to identify staff that will communicate within the institution and with external stakeholders (including the CBA, the press, local emergency response organizations and critical service providers);
- communication protocols that clearly outline the chain of command;
- a directory of all recovery team members, including the crisis management team, emergency teams, local emergency response organizations, and critical service providers;
- a copy of mentioned directory/contact list, which should be provided to all team members;
- a protocol to address obstacles that may arise due to failure in primary communication systems (electricity, mobile phone network, data infrastructure, road network). Ensure that the FI has set up alternative modes of communications; and
- the regular update and testing of call trees.

Principle 3.

Financial Institutions should test their BCP regularly, evaluate their effectiveness, and update the BCP as appropriate.

Testing the ability to recover critical operations as intended is an essential component of BCM. Such testing can take many forms and should be conducted periodically, with the nature, scope and frequency determined by:

- the criticality of the applications and business functions;
- the organization's role in broader market operations; and
- material changes in the organization's business or external environment.

FIs are encouraged to carry out different types of tests. FI should conduct tests in modules and at different but regular intervals. The test schedule should be in a way that all business continuity components are tested within a reasonable time frame, having regard of the size of the FI and its dependency on IT systems. The disaster recovery plan for the information technology environment should also be tested regularly, because of its dynamic and vital nature.

FI should provide regular training sessions and awareness programs for their staff to familiarize them with their roles, accountabilities, responsibilities and authority in response to a disruptive event.

FI should evaluate the necessity to test the entire enterprise at once, including service providers and key market participants versus testing on a one-at-a-time basis of business units or branches. Test methods may include, but not limited to:

- Orientation/walk through;
- Tabletop/mini drill;
- Functional testing; and
- Full scale testing.

Test plans and results should be formally documented, including test objectives, scripts, and schedules. BCP should be updated as appropriate after reviewing the test results and lessons learned.

Senior Management should review the testing documentation to assure the objectives of the test plans are aligned with the business functions and applications that were identified as critical for the business. Senior Management should concur with the proposed amendments to the BCP based upon the test results and lessons learned.

Test documentation, approved plans and results should be filed for at least 5 years, in the case that significant weaknesses have been identified a longer retention period is appropriate.

Principle 4.

Financial Institutions should embed the update of BCP into policies, standards and procedures of activities/processes that affect the plans.

The following are activities/processes that affect BCP:

- System development life cycle (SDLC) and project management

The SDLC process should incorporate business continuity considerations into project plans. Evaluating business continuity requirements during the SDLC process allows for advance preparation when an institution is acquiring or developing a new system. Evaluating business continuity requirements during the SDLC stages facilitates the development of a more robust system that will permit easier continuation of the business in the event of a disruption.

During the development and acquisition of new systems, SDLC standards and project plans should address at a minimum the following issues:

- Business unit requirements for resumption and recovery alternatives;
- Information on back-up and storage;
- Hardware and software requirements at recovery locations;
- Disaster recovery testing; and
- Staffing and facilities.

- Changes in hardware and software

Change management and control policies, standards and procedures should appropriately address changes to the operating environment. Just as all changes should be fully authorized and documented, business continuity considerations should be included in the change control process and implementation phase.

Whenever a change is made to an application, operating system, or utility that resides in the production environment, a procedure 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, the FI should ensure that the BCP is updated and that the recovery site can support the new production environment.

- Changes in staff

Human resource policies, standards and procedures should appropriately address changes to resources that have roles in the BCP.

- Other changes

Certain events may trigger the need for an immediate review and update of the BCP. Examples hereof are:

- Restructuring of an institution, either through expansion or through a merger;
- Occupancy of new buildings;
- Changes in the institution's business strategy and risk appetite; and
- Changes in service providers.

Principle 5.

Financial Institutions should ensure the quality of all aspects of BCM by assessing independent audits.

Audits should provide independent, objective assurance, and consulting service designed to add value and improve the FI's BCM.

The auditor should review if the BCM policy, standards, procedures and plans are adequate and effective, and if the FI operates accordingly in a manner to ensure that:

- Risks are appropriately identified and managed;
- Interactions with the various stakeholders occur as needed;
- Significant financial, managerial, and operating information is accurate, reliable and timely;
- Employees' actions are in compliance with policies, standards, procedures, and applicable laws and regulations, including the Guidelines for BCM;
- Resources are acquired economically, used efficiently, and adequately protected;
- Programs, plans and objectives are achieved;
- Quality and continuous improvement are accomplished; and
- Opportunities for improving the BCM processes or the organization as a whole are recognized and addressed appropriately.

Audits should be scheduled according to the FI's nature, size, scope of operations, and the complexity of the business. FI that are highly dependent on their IT systems should undergo at least once every two years an audit in this area, or more frequent if significant weaknesses have been identified during the previous audit. The SB should see to it that the aforementioned is adhered to.

Appendix 1: Definitions

Backup	A process by which data, electronic or paper based, is copied in some form to be available in case the original data is lost, destroyed or corrupted.
Business Continuity Coordinator	A role that is assigned the principal responsibility for coordinating the organization(s)/business unit(s) BCM program.
Business Continuity Management (BCM)	A holistic business approach that includes policies, standards, frameworks and procedures for ensuring that specific operations can be maintained or recovered in a timely and controlled fashion in the event of a disruption. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruption.
Business Continuity Plans (BCP)	A comprehensive, documented plan of actions that sets out procedures and establishes the processes and systems necessary to continue or restore the operation of an organization in the event of a disruption. The plan will cover all the key personnel, resources, services and actions required to recover the business.
Business Impact Analysis	The process of identifying, and measuring (quantitatively and qualitatively) of the business effects and losses that might result if the organization were to suffer from a disruptive event. It is used to identify recovery priorities, recovery resource requirements and essential staff and to help shape the business continuity plan. All impacts should be measured on financial, regulatory, legal and reputational damage basis.
Disruptive event / Operating Disruption	A sudden, unplanned event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time, causing unacceptable damage or loss.
Recovery Time Objective (RTO)	The duration of time required to resume a specified business operation. It has two components, the duration of time from activation of the business continuity plan and the recovery of business operations.
Recovery Point Objective (RPO)	A point in time to which data, should be restored from back-up storage for normal operations to resume if a computer, system, or network goes down as a result of a disruption.
Resilience	The ability of an organization, network, activity, process or financial system to absorb the impact of a major operational disruption and maintain critical operations or services running.
Single point of failure	A unique source of a service, activity, and/or process, where there is no alternative and whose loss could lead to the failure of a critical function.