CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN (Central Bank)

Provisions and Guidelines

For

Business Continuity Management

WILLEMSTAD, Updated version April 2011

Provisions and Guidelines for Business Continuity Management

I. Introduction

The "Provisions and Guidelines for Business Continuity Management" (hereafter "Provisions for BCM") are issued to continue promote and ensure safe and sound practices among the (financial) institutions falling under the supervision of the Centrale Bank van Curaçao en Sint Maarten (hereafter "the Bank").

Business Continuity Management (hereafter BCM) is a holistic management process. It identifies potential events regarding operating disruptions that threatens an organization. Such a disruption may include the complete destruction of the building that houses the institution's core business. BCM provides a framework for building resilience and the capability for an effective response after such a disaster. It's 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 supervised financial institutions (hereafter "supervised institutions") play a crucial role in the financial sector and the economy as a whole of Curacao and Sint Maarten, it is important that the effects of disruptions, regarding services to the public, are mitigated. This will contribute to maintain public trust and confidence in our financial sector.

The responsibility for BCM ultimately rests with the Board of Supervisory Directors[1] and the Board of Managing Directors of an institution. They should formulate the business continuity policy, standards, procedures and guidelines for the institution.

The Provisions for BCM apply to all supervised institutions irrespective of their size. Supervised institutions should draft business continuity plans and mitigate operational risks tailored to the nature, size, scope of its operations and complexity of its business.

The Provisions for BCM set out **what** the supervised institution needs to do. **The manner** in which the organization implements the Provisions for BCM and **to which extent** inherent risks are mitigated is the responsibility of the supervised institution. The institution's external auditor, its internal auditor and the Bank's supervision auditor will verify if the principles provided in the Provisions for BCM are adhered to and if controls are in place to ensure that inherent risks are managed adequately.

[1] Some institutions do not have a two- tier organizational structure. In such a case only the Board of Managing directors applies.

II. Risk Assessment and Business Impact Analysis

BCM of supervised institutions should include the establishment of business continuity teams, who are responsible for the drafting, testing and updating of business continuity plans. Before the plans are written, the business continuity team has to determine the likelihood of and subsequent impact of disruptive events on the institution's business, by performing a risk assessment and a business impact analysis. The assessments and analysis can only be performed by a team that thoroughly understands the institution's business, its processes, technology and internal and external interdependencies.

The risk assessment and business impact analysis should include a worst-case scenario of completely damaged facilities and destroyed resources. It should address geographic situations, current and planned services, lead-times of services, and existing service contracts. Each analysis should also include an estimate of the financial impact of replacing damaged equipment, acquiring additional resources, and setting up additional service contracts. All impacts should also be measured with respect to reputational, regulatory and legal damage.

The risk assessment should at least focus on the following threats that manifest:
- Natural events[2] 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 network security attacks, fraud, assaults and public riot; and
- Fires.

This chapter serves to emphasize that only through a thorough assessment process a complete picture of the risks and the impact on the supervised institution's business can be obtained. Once the assessment is complete, it can provide the organization with the necessary information to make appropriate, properly prioritized and cost-effective risk mitigation plans. It is very important to undertake above-mentioned processes before business continuity plans are written. Chapter 2.4 contains further details on how to prepare for better business resilience.
It should also be emphasized that the execution of BCM programs have already been executed by many organizations and that a lot of material is available. Therefore the Bank recommends using a standard methodology such as the BS_25999[3] of the British Standards Institution.

[2] Chances for tsunami's and earthquakes are very limited, yet possible.
[3] BS 25999-1:2006 is a code of practice that takes the form of guidance and recommendations. It establishes the process, principles and terminology of BCM, providing a basis for understanding, developing and implementing business continuity within an organization and to provide confidence in business-to-business and business-to-customer dealings. In addition, it provides a comprehensive set of controls based on BCM best practice and covers the whole BCM lifecycle.

III. Legal base and scope

The Provisions for BCM are issued pursuant to:

- Article 2, paragraph 2 of the National Ordinance on the Supervision of Banking and Credit Institutions 1994 (N.G. 1994, no. 4)
- Article 31, paragraph 1 of the National Ordinance on Insurance Supervision (N.G. 1990, no. 77)
- Article 9, paragraph 1 and Article 18 paragraph 1 of the National Ordinance on the Supervision of Investment Institutions and Administrators (N.G. 2002, no. 137)
- Article 11, paragraph 1 of the National Ordinance on the Supervision of Trust Service Providers (N.G. 2003, no. 114)
- Article 2, paragraph 5 of the National Ordinance on the Supervision of Securities Exchanges (N.G. 1998, no. 252)

The Provisions for BCM apply to all institutions that fall under the supervision of the Bank. However, the business continuity plans should be proportionate to the supervised institution's operational risk (arising from both internal and external sources) and tailored to the nature, size and scope of its operations and the complexity of its business.

IV. Implementation

To ensure a high standard of financial management on the islands of Curaçao and Sint Maarten, supervised institutions are required to have implemented the Provisions for BCM by July 1, 2011.

The Provisions for BCM contain the minimum requirements for establishing sound and effective BCM practices. The Bank may prescribe additional rules and regulations to administer and carry out the purposes of the Provisions for BCM. This may include rules and regulations to (further) define terms used and to establish limits or requirements other than those specified in the provisions for BCM. The Bank also reserves the right, in individual cases of (partially) non-compliance, to impose mandatory instructions.

The Bank will verify the implementation of the Provisions for BCM during its onsite examinations. Based on these examinations and its offsite reviews, the Bank will determine the adequacy of supervised institutions' BCM processes.

The Board of Supervisory Directors and the Board of Managing Directors of the supervised institutions should familiarize themselves with the provisions for BCM and guidelines and understand the intent and implications of the principles elaborated upon in the following chapters.

V. Business Continuity Management principles

Principle 1.

The Board of Supervisory Directors and the Board of Managing Directors should establish effective management oversight with respect to potential events that threatens the continuity of the business operations of supervised institutions.

The Board of Supervisory Directors and the Board of Managing Directors should establish effective management oversight by:

1.1 Establish BCM policies, standards and procedures

The Board of Supervisory Directors and the Board of Managing Directors are 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 supervised institution should evaluate its own unique circumstances and environment to develop appropriate BCM policies, standards and procedures.

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

The Board of Supervisory Directors and the Board of Managing Directors should allocate sufficient time and resources to accomplish the BCM principles mentioned in the Provisions for BCM. A large and or complex institution may need a business continuity planning department with a team of departmental liaisons throughout the enterprise. A smaller and or less complex institution may only need a single business continuity planning coordinator. While the appointed BCM team or coordinator recommend certain prioritization, ultimately the Board of Supervisory Directors and the Board of Managing Directors are responsible for understanding critical business processes and subsequently establishing plans to meet business process requirements in a safe and sound manner.

1.3 Provide for training of personnel and testing of the business continuity plans

Testing the ability to recover critical business operations is an essential component of effective BCM. The Board of Supervisory Directors and the Board of Managing Directors should verify at the beginning of each year that business continuity testing is scheduled and personnel are sufficiently trained to perform the task. The board of executive management should review test plans to ensure all business critical

elements are included. The Board of Supervisory Directors and the board of managing directors should both review the test results.

1.4 Formally approving the updated business continuity plans

Each supervised institution changes during its existence. New technology, new personnel and new business products requires updating the business continuity plans. By embedding the update of the business continuity plans into policies, standards and procedures the institution ensures operational update of its business continuity plans. The Board of Managing Directors should formally approve updated business continuity plans. The Board of Supervisory Directors should at least annually verify if the business continuity plans are updated and approved by the Board of Managing Directors.

1.5 Ensuring the quality of the BCM activities and products by assessing independent audits

The Board of Supervisory Directors and the Board of Managing Directors should see to it that audits are scheduled according to the supervised institution's nature, size, scope of operations and the complexity of its business. The BCM activities and products should be subject to independent reviews and the findings should be reported to the Board of Supervisory Directors and the Board of Managing Directors promptly.

Principle 2.

Financial Institutions should prepare business continuity plans to recover from disruptive events in a timely fashion.

The purpose for creating business continuity plans 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 business continuity plans are a comprehensive set of plans for the entire enterprise including all business processes, business units, branches and subsidiaries. It covers the recovery of technical and non-technical infrastructures.

2.1 Supervised institutions should plan for disruptive events

Supervised Institutions 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 network security attacks, fraud, assaults and public riot; and
- Fires.

2.2 Supervised 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 assesses the risk of likelihood and potential impact of disruptive events and establishes appropriate recovery objectives for the organization.

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 function[4];
- The acceptable quantity of data loss[5];
- The acceptable recovery time per business function; and
- The acceptable recovery time per business application.

Management should establish recovery priorities for business functions and identify essential personnel, technologies, facilities, communications systems, vital records and data. The relationship/dependencies between critical business functions and

[4] Also known as Recovery Time Objective "RTO"
[5] Also known as Recovery Point Objective "RPO"

critical information sources, systems, processes, internal and external parties should also be clearly documented.

Methods and techniques
A combination of the following methods and techniques may be used to carry out the risk assessment and business impact analysis:
- Interviews;
- Workshops; and
- Questionnaires.

All relevant information should be filed for future reference.

2.3 Supervised institutions should review single points of failure
Each supervised institution is unique and has different concentrations of risks and single point of failures. The BCM team might not be aware of all these specific risks concentrations. Therefore, special attention should be given to single points of failure during the interviews, workshops and completion of questionnaires.
Supervised Institutions should at least take into account the following single points of failure:

Organizational spread
Supervised institutions that operate from a single location lack organizational resilience. It is better to occupy more than one location than concentrate the whole business in one location. The spread should be sufficiently remote and should not depend on the same physical infrastructure components. Ideally, electrical substations and telecommunication circuits differ per location. Smaller supervised institutions might opt for reciprocal agreements with befriended institutions, by which organizations agree to use one another's resources when a disruptive event occurs.

Data Center
Having a single Data Center bears a concentration of risk. Supervised institutions may set up for an alternate data center at another location of the same institution, at a commercial party, or with a befriended institution. The decision to have a hot, warm or cold site depends on the nature of the business. Special attention should be given to critical data on the hard disk of personnel and stand alone systems. All corporate data such as Word Documents, Excel files, MS Access databases, but also E-mail archives, should be stored on central data media systems and not on the hard disk of a laptop or desktop. Stand alone systems like a salary administration require strict procedures in order to have the same resilience as applications running on central servers.

Paper files
Supervised institutions should take special interest in paper files. Paper files can be scanned and uploaded to modern electronic document management systems ('EDMS'). Backups of the EDMS files can be stored at an off-site location. Supervised Institutions should examine which critical paper files are single points of failure.

In addition to before mentioned, EDMS systems have very advanced functionalities like record retention, full text search capabilities, and workflow options, which might be of great value to the business.

Tacit knowledge and specific expertise of personnel
Supervised institutions that rely on personnel with specific expertise should consider cross training, backup personnel and documenting specific knowledge. When traveling abroad it is good policy to book different flights for senior managers or other personnel who share specific tacit knowledge. Using modern technology, like video conferencing, reduces traveling needs which reduces risk and saves money.

Hardware equipment
Administrators should report single points of failure for hardware equipment and components like routers, switches, firewalls, data media, servers or controllers.

Power sources
Technicians should report single point of failures regarding power supply as interruptions and fluctuations might occur. Special attention should be given to the protection of power sources against malicious activities such as burglary and sabotage. This applies also to generators. Generators should also be sufficiently elevated from the street level to withstand flooding.

Tele-communication
International telecommunication can be a single point of failure. Supervised Institutions that depend heavily on international communication with branches, the head office or clients, should become aware of all possibilities provided, and single points of failure existing, at local telecommunication providers. Modern technology like satellite solutions provide alternate routing to sea cables.

Internet providers or other outsourced services
Having a single internet service provider is a single point of failure. Depending on the impact on the supervised institution when this service is unavailable, the institution should decide to contract a second provider or set up the internet services in house. The same principle adheres to services that are outsourced.

2.4 Supervised institutions should make their business more resilient to disruptive events by reducing or mitigating risk

When a complete picture of the critical business elements is obtained and the risk assessment has determined the probability and impact of specific threats to the business, management should decide how to manage the identified risks.
It is better to make the business more resilient to disruptive events by taking preventive actions before preparing business continuity plans that are geared towards actions to be taken after a disruptive event occurs. Risk management decisions can influence the setup of the business continuity plans. If for example the organization agrees that operating from a single location is undesirable and another location will be occupied, the set up of business recovery plan and disaster recovery plan for the information technology environment will be quite different.

The initial focus should be to solve issues of high probability and high business impact. Risk for these issues should be reduced or eliminated as soon as possible with high priority. Options for risk management are the following:

Risk Reduction

Risk reduction involves precautions to reduce the severity of the loss or the likelihood of the loss from occurring. For a natural event like a hurricane, supervised institutions can make a building more hurricane proof by e.g. attaching hurricane proof windows, improving the roof of the building or elevate the floor in the computer room. To be better prepared for fires institutions can e.g. use fireproof file cabinets, use a fire suppressing system in the computer room, install smoke detectors, fire extinguishers or offsite storage of backup tapes and files. To prepare for armed assaults institutions can install surveillance cameras, place a guard, an alarm system, limit the amount of cash available, place a panic button, use revolving doors and give instructions to personnel. For technical events such as power outage/fluctuations institutions can e.g. use generators, UPS[6] and surge protectors. For hard disk failures institutions can install raid 1 systems, raid 5 systems or a SAN solution.

Supervised institutions should determine potential exposures for the various types of disasters and review the current controls in place and decide to take extra precautions to reduce or eliminate risk.

Risk Transfer

Risk transfer involves transferring the weight or the consequence of a risk to some other party. Insurance coverage is a commonly used method of risk transfer. It is obtained for risks that cannot be entirely controlled, yet could represent a significant potential for financial loss or other disastrous consequences. The decision to obtain insurance should be based on the probability and degree of loss identified during the risk assessment and business impact analysis. Supervised institutions should determine the potential exposure for various types of disasters and review the insurance options available to ensure appropriate insurance coverage. Management should know the limits and coverage detailed in insurance policies to ensure coverage is appropriate given the risk profile of the institution. Financial institutions should perform an annual insurance review to ensure the level and types of coverage are commercially reasonable, and consistent with any legal, management, and supervisory board requirements. Also, financial institutions should set up and retain a comprehensive inventory list of insured items in a secure off-site location in order to facilitate the claims process.

Financial institutions should be aware of the limitations of insurance. Insurance cannot always reimburse an institution for all of the financial losses incurred as the result of a disaster or other significant event. However, insurance is by no means a substitute for effective business continuity plans, since its primary objective is not the recovery of the business. For example, insurance companies can not reimburse a supervised institution's loss of reputation.

[6] Appendix 1 has a Glossary/Definitions section

Outsourcing specific tasks to organizations that are better equipped to perform the task is another form of risk transfer. For example to protect a company against cyber attacks the security setup and monitoring of the network can be outsourced to a company with specialized resources in this field. However, the supervised institution remains responsible for all outsourced tasks.

Risk Avoidance
Risk avoidance generally involves not undertaking an activity to avoid the risk involved. The downside of using avoidance as your main form of risk management is that by avoiding taking risks, business opportunities are also excluded. E.g. a supervised institution can decide not to open its network to inbound traffic. Because of such a decision customers can not connect to the supervised institution's network, resulting in missed opportunities to provide customers extra services.

Risk Acceptance
Risk acceptance generally involves accepting the identified risk without taking any measures to prevent loss or limit the probability of the risk happening. This approach is ideal for those risks that will not create a high amount of loss if they occur. These risks in fact would be considered more costly to manage than to allow. E.g. residual risk (= the risk that stays present after controls have already been put into effect).

The risk assessment and business impact analysis, including the management of risks, should be addressed at least annually. In this regard, all external and internal changes that may have impact on the continuity of the business over the past year should be discussed.

2.5 Supervised institutions should create business continuity plans as a recovery strategy to address disruptive events

Only after all previously mentioned steps have been taken the preparation of business continuity plans can start.

Business continuity plans should provide detailed guidance on how to react after a disruptive event occurs. Business continuity plans can be organized in different ways. In general a principal plan should be established to address the general objects for BCM.

The principal business continuity plan should at least address the following:
- The command structure of the management crisis team with the decision-making authorities and their responsibilities;
- The location of the primary and secondary command center;
- The principal call tree;
- The designation of a PR spokes person and a communication plan;
- A list of all action plans;
- The exact conditions when specific action plans will be triggered;
- All internal support- and emergency teams;
- A list of key country emergency responders;

- A list of key vendors (hardware/software/communication systems);
- A list of key supporting firms/persons (e.g. electricians, carpenters, welders);
- A plan to safeguard the family members and housing of personnel that form part of the crisis teams; and
- Interdependencies among business continuity plans of other organizations such as local service providers, public services, country crisis response team.

At least the following specific action plans should be in place:
- Hurricane plan;
- Building evacuation plan;
- Business Recovery plan;
- Disaster recovery plan for the information technology environment;
- Network security defense and recovery plan; and
- Armed assault plan (only for financial institutions that handle cash).

For each line of business, office or building a specific action plan may be required. Supervised institutions should create templates in order to standardize the setup of the specific action plans.

The institution should ensure that the business continuity plans are:
- Written and disseminated so that various groups of personnel can implement it in a timely and controlled manner;
- 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;
- Focused on preserving human life; and
- Addressing the return to normal operations and original business locations once the situation has been resolved and permanent facilities are again available.

Supervised institutions should include in their business continuity plans procedures for communicating within their institution and with relevant external parties. The communication procedures should at least include:
- A plan to identify staff that will communicate within the institution and with external stakeholders (including the Bank, the press, local emergency response organizations and critical service providers);
- Establish communication protocols clearly outlining the chain of command;
- Develop 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 should be provided to all team members;

- Address obstacles that may arise due to failure in primary communication systems (electricity, mobile phone network, road network). Ensure that the institution has set up alternative modes of communications.
- Ensure the regular update and testing of call trees at least quarterly;
- Ensure that copies of the business continuity plans are disseminated to the relevant personnel, command center(s) and recovery site(s).

Principle 3.

Supervised Institutions should train personnel and test the business continuity plans, evaluate their effectiveness, and update the plans 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.

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

By testing the business continuity plans it becomes evident whether or not the training program and the business continuity plans are effective. Training programs and test plans should be updated as appropriate, after reviewing the test results.

Supervised institutions should set up test plans for their principal business continuity plan and all specific action plans (=the hurricane plan, business recovery plans etc.). The test schedule should be setup in a way that all business continuity plans are tested at least every 2 years.

The supervised institution 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 base of business units or branches.

The disaster recovery plan for the information technology environment should be tested at least annually, because the information technology environment is most dynamic and vital. Test may vary between running one business application at a time after business hours from the alternate location to running a complete production site from the alternate location for a longer period of time (e.g. a full week). For the latter, we advise supervised institutions to run this specific test yearly.

Test plans should be documented including test objectives, scripts and schedules. Each testing method used should have its own test plan. Supervised institutions are expected to employ various methods of testing included, but not limited to:

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

The Board of Managing Directors should review the scope and the objectives of the test plans to ensure that business functions and applications, that were identified as critical during the business impact analysis, are included in the tests.

The test results should be documented and reviewed by the Board of Supervisory Directors, the Board of Managing Directors and internal/external auditors. Test plans and results should be filed at least until the on-site examiners of the Bank have reviewed them.

Principle 4.

Supervised Institutions should embed the update of business continuity plans into policies, standards and procedures of activities/processes which affect the plans

The following are activities/processes that affect business continuity plans:

- System development life cycle (SDLC) and project management

As part of the SDLC process, management 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 as 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, management should ensure the business continuity plans are updated and 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 business continuity plans.

- Other changes

Certain events may trigger the need for an immediate review and update of the business continuity plans, which can not be handled by operational procedures. These are changes in:

- Restructuring of an institution, either through expansion or through a merger;
- Habitation of buildings (movements of departments or occupancy of new buildings);
- The institution's business strategy and risk appetite;
- Service providers; and
- Regulatory and legislative requirements.

Principle 5.

Supervised 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 institution's BCM.
The auditor should review if the BCM policy, standards, procedures and plans are adequate and effective, and if the institution 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 provisions and 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.

The Board of Supervisory Directors and Board of Managing Directors should see to it that audits are scheduled according to the financial institution's nature, size, scope of operations and the complexity of the business.

Appendix 1: Glossary/Definitions

Alternate Site	A site held in readiness for use in the event of a major disruption to continue daily operations.
Alternative Routing	The routing of information via an alternative cable routing media i.e. using different networks should the normal network be rendered unavailable
Armed assault plan	A plan, procedure or instructions to personnel on how to deal during and after armed assaults occur and physical measures to prepare for armed assaults.
Audit	The process by which procedures and/or documentation are measured against pre-agreed standards.
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 currupted.
Building evacuation plan	A plan to evacuate personnel out of the building when a threat to human life occurs e.g. a fire or bomb threat
Business Continuity Coordinator	A role that is assigned the principal responsibility for coordinating the organization(s)/business unit(s) BCM programme.
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 disruption. Its purpose is to minimize the operations, financial, legal, reputational and other material consequences arising from disruption.
Business Continuity Plan	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.
BCM Policy	A policy that sets out an organization's aims, principles, and approach to BCM; key roles and responsibilities and how the BCM will be governed and reported upon.
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.

Call Tree	A structured cascade process (system) that enables a list of persons, roles and/or organizations to be contacted as part of information or plan invocation procedure.
Cold Site	Is the most inexpensive type of alternate site for an organization to operate. It does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. The lack of hardware reduces startup costs of the cold site, but requires additional time following the disaster to have the operation running at a capacity close to that prior to the disaster. Organizations that can not afford the long startup time of an Cold Site should opt for a Warm or Hot Site.
Command Center	The facility used by a Crisis Management team after the first phase of a disruptive event. An organization should have a primary and a secondary location for a command center in the event of one being unavailable. It may also serve as a reporting point for deliveries, services, press and all external contacts.
Communication Protocols	An established procedure for communication that is agreed in advance between two or more parties internal or external to an institution. Such procedure also includes the nature of the information that should be shared with internal and external parties and how certain types of information should be shared with internal and external parties.
Critical Services	Any activity, function, process or service, of which the loss would be material to the continued operation of an organization.
Crisis	An event, occurrence and/or perception that threatens the operations, staff, shareholder value, stakeholders, brand, reputation, trust and/or strategic/business goals of an organization.
Crisis Management Team	A team consisting of key executives, key role players (i.e. legal counsel, facilities manager, business continuity coordinator), and the appropriate business owners of critical functions, who are responsible for recovery operations during a crisis.
Disaster recovery plan for the information technology environment	A plan for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure when a disaster occurs. The plan includes the move to a cold, warm or hot site.
Disruptive event	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.

Electrical substation	An electrical substation is a subsidiary station of an electricity generation, transmission and distribution system. Electric power flows through several substations between generating plant and consumer
Emergency Response Team	Any organization team that is responsible for responding to hazards to the general population (e.g. fire brigades, police services, hospitals, internal emergency response team)
Evacuation	The movement of employees, visitors and contractors from a site and/or building to a safe place (rendez-vous point) in a controlled and monitored manner.
Federal Financial Institutions Examination Council (FFIEC)	A formal interagency body of the United States government empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS) and to make recommendations to promote uniformity in the supervision of financial institutions.
Full-scale testing	Comprises the most comprehensive type of test. In a full-scale test, the institution implements all or portions of its business continuity plans by processing data and transactions using back-up media at the recovery site. It involves: - Validation of crisis response functions; - Demonstration of knowledge and skills, as well as management response and decision-making capability; - On-the-scene execution of coordination and decision-making roles; - Actual, as opposed to simulated, notifications, mobilization of resources, and communication of decisions; - Activities conducted at actual response locations or facilities; - Enterprise-wide participation and interaction of internal and external management response teams with full involvement of external organizations; - Actual processing of data utilizing back-up media; and - Exercises generally extending over a longer period of time to allow issues to fully evolve as they would in a crisis, and allow realistic role- play of all the involved groups.

Functional testing	Functional testing is a type of test that involves the actual mobilization of personnel at other sites in an attempt to establish communications and coordination as set forth in the business continuity plan. It includes: - Demonstration of emergency management capabilities of several groups practicing a series of interactive functions, such as direction, control, assessment, operations, and planning; - Actual or simulated response to alternate locations or facilities using actual communications capabilities; - Mobilization of personnel and resources at varied geographical sites; and - Varying degrees of actual, as opposed to simulated, notification and resource mobilization.
Hot site	A duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data. Real time synchronization between the two sites may be used to completely mirror the data environment of the original site using wide area network links and specialized software. Following a disruption to the original site, the hot site exists so that the organization can relocate with minimal losses to normal operations. Ideally, a hot site will be up and running within a matter of hours or even less. Personnel may still have to be moved to the hot site so it is possible that the hot site may be operational from a data processing perspective before staff has relocated. The capacity of the hot site may or may not match the capacity of the original site depending on the organizations requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organizations that operate real time processes such as financial institutions, government agencies and ecommerce providers.
Hurricane plan	A plan on how to deal with hurricanes before, during and after the hit.
Inbound traffic	Electronic traffic originating from outside the company's network.
Major operational disruption	High impact disruption of normal business operations, affecting a large geographic area and adjacent communities that are economically integrated to it.
Network security defense and recovery plan	A plan to defend against all types of forms of cyber crimes. When a security breach is in effect the institution should have a plan to control the situation and recover to normal operations.
Operational Risk	The risk of loss from inadequate or failed internal processes, people and systems or from external events.

Orientation/walk-through	An orientation/walk-through is the most basic type of test. Its primary objective is to ensure that critical personnel from all areas are familiar with the business continuity plan. It is characterized by: - Discussion about the business continuity plan in a conference room or small group setting; - Individual and team training; and - Clarification and highlighting of critical plan elements.
Outsourcing	The transfer of business functions to an independent third party supplier.
Public services for emergency response	The emergency responders like 911, Police, Fire Department or Ambulance Services.
RAID 1 (Redundant Array of Inexpensive Disks)	A backup solution, using two (possibly more) disks that each store the same data so that data is not lost when a hard disk crach occurs. This backup solution is also known as 'mirroring'.
RAID 5 (Redundant Array of Inexpensive Disks)	A backup solution that combines three or more disks in a way that protects data against loss of any one disk. This backup solution is also known as 'striped disks with parity'.
Reciprocal Agreement	An arrangement by which one organization agrees to use another's resources when a disruptive event occurs and visa versa.
Recovery	The rebuilding of a specific business operation following a disruption to a level sufficient to meet outstanding business obligations.
Recovery Objective	A predefined goal for recovering specific business operations and supporting systems to a specified level of service (recovery level) within a defined period following a disruption (recovery time).
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 backup storage for normal operations to resume if a computer, system, or network goes down as a result of a disruption.
Residual risk	Exposure to loss remaining after other known risks have been countered, factored in, or eliminated.
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 run smoothly.

Risk Appetite	Risk appetite is the amount of risk, on a broad level, an entity is willing to accept in pursuit of objectives. It reflects that organization's risk management philosophy and, in turn, influences the organization's culture and operating style. Risk appetite is also referred to as an acceptable level of risk in an organization in order to gain better benefit.
Risk Assessment	Steps in the assessment include: - Identification of assets; - Identification of threats and vulnerabilities; - Identification of controls; - Analyzing risk (probability/impact); - Evaluate risk (assessing residual risk) and - Treat risk.
Risk Management	A structured approach to managing uncertainty related to a threat. It includes a sequence of human activities to manage risk namely: risk assessment, strategies development to manage it, and mitigation of risk using managerial resources. The strategies include transferring the risk to another party, avoiding the risk, reducing the negative effect of the risk, and accepting some or all of the consequences of a particular risk.
Storage Area Network (SAN)	An architecture to attach remote computer storage devices (such as disk arrays, tape libraries and optical jukeboxes) to servers in such a way that, to the operating system, the devices appear as locally attached. SANs tend to enable more effective disaster recovery processes.
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.
Tabletop test/mini-drill	A tabletop/mini-drill is somewhat more involved than an orientation/walk-through type of test, because the participants choose a specific event scenario and apply the business continuity plan to it. It includes: - Practice and validation of specific functional response capability; - Focus on demonstration of knowledge and skills, as well as team interaction and decision-making capability; - Role playing with simulated response at alternate locations/ facilities to act out critical steps, recognize difficulties, and resolve problems in a non-threatening environment; - Mobilization of all or some of the crisis management/ response team to practice proper coordination; and - Varying degrees of actual, as opposed to simulated, notification and resource mobilization to reinforce the content and logic of the plan.

Tacit knowledge	Refers to a knowledge which is only known by an individual and that is difficult to communicate to the other individuals in an organization. With tacit knowledge, people are not often aware of the knowledge they possess or how it can be valuable to others. Tacit knowledge is considered valuable, because it provides context for people, places, ideas, and experiences.
Uninterruptible Power Supply (UPS)	Equipment that offer short-term protection against power surges and outages. UPS systems usually only allows enough time for vital services to be correctly powered down.
Warm site	Alternate site that typically contains pre-configured equipment necessary to rapidly start operations, but does not contain live data. Thus commencing operations at a warm site will (at a minimum) require the restoration of current data.

Appendix 2: Links to helpful websites

Organization	Website
FFIEC	www.**ffiec**.gov/**ffiec**infobase/**booklets**/bcp/bus_continuity_plan.pdf http://www.ffiec.gov/katrina_lessons.htm
ISACA	IS Auditing Guideline BCP
BSI	BS 25999-1:2006 BS 25999-2:2007
BIS	High level principles for business continuity management
Association of local authority risk managers	http://www.alarm-uk.org/PDF/BCM_and_the_CCA_Guide.pdf
Florida State	http://www.fldisasterkit.com/information_center/bcp_checklists.shtml
Weather.com	http://www.weather.com/maps/maptype/satelliteworld/caribbeansatellite_large.html

The Bank recommends supervised institutions to consider buying the Business Continuity Plan Generator[7]
The Software provides all the tools and support necessary to easily deliver an effective BCP by providing step-by-step guidance on each stage of the plan's development.
It comprises two volumes: -

- Part I - Business Continuity Planning Guidelines
- Part II - Business Continuity Planning Templates

It supports all aspects of the BCP process including the preparation of a detailed business risk assessment, development of strategic plans to mitigate the potential crisis, procedures to handle the disaster recovery phase, procedures to handle the business recovery phase, separate phases for testing and training in simulated conditions and instructions for keeping the plan up to date.

[7] http://www.bcpgenerator.com/

Appendix 3: Guide to the BCP Process