IVf

Overig toezicht

Guidelines for the Statement of Regulatory Compliance

BANK OF THE NETHERLANDS ANTILLES
(Central Bank)

Willemstad, August 2007

1. Introduction

In view of the importance of compliance, all supervised institutions that conduct foreign operations, either through a branch and or a subsidiary (hereinafter "entity"), should provide the Bank with a "Statement of Regulatory Compliance" (hereinafter "the Statement") as specified in these guidelines.

2. Purpose

The Statement serves to update the Bank on the ongoing compliance by the supervised institution's foreign entity with the laws and regulations of the relevant foreign jurisdiction(s) in which each operates (hereinafter "the regulatory regime").
These guidelines enter into effect as of September 2007, with the exception of the requirements specified under item 3.a, which enter into effect as of January 1, 2008.

3. Guidelines

a. With respect to the Statement:
   - the supervised institution should inform the Bank in a narrative form on its foreign entity's compliance with the regulatory regime.
   - the cut-off date for the Statement is December 31 of each year, and the Statement should be submitted to the Bank no later than March 31 of the following year.
   - in case of noncompliance the supervised institution should in the narrative form at least:
     a. indicate the relevant regulatory regime,
     b. inform the Bank on the reason(s) for the noncompliance, and
     c. indicate the steps that have been taken or are in progress and/or will be taken to become compliant with the regulatory regime.

     b. In addition to the requirements of item 3.a, and for its early update, the Bank should immediately be notified and informed by the supervised institution of any event of noncompliance with the regulatory regime that appears to be a potential threat to the continuity and /or reputation of its foreign entity. All notifications should be in writing.

The Bank is entitled to periodically verify the content of each Statement with the relevant foreign Supervisory Authorities.

4. Legal basis

These guidelines are based on the:

- National Ordinance on the Supervision of Banking and Credit Institutions (N.G. 1994, no.4), article 12, paragraph 1;
- National Ordinance on Insurance Supervision (N.G. 1990, no. 77), article 28, paragraph 1;
- National Ordinance on the Special Insurance License Degree (N.G. 1992, no. 50), article 18, paragraph 1;
- Funeral Service Insurers Decree (N.G. 1992, no. 53), article 4, paragraph 2;
- Lloyd's Underwriters National Decree (N.G. 1992, no. 54), article 3, and article 28, paragraph 1 National Ordinance on Insurance Supervision (N.G. 1990, no. 77);
- National Ordinance on Corporate Pension funds (N.G. 1985, no. 44), article 19;
- National Ordinance on the Insurance Brokerage Business (N.G. 2003, no. 113), article 18, paragraph 2, section a;
- National Ordinance on the Supervision of Trust Service Providers (N.G. 2003, no. 114), article 20, paragraph 2, section a;
- National Ordinance on Foreign Exchange Traffic (N.G. 1981, no. 67), article 26, paragraph 2 section a for money remitters; and
- National Ordinance on the Supervision of Investment Institutions and Administrators (N.G. 2002, no. 137), article 36, paragraph 2, section a.

IT Framework Memorandum For Supervised Institutions

CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

1. Introduction

For many organizations including the institutions supervised by the Centrale Bank van Curaçao en Sint Maarten (hereafter the Bank), information and their supporting systems are amongst their most valuable assets. Those organizations recognize the benefits of information technology and use it to drive their stakeholders' value. However, the evolving role technology plays in supporting the business function has become increasingly complex. Information Technology (hereafter IT) operations have become more dynamic and include distributed environments, integrated applications, telecommunication options, internet connectivity, and an array of computer operating platforms. As the complexity of technology grows, information systems and networks are faced with control weaknesses. Dependence on information systems and services means that organizations are more vulnerable to threats. It is a challenge to secure information systems and to have a good control environment in place.

Security should not only be achieved through technical means, but also supported by appropriate management policies and procedures. Identifying which controls should be in place requires careful planning and attention to detail.

The need for assurance about the value of IT, the management of IT-related risks and increased requirements for control over information are now considered as key elements of enterprise governance. Value, risk and control constitute the core of IT governance.

This IT Framework Memorandum (hereafter Memorandum) is the basis for the Supervised Institution IT Questionnaire (SIIQ) for Supervised Institution's and various Provisions and Guidelines that the Bank will issue. The SIIQ and related provisions and guidelines will provide Senior Management of supervised institutions with a firm basis to evaluate the risks inherent to the use of IT in their institutions. In addition the Memorandum serves to increase Senior Management's awareness of the general control elements that may be effective in safeguarding the institution's operations against such risks.

A strong control environment consists of policies, standards, procedures, practices, technologies and organizational structures designed to provide reasonable assurance that the business objectives are achieved and that undesirable events are prevented or detected and corrected.

Memorandum Objectives:
By executing this Memorandum the Bank aims to:
- Streamline the level of competence on the governance of IT for all supervised institutions;
- provide the institution's daily management and the board of supervisory directors a framework for effective governance of IT processes;
- provide the institution's IT management with guidelines that can be used to create a strong control environment;
- improve the security, stability and resilience of IT systems and professionalism of IT staff in the financial sector; and supply internal and external auditors of the financial sector with a framework to audit IT processes.

By complying with the IT Framework each supervised institution will contribute to maintaining a strong financial sector.
The Memorandum applies to all supervised institutions that are licensed to conduct activities in and/or from the islands of Curaçao and Sint Maarten.
The Provisions and Guidelines will cover different IT areas and the SIIQ should be proportionate to the operational risk (arising from both internal and external sources) and tailored to the nature, size, complexity, scale and scope of a supervised institution.

2. Legal Base
The Policy Memorandum is 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)

This Policy Memorandum applies to all financial institutions that are licensed to conduct activities in and/or from the islands of Curaçao and Sint Maarten pursuant to the aforementioned National Ordinances. The Policy Memorandum is intended to financial institutions of all sizes. However, the Provisions and Guidelines of the different IT areas and the Financial Institution IT Questionnaire should be proportionate to the operational risk (arising from both internal and external sources) and tailored to the nature, size, complexity, scale and scope of a Financial Institution.

3. Compliance

The board of supervisory directors[1] and the board of managing directors of supervised institutions should ensure that:

- the provisions and guidelines per IT area, covered in this Memorandum, are adhered to; and
- that audits are scheduled according to the nature, size, complexity, scale and scope of operations of the supervised institution.

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

The auditor should review and ascertain whether the provisions and guidelines are adequately executed 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 the provisions and guidelines per IT area;
- resources are acquired economically, used efficiently, and are adequately protected;
- programs, plans and objectives are achieved;
- quality and continuous improvement are accomplished; and
- opportunities for improving the business or the organization as a whole are recognized and addressed appropriately.

Each institution should perform such an audit of the IT area covered in this Memorandum at least once every two years unless indicated differently in the provisions and guidelines of the specific IT area. The audit has to be performed by a professional accredited IT-auditor. Based on the ordinances mentioned in chapter 2, the Bank will verify the implementation of the provisions and guidelines during its offsite supervision and/ or on-site examinations. Based on the outcome, the Bank will determine the adequacy of the supervised institutions' implementation of the provisions and guidelines.

4. IT Provisions and Guidelines

The policy objectives are realized by the design, implementation, monitoring, testing and maintenance of controls set out in the provisions and guidelines.

The Bank introduces provisions and guidelines to give direction to the governance of IT for the financial sector. The Bank keeps abreast with the actions of international regulatory bodies and institutions (e.g. BIS, FFIEC, ISO, OGC, and ISACA) and uses their standards to set tailored provisions and guidelines according to the nature, size, complexity, scale and scope of the institutions supervised by the Bank.

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

4.1. IT areas for which provisions and guidelines will be established

The Bank will provide further provisions and guidelines[2] for the following six (6) IT areas:

I. Information Security:

Its objective will be to provide guidance to:

– maximize the protection[3] of the supervised institution's information assets; and
– minimize potential legal and liability exposures in a cost effective manner.

The provisions and guidelines define the security requirements to protect information and data throughout their lifecycle. This includes the generation, capture, storage, processing, usage and destruction of information and data.

II. Business Continuity:

Its objective will be to ensure business resilience by protecting against threats that may manifest such as:

– natural events such as hurricanes, floods, fires and severe weather conditions;
– technical events such as power outage and fluctuations, communication failure, equipment and software failure; and
– malicious activities including network security attacks, public riots and armed assaults

III. IT Service management:

Its objective will be to ensure a controlled support and delivery of IT services executed by applications on:

– network devices (e.g. routers, switches, firewalls, intrusion detection systems, intrusion prevention systems);
– server and workstation, including operating systems; and
– databases.

IT Governance:

Its objective is to provide a framework for effective governance of IT that will assist those at the highest level of the supervised institutions to understand and fulfill their legal, regulatory, and ethical obligations in respect of their organization's use of IT.

IT governance aims to ensure that the institution's information and related technology support its business objects, that its resources are used responsibly, and its risks are managed appropriately.

[2] The Bank introduced the provisions and guidelines for E-Banking for commercial banks in 2007

[3] Protection in this regard means the integrity, confidentiality and availability of information assets.

IV. Development and Acquisitions:
Its objective is to effectively identify, acquire, install, and maintain appropriate information technology systems.
The provisions and guidelines will describe common project management activities and emphasize the benefits of using a well-structured project management and system development methodology.

V. Outsourcing IT services:
Its objective is to give guidance how to control the risks that are associated with the management of technology services outsourced to third parties.
By outsourcing services to a third party the responsibility of the availability of an all-encompassing control environment still remains at the outsourcing party being the supervised institution.
The following paragraphs contain an overview of what the Bank aims for within each of the IT areas.

4.2. Information Security

Information is one of the supervised institution's most important assets. Protection of this asset is necessary to establish and maintain trust between the supervised institution and its customers, remain compliant with the law, and protect the reputation of the institution. Timely and reliable information is necessary to process transactions and support the decisions of the supervised institution and its customers. A supervised institution's earnings and capital can be adversely affected if information is not available when needed, is wrongly altered, or becomes known to unauthorized parties.

In general, the financial sector also plays an important role in taking care of the financial services infrastructure. The security of the systems and information of the sector is essential to its safety and soundness and to the confidentiality of customer and business financial information.

The provisions and guidelines for information security requires supervised institutions to set up security programs to maximize the protection of their assets, satisfy regulatory obligations and minimize potential legal and liability exposures in a cost-effective manner.

The security program is the process by which the supervised institution's:
- security requirements are investigated, documented, analyzed and prioritized;
- physical, functional and operational security systems/controls are designed, built, tested, deployed, maintained and removed from service; and
- personnel is trained.

These security programs should have strong executive management level support, integration of security activities and controls throughout the organization's business processes, and clearly indicate the person(s) accountable for carrying out security responsibilities.

The supervised institution should develop, implement and manage a strategy to execute the security program. The strategy should embrace the following six basic outcomes of effective security governance:

a. strategic alignment:
   Aligning information security with business strategy to support organizational objectives;
b. risk management:
   Executing appropriate measures to mitigate risks and reduce potential impacts on information resources to an acceptable level;
c. value delivery:
   Optimizing security investments in support of business objectives;
d. resource management:
   Using information security knowledge and infrastructure efficiently, effectively and safely;
e. performance measurement:
   Monitoring and reporting on information security processes to ensure that objectives are achieved; and
f. assure process integration:
   Integrating all relevant assurance functions to ensure that processes operate efficiently and as intended.

The provisions and guidelines for information security will further require supervised institutions to create information security policies, standards, procedures and guidelines to cover the following topics:

- Asset Management:
  To achieve and maintain appropriate protection of the institution's assets;
- Human resource security:
  To ensure that employees, contractors, and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities;
- Physical and environmental security:
  To prevent unauthorized physical access, damage, and interference to the the institution's premises and information;
- Communications and operations management:
  To ensure the correct and secure operation of information processing facilities;
- Access control:
  To control read, add, update and delete access to information;
- Information systems acquisition, development and maintenance: To ensure that security is an integral part of information systems;
- Information security Incident Management:
  To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken; and
- Compliance:
  To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

4.3. Business Continuity Management

Disruption of operating can occur with or without warning, and the consequences may be predictable or unknown. Because supervised institutions play a crucial role in the country's economy, it is important that their business operations are resilient and the effects of disruptions in service are minimized in order to maintain public trust and confidence in our financial system. Effective business continuity planning establishes the basis for supervised institutions to maintain and recover business processes when operations have been disrupted unexpectedly.

The responsibility for business continuity management ultimately rests with the board of supervisory directors and senior management of the supervised institution. The board of supervisory directors and senior management are responsible for formulating the business continuity policy, standards, procedures and guidelines for the institution.
Business continuity management includes the drafting business continuity plan(s). But before the plans can be written, the institution should determine the impact disruptive events may have on the business.

Business Impact Analysis is the process of identifying, and measuring the business impacts, effects and loss that might result if the institution would suffer from a disruptive event. It is used to identify recovery priorities, recovery resource and essential staff requirements and to help shape the business continuity plan. All impacts should be measured based on financial, regulatory, legal and reputational damage

When a complete picture of the critical business elements is formed, a risk assessment will determine the probability and impact of specific threats to the business.

At least the following threats manifest in our region:
- natural events such as hurricanes, floods, fires and severe weather conditions;
- technical events such as power outage and fluctuations, communication failure, equipment and software failure; and
- malicious activity including network security attacks, fraud, assaults, public riot.

Before business continuity plans are drawn up to react on a disruptive event, it is important to make the business resilient by taking preventive actions to reduce either the likelihood and or impact of any disruptive event. Every specific disruptive event should have a set of cost effective preventive actions depending on the size of the supervised institution, the nature, the scale and the scope of operations and the complexity of its business.
For each disruptive event there should be an action plan to react after the event. I.e. Hurricane plan, Armed Assault plan, Building Evacuation plan, Business Recovery plan, and Disaster Recovery plan for the technical environment.
Business continuity plans can be organized in different ways. An effective setup is to create a principal plan, containing the mutual parts of the specific action plans, like the command structure of the management crisis team, emergency response teams, PR spokes person and a communication plan. Specific actions for disruptive events will be placed in the specific action plans.

The Bank will not dictate the format. However, the Bank will verify if the different disruptive events are covered by business continuity plans and if sufficient risk reducing controls are in place to reduce the impact and or likelihood.

4.4. IT Service Management

IT Service Management ('ITSM') is a process-based practice intended to align the delivery of information technology services with the requirements of the organization, emphasizing the benefits to customers (internal and external). ITSM involves a paradigm shift from managing IT as stacks of individual components to focusing on the delivery of end-to-end services. ITSM is a concept that compromises processes and procedures for efficient and effective delivery and support of various IT Functions. It focuses on tuning IT services to meet the changing demands of the organization, and to measure and show improvements in the quality of IT services offered with a reduction in cost of service in the long term.
The transformation from traditional "Business - IT paradigm" can be depicted by some of the following attributes:

Traditional IT	**becomes**	**ITSM Process**
Technology focus		Business process focus
"Fire-fighting"		Preventative
Reactive		Proactive
Users		Customers
Isolated, silos		Integrated, enterprise-wide
Adhoc		Repeatable, accountable
Informal processes		Formal best- practices
Operational specific		Service orientation

The provisions and guidelines for IT service management will require supervised institutions to set up the processes and controls for the support and delivery functions of IT services.

IT support services

- *Service desk*:
  This provides a central point of contact between customers and IT;
- *Incident management*:
  The day-to-day process that restores normal acceptable service with a minimal impact on business;
- *Problem management*:
  The diagnosis of the root causes of incidents in an effort to proactively eliminate and manage them;
- *Configuration management*:
  Physical and logical perspective of the IT infrastructure and the IT services being provided;
- *Change management*:
  Standard methods and procedures for effective managing of all changes; and
- *Release management:*
  Testing, verification, and release of changes to the IT production environment.

IT delivery services

- *Service level management*:
  Maintain and improve the level of service to the organization;
- *IT financial management*:
  Managing the costs associated with providing the organization with the resources needed to meet requirements;
- *Capacity management*:
  Enables an organization to tactically manage resources and strategically plan for future resource requirements;
- *IT service continuity management*:
  Managing an organization's capability to provide the necessary level of service following an interruption of service; and
- *Availability management*:
  Optimize IT infrastructure capabilities, services, and support to minimize service outages and provide sustained levels of service to meet business requirements.

Service levels are often defined to include hardware and software performance targets (such as user response time and hardware availability), but can also include a wide range of other performance measures. Such measures might include financial performance measures (such as year-to-year cost reduction), human resource measures (such as competence level of personnel) or risk management measures (compliance with control objectives).

4.5. IT Governance

IT Governance fundamentally comprises two issues, namely that IT delivers value to the business and that IT risks are mitigated. The first is driven by strategic alignment of IT with the business. The second is driven by embedding accountability into the organization. IT Governance is the responsibility of the board of supervisory directors together the board of managing directors. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the institution's IT sustains and extends its strategy and objectives. Additionally, IT should enable the institution by exploiting opportunities and maximizing benefits. IT resources should be used responsibly, and IT-related risk should be managed appropriately.

Additional to the regular IT functions (e.g. IT Management, Operations, and Development) the organizational structure should include the availability of:

- an IT steering committee;
- an Audit function;
- an IT security function; and
- a Risk Management function.

Critical to the success of these IT functions is effective communication among all parties based on constructive relationships, a common language, and a shared commitment to address issues.

All supervised institutions should have:
- defined roles and responsibilities for all IT related functions (including committees);
- an effective planning process that aligns IT and business objectives;
- an ongoing risk assessment process that evaluates the environment and potential changes;
- establishment of policies, standards, procedures and guidelines and appropriate controls per IT area;
- a defined audit universe[4] and long term plans to audit all areas of the universe;
- an effective human resource management plan;
- financial oversight and controls to manage and adjust IT budgets as the book year progresses; and
- measurement and monitoring efforts that effectively identify ways to manage IT processes.

4.6. Development and Acquisition

Project failures are all too common. The reasons for failure are diverse. Some common causes are:
- lack of co-ordination of resources and activities;
- lack of communication with interested parties, leading to products being delivered which are not what the customer wanted;
- poor estimation of duration and costs, leading to projects taking more time and costing more money than expected;
- insufficient measurability;
- inadequate planning of resources, activities, and scheduling;
- lack of control over progress so that projects do not reveal their exact status until too late; and
- lack of quality control, resulting in the delivery of products that are unacceptable or unusable.

Without a project management method, those who commission a project, those who manage it and those who work on it might have different ideas how things should be organized and when the different aspects of the project will be completed. Those involved will not know how much responsibility, authority and accountability they have and, as a result, the project is insufficiently transparent to the participants.

Without a project management method, projects are rarely completed on time and within acceptable costs. This is especially true for large projects.
A good project management method will guide the project through a controlled, well-managed, visible set of activities to achieve the desired results. Principles of good project management avoid the problems identified above and thus help to achieve successful projects.

[4] Audit universe is the set of all the functions, processes, systems, data, and facilities within the organization that require audit attention in other words the domain that can be audited by the IT Auditors

These principles are the following:
– a project is a finite process (with a start and ending date);
– a project always needs to be managed in order to be successful; and
– for genuine commitment to the project, all parties should understand why the project is needed, what is its objective, how the outcome is to be achieved and what their responsibilities are in that achievement process.

The Development and Acquisition provisions and guidelines will describe common project management activities and emphasize on the benefits of using well-structured project management and system development methodology. Mentioned guidelines will detail general project management standards, procedures, and controls and discuss development, acquisition, and maintenance risks.

Subjects that will be dealt with are:
- Project Management;
- Design;
- Acquisition/Development;
- Testing;
- Implementation; and
- Maintenance.

4.7. Outsourcing Technology Services

The evolving role technology plays in supporting the business function has become increasingly complex. IT operations have become more dynamic and include distributed environments, integrated applications, telecommunication options, internet connectivity, and an array of computer operating platforms. As the complexity of technology has grown, the financial industry has increased its reliance on vendors, partners, and other third parties for a variety of technology solutions and services. Institutions will frequently operate or manage various IT resources from these third-party locations.

Supervised institutions can outsource many areas of their operations, including all or part of any service, process, or system operation.

Management may choose to outsource operations for various reasons. Some of these are to:
- gain operational or financial efficiencies;
- increase management focus on core business functions;
- refocus limited internal resources on core functions;
- obtain specialized expertise;
- increase availability of services;
- accelerate delivery of products or services through new delivery channels;
- increase the ability to acquire and support current technology and avoid obsolescence; and
- conserve capital for other business ventures.

Before considering the outsourcing of significant functions, a supervised institution's board of managing directors should ensure that such actions are consistent with the institution's strategic plans and should evaluate outsourcing proposals against well-developed acceptance criteria.

Outsourcing, however, does not reduce the fundamental risks associated with information technology or the business lines that use it. Risks such as loss of funds, loss of competitive advantage, damaged reputation, improper disclosure of information, and regulatory action remain present.

Because the functions are performed by an organization outside the supervised institution, the risks involved may unfold in a different manner than when the functions were performed by the supervised institution itself. This requires the need for controls designed to monitor such risks.

Supervised institutions should have a comprehensive outsourcing risk management process to govern their technology service provider relationships. The process should include risk assessment, selection of service providers, contract review, and monitoring of the service providers. The outsourced activities should be subject to the same risk management, security, privacy, and other policies that would be expected if the supervised institution would conduct the activities in-house.

5. Implementation of IT provisions and guidelines

On completion of the IT provisions and guidelines the Bank will send the draft version for comment to the representative organizations of the supervised institutions.

The organizations have a period of two months to provide their comments.

Relevant received feedback will be taken into account and the final version will be put on the Bank's web-site.

All supervised institutions will receive a notification with the exact URL-link of the IT provisions and guidelines.

The Bank can also choose to introduce a particular IT provisions and guidelines by inviting the representatives of supervised institutions of all sectors at the Bank's premises for an introductive explanatory presentation.

The provisions and guidelines per IT area are scheduled to be introduced during the coming years. The first one will be the "Provisions and Guidelines for Business Continuity Management". This will be succeeded by the IT areas:

- Information Security;
- IT Service management;
- IT Governance;
- Development and Acquisition; and
- Outsourcing Technology Services.

6. The Supervised Institution IT Questionnaire

In addition to the provisions and guidelines the Bank will also introduce a Supervised Institution IT Questionnaire ('SIIQ'), which is aligned with the IT areas mentioned above. The purpose of the questionnaire is that every supervised institution can audit its IT areas and determine the IT maturity level of the institutions and thus pro-actively improve weak areas. The Bank will send out the IT questionnaire to all supervised institutions in 2010.

The areas that will be covered within the questionnaire are the same areas covered by the provisions and guidelines. Because the questionnaire will be sent prior to most of the IT provisions and guidelines, institutions can already take notice of the controls the Bank requires per IT area. In this regard, institutions can already plan for the implementation of the controls prior to receiving the provisions and guidelines of an IT area.

The majority of questions refer to existing controls and policies at a supervised institution. Policies, however, differ per institution. One institution can integrate all possible security controls in one security policy whereas another institution separate security controls in multiple policies.

The purpose of this questionnaire is to test if a control is in place. The name of the policy is less important. For example: The control "Each User must have a unique account identifier or user ID" can be part of a 'Password policy', 'User account management policy' or a 'Security policy'.

The questions are formulated in such a manner that they may be answered "Yes", if the control is in place or "No" if that is not the case. In the event that a particular question does not apply, this should be clearly indicated in the "N/A" column. Where necessary, explanations should be provided in the "Comments" column or included in a separate annex.

Each institution should complete this questionnaire and send it to the Bank once every two years. The questionnaire should be signed by the senior management. In addition the electronic version should be sent to the Bank. The Bank will provide a secure way to send the electronic version through the Bank's website.

7. Reference

BIS The Bank for International Settlements is an international organization of central banks, which "fosters international monetary and financial cooperation and serves as a bank for central banks." The BIS carries out its work through subcommittees, the secretariats it hosts, and through its annual General Meeting of all members. One of the committes, the Basel Committee on Banking Supervision, has issued recommendations on banking laws and regulations.

FFIEC The Federal Financial Institutions Examination Council is 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 Fe-

deral 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.

ISO The International Organization for Standardization is an international-standard-setting body composed of representatives from various national standards organizations. While ISO defines itself as a non-governmental organization, its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most non-governmental organizations.

OGC The Office of Government Commerce is an independent office of Her Majesty's Treasury, a department of state in the government of the United Kingdom. The organization developed the standards:

- Information Technology Infrastructure Library (ITIL)
- PRojects IN Controlled Environments (PRINCE2)
- Managing Successful Programmes (MSP)
- Management of Risk (M_o_R)

ISACA Information Systems Audit and Control Association is an international professional association for IT auditors, consultants, educators, IS security professionals, regulators, chief information officers and internal auditors. ISACA provides the certifications:

- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified in the Governance of Enterprise IT (CGEIT)

The organization developed:

- Standards, Guidelines and Procedures for information system auditing
- COBIT (Control Objectives for Information and related Technology is a set of best practices (framework) for information technology (IT) management
- Val IT (Getting best value from IT investments)

Provisions and Guidelines For Business Continuity Management

CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

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 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,

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

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.

[6] Appendix 1 has a Glossary/Definitions section

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 cannot reimburse a supervised institution's loss of reputation.

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 corrupted.
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 crash 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	Equipment that offer short-term protection against power surges
Power Supply (UPS)	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

FFIEC www.ffiec.gov/ffiecinfobase/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 Florida State
http://www.alarm-uk.org/PDF/BCM_and_the_CCA_Guide.pdf
http://www.fldisasterkit.com/information_center/bcp_checklists.shtml
Weather.com
http://www.weather.com/maps/maptype/satelliteworld/caribbeansatellite_large.html

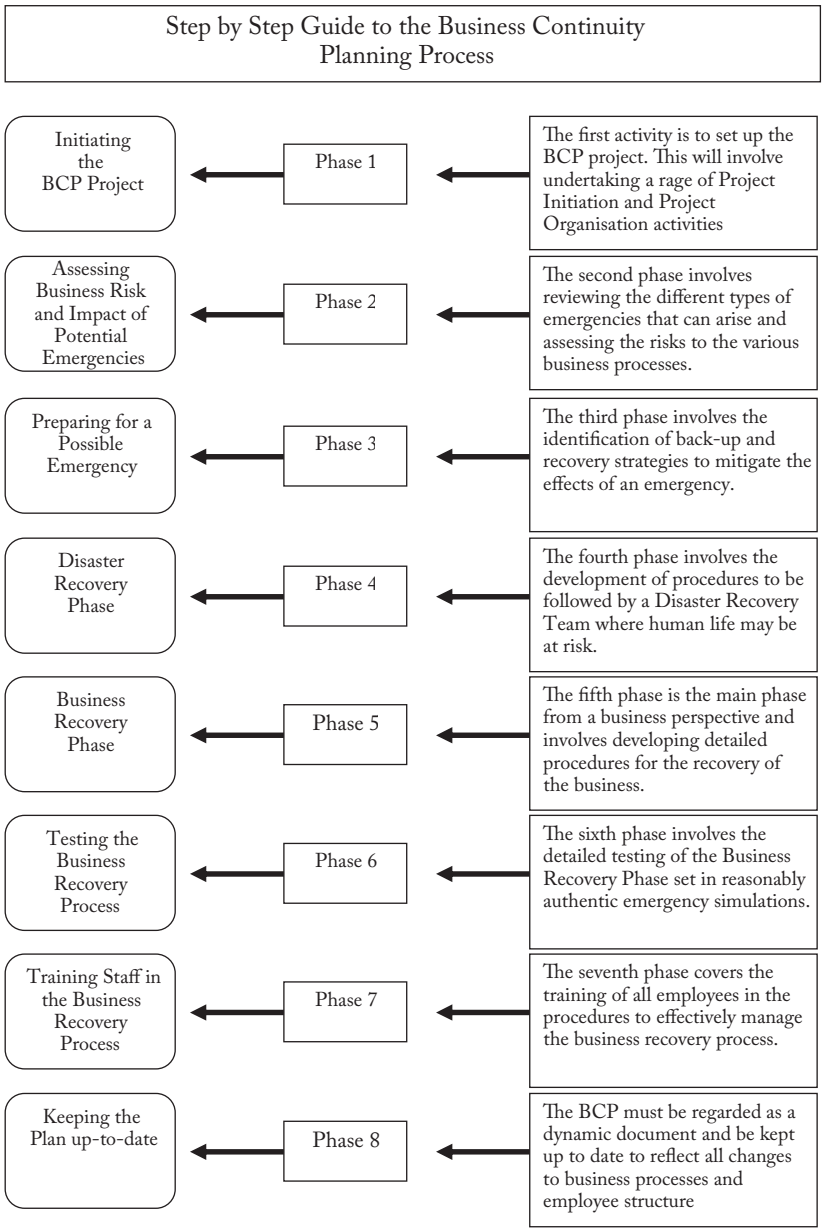
The Bank recommends supervised institutions to consider buying the Business Continuity Plan Generator[7]
The Software provides all the tools and support necessary to easily deliver an effective BCP by providing step by step guidance on each stage of the plan's development It comprises two volumes:

- 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



Provisions and Guidelines For Information Security Management

CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

I. Introduction

The "Provisions and Guidelines for Information Security Management" (hereafter "ISM Provisions") are issued with the objective to further promote and ensure safe and sound practices with respect to Information Security Management (hereafter "ISM") among the institutions subject to the supervision of the Centrale Bank van Curaçao en Sint Maarten (hereafter "the Bank").

The objective of ISM is to:
- Maximize the protection of the supervised institution's information assets;
- Meeting regulatory requirements; and
- Minimize potential legal liability and reputational exposures in a cost effective manner.

With "protection" in this context is meant:
"Ensuring confidentiality[1]*, integrity and availability of information assets".*
Information assets not only include supervised institution's data and documents, but also supporting systems and personnel.

With "regulatory obligations" in this context is meant:
"Complying with regulations set by the Bank, but also international agreements and regulations set by international institutions such as IMF and BIS"

With "Minimize potential legal liability and reputational exposures" is meant:
"Minimizing breaches of country and international laws, breaches of contracts with third parties and exposures to ethical issues"

With "cost effective" is meant:
"Prioritizing information security investments to areas where it is most needed".
This can only be determined after a thorough information security risk assessment.

The ISM Provisions provides principles for structuring a comprehensive ISM program and implement an Information Security Management Framework[2].

The ISM Provisions' objective is to safeguard the interest of the supervised institutions' key stakeholders, reputation, brand and value creating activities. As supervised institutions play a crucial role in our economy, it is important, that the effects of disruptions, cyber threats,

1 Please refer to Appendix 1 for definitions.
2 See principle 2 §2.1 for information on what should be included in this framework

privacy violations and other information security threats regarding services to the public are also mitigated. This will contribute to maintain public trust and confidence in our financial sector.

The responsibility for ISM ultimately rests with the Board of Supervisory Directors[3] and the Board of Managing Directors of an institution. The Board of Supervisory Directors oversees and approves the establishment of the ISM framework, while the Board of Managing Directors is responsible for the implementation thereof. The Board of Managing Directors and Senior Management, as appropriate, are actively involved in the oversight of the implementation of the ISM framework. It is important to understand that information security is a shared responsibility for various roles in the organization. The cooperation and collaboration of managers, users, administrators and specialists in the areas such as insurance, legislation, human resources, IT, security, risk management and auditing will determine the success of the ISM framework.

The ISM Provisions apply to all supervised institutions. However, supervised institutions should mitigate operational risks tailored to the nature, size, and scope of its operations and complexity of its business.

The ISM Provisions sets out **what** principles need to be carried out. **The manner** in which the organization implements the ISM Provisions and **to which extent** inherent information security risks are mitigated is the responsibility of the supervised institution. The institution's internal and external auditors will verify if the principles provided in the ISM Provisions are adhered to and if controls are in place to ensure that inherent information security risks are managed adequately.

II. Legal base and scope

The ISM Provisions 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 ISM Provisions apply to all institutions that fall under the supervision of the Bank. However, information security controls should be proportionate to the supervised institu-

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

tion'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.

The ISM Provisions adds on to other regulations of the Bank and do not replace any.

III. Implementation

To ensure a high standard of financial management in our country, supervised institutions are required to start the implementation of the ISM Provisions by July 1, 2011.
The implementation of the initial ISM program must be completed by July 1, 2015, and according to the schedule detailed in paragraph 2.4

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

In the role of supervisor the Bank's examiners will review the work performed by the supervised institution and its auditors during onsite examinations and offsite reviews.

The Board of Supervisory Directors and the Board of Managing Directors of the supervised institutions should familiarize themselves with the ISM Provisions and understand the objectives and implications of the principles elaborated upon in the following chapters.

IV. Information Security Management principles

Principle 1.

The Board of Supervisory Directors and the Board of Managing Directors of a supervised institution should establish effective management oversight with respect to potential events that threatens the security of information assets of the supervised institution.

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

1.1 Establishing ISM policies, standards and procedures

The Board of Supervisory Directors and the Board of Managing Directors are ultimately responsible for identifying, assessing, prioritizing, managing, and controlling information security risks. By establishing ISM policies, management sets out:

- The organization's aims, principles, and approach to ISM;
- Key roles and responsibilities in the ISM process; and
- How ISM will be governed and reported upon, including key performance indicators and key goal indicators.

The effectiveness of ISM depends on management's commitment and ability to clearly identify what makes existing business processes work properly and safely. Each supervised

institution should evaluate its own unique circumstances and environment to develop appropriate ISM policies, standards and procedures.

Adapting to the Information Security Standard 'ISO 27000-series' will provide the supervised institution a solid base to build on. Supervised institutions are free to choose any standard, however in order to have a common and solid foundation for ISM, the ISM policies, standards and procedures should at least cover the ISO 27002 control objectives[4]:

- *Asset Management:*
  To achieve and maintain appropriate protection of information assets;
- *Human Resource Security:*
  To ensure that employees, contractors, and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, ethical issues, fraud or misuse of facilities;
- *Physical and Environmental Security:*
  To prevent unauthorized physical access, damage, and interference to the organization's premises and information;
- *Communications and Operations Management:*
  To ensure the correct and secure operation of information processing facilities;
- *Access Control:*
  To control read, add, update and delete access to information;
- Information systems acquisition, development and maintenance:
  To ensure that security is an integral part of information systems;
- *Information Security Incident Management:*
  To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken;
- *Business Continuity Management* [5]:
  To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption;
- *Compliance:*
  To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements; and also
- *Implementing technical security standards* [6] *for amongst others:*
  - Servers;
  - Desktops;
  - Mobile devices;
  - Network peripherals;
  - Software; and
  - Database Management Systems.

4 Please refer to the ISO 27002 standard for the details of these control objectives

5 See also the Provisions and Guidelines for Business Continuity Management

6 Development of appropriately hardened systems using standard configurations; Controlled introduction of changes using a formal change management procedure; Controlled Patch Management; Anti-virus update management

1.2 Allocating sufficient resources and knowledgeable/competent staff

The Board of Supervisory Directors and the Board of Managing Directors should allocate sufficient time and adequate resources to accomplish the ISM principles. A large and or complex institution may need a steering committee for ISM and establish multi disciplinary teams to accomplish ISM. In contrast, a smaller and or less complex institution may only require a single ISM coordinator.

While the appointed ISM steering committee[7] recommends certain prioritization and plans to mitigate risks, ultimately the Board of Supervisory Directors and the Board of Managing Directors are responsible for understanding ISM risks. Subsequently plans should be made to ensure that business objectives are achieved and undesirable events are prevented or detected and corrected.

1.3 Formally approving ISM policies, standards and plans

The Board of Managing Directors should formally approve the ISM policies, standards and all plans to mitigate information security risks. In addition the Board of Managing Directors should ensure that new business endeavors also apply the Information security policies and standards. The Board of Supervisory Directors should at least annually verify the effort of the Board of Managing Directors on ISM activities.

1.4 Ensuring the quality of the ISM 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 ISM activities and deliverables 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.
Supervised Institutions should design, implement and maintain an ISM framework

With respect to the ISM framework, the supervised institution should undertake the following.

2.1 Design an ISM management framework

Supervised institution should design an ISM framework, which includes:

- The policies, standards, procedures and guidelines;
- Technologies; and
- Organizational structures

and is designed to provide reasonable assurance that:

- The information security strategy is achieved in alignment with the business objectives;
- Appropriate measures are taken to mitigate risks and reduce potential impacts on information resources to an acceptable level;

[7] We will only refer to "SIM steering Committee" for the remainder of the text of the "Provisions for ISM', however, smaller and or less complex institutions can substitute "ISM steering Committee" for "ISM coordinator".

- Investments in information security are optimized;
- Information security knowledge and infrastructure are used efficiently, effectively and safely;
- Information security processes are monitored and reported on to ensure that objectives are achieved and undesirable events are prevented or detected and corrected;
- All relevant information security assurance functions are integrated to ensure that business processes operate efficiently and as intended; and
- Responsibilities of information security are clearly assigned, managed and enforced.

As mentioned in paragraph 1.1 adapting to the Information Security Standard 'ISO 27000-series' will give the supervised institution a solid base to build on. However, there are more standards available such as the "Sherwood Applied Business Security Architecture" (SABSA[8]). SASBA is a framework and methodology for enterprise security architecture and service management. Also, the bigger consulting firms have proprietary security frameworks. Furthermore, a good source for information security standards is the National Institute for Standards and Technology ('NIST').

In addition, for information security risk management several methodologies are available including ISO 31000, "Operational Critical Threat, Asset and Vulnerability Evaluation" (Octave) and the NIST SP 800-37.

2.2 Collect, document, analyze and prioritize information security requirements
To establish the framework supervised institutions should collect, document, analyze and prioritize information security requirements[9].

ISM work group
Supervised institutions that have not created an ISM framework as yet might want to establish an ISM working group to start the ISM process. This group should consist of experts on subject matters of the business and IT. The goal for this group is to establish the ISM program, which will lead to the implementation of the ISM framework.
Implementing an ISM framework takes several years to accomplish. Most commonly supervised institutions will have some parts of the ISM framework already implemented. In order to schedule the work that still has to be performed an ISM program should be drafted. The ISM program will consist of many projects, which will require many different resources.

Quick scan/Gap analyses
In order to determine the size of the information security program the ISM workgroup might want to perform a quick scan (using questionnaires and interviewing key personnel) to quickly analyze the gap between current controls versus required controls. This will

8 See appendix 2 for an overview of helpful websites
9 It is not the Banks intention to prescribe the steps to take to collect, document analyze and prioritize information security requirements. In section 2.2 we only want to provide some guidance on how to reach to this goal.

assist in determining the amount of work that needs to be performed and the required investment to be made. The required controls can be derived from the ISO 27002 standard, internal sources or other sources such as ISACA - COBIT, the NIST SP 800-53 publication, FFIEC - Information Security Booklet or the Bank's Supervised Institution IT Questionnaire.

2.3 Create a written ISM program

The ISM program will be unique to every institution. Some important elements may have already been executed. To give a general idea of the topics that could be covered by the ISM program we mention:

- Short term risk mitigating actions for high risk situations (exposed as a result of the quick scan);
- Setup of the information security policy, standards and procedures;
- Setup of information security governance (e.g. establishing an IS steering committee, determining IS ownership and responsibilities, appointing an Information Security Manager);
- Setup of security baseline configurations for devices, DBMS and software;
- Identification of information assets and establishing and executing a risk assessment plan;
- Data classification and protection;
- End point security (e.g. USB sticks, mobile phones, laptops);
- Document and e-mail control (e.g. Secure document workflow and record management);
- Human resource security;
- Physical and environmental security;
- User management security;
- Outsourced services risk review;
- Customer, retailers and business partners risk review;
- Legal security requirements regarding country or international law and contracts with external parties;
- Software and user license management;
- Adding information security procedures to information systems acquisition, development, deployment and maintenance procedures;
- Network security assessment;
- Vulnerability management;
- Patch and anti-virus management;
- Backup/restore management;
- Information security awareness training;
- Creating a change management procedure for hardware and software changes;
- Disaster Recovery;
- Incident Management and Response;
- Intrusion Detection / Intrusion Protection; and
- Log analyses and network monitoring.

To create and execute the ISM program the supervised institution might want to adopt a project management methodology such as Prince2[10] or PMBok. These methodologies can assist the supervised institution in developing a thorough program.

2.4 Implement the initial ISM Program within four years

It is important that the supervised institution schedules all the projects that need to be executed. The IS steering committee needs to prioritize the projects and determine the time frame to accomplish the initial ISM program.

Some projects, e.g. the first time a risk assessment is executed, require a heavier load on resources initially, but require lesser effort in the future (if executed correctly the first time). Most of the projects need to be repeated in the future and some are continuous.

In order to have the initial program finished by July 1, 2015, the Bank recommends applying the following schedule.

Scheduled work	**Must be completed by:**
Business Continuity Management[11]	1-Jul-2011
Information security policy	31-Dec-2011
Initial ISM plan	1-Apr-2012
Implemented formal information security risk assessment methodology	1-Jul-2012
Information security training for all personnel	1-Oct-2012
Comply with ISO 27002 control objectives for: – Asset Management; – Human Resource Security; – Physical and Environmental Security; – Communication and Operations Management; – Access Control; – Information Security Incident Management; and – Compliance.	31-Dec-2012
Implementing technical security standards for amongst others: – Servers; – Desktops; – Mobile devices; – Network peripherals; – Software; and – Database Management Systems.	1-Jul-2013
All aspects of Principle 4 - Implement information security monitoring.	31-Dec-2013
All aspects of initial ISM plan and ISM Provisions implemented	1-Jul-2015

[10] For further reference see appendix 2

[11] See Provisions and Guidelines for BusinessContinuity Management.

2.5 Maintain the ISM framework
The ISM framework should be reviewed by the supervised institution at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness.

These changes occur amongst others due to:
– Restructuring of an institution, either through expansion or through a merger;
– Changed IT or business strategy ;
– Changed risk appetite;
– Reported security incidents;
– Altered legal and regulatory conditions;
– Changed technical environment or outsourcing; and
– Trends related to threats and vulnerabilities.

Principle 3.
Supervised Institutions should maintain an ongoing information security risk assessment program

The implementation of an ongoing information security risk assessment program should be part of the ISM framework.

With respect to the ongoing program, the supervised institution should undertake the following.

3.1 Implement a risk management methodology
By implementing a risk management methodology supervised institutions assure that the risk assessment process is standardized. In addition, the institution should develop standardized assessment and reporting templates. A standardized risk assessment process ensures that the risk assessment renders comparable and reproducible results. All relevant information should be properly documented and archived for future reference and to serve as evidence during audits and reviews.

Risk assessment
A combination of the following methods and techniques may be used to carry out the risk assessment:
– Interviews;
– Walkthroughs;
– Workshops;
– Questionnaires;
– "Computer-assisted audit techniques" (CAAT) (e.g. vulnerability scanning); and
– Network penetration testing.

Information assets
The process should at least identify:
– The supervised institution's information assets, such as:
  • Policies, procedures, guidelines, user manuals;
  • Organizational chart;
  • Function descriptions;
  • Business applications;
  • The data used by business applications and flow and staging of data;
  • Roles and Authorization matrix;
  • Operating Systems;
  • Database management systems;
  • IT utility programs;
  • The existing network infrastructure;
  • The communication links between the IT systems and the outside world; and
  • The hardware in use (e.g routers, firewalls, servers);
– The owners of these assets;
– The value and sensitivity of information assets;
– The threats to those assets;
– The vulnerabilities that might be exploited by the threats; and
– The implemented security controls.

Business impact analyses and evaluation
The process should at least:
– Assess the business impacts upon the institution that might present as a result of:
  • Losses due to failure of confidentiality, integrity or availability of information assets;
  • Non compliance with international agreements and regulatory bodies; and
  • Legal liability and reputational exposure when breaching country or international law, contracts with external parties or as a result of ethical issues.
– Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented; and
– Estimate and document the levels of risk (e.g. high, medium, and low).

Risk treatment
Possible ways to mitigate a risk include:
– Applying appropriate controls or enhancing implemented controls, such as
  • Enhanced policies, standards, procedures and guidelines;
  • Organizational structures with clearly defined authorization levels;
  • Four eyes principle;
  • Least privilege principle;
  • Application controls; and
  • IT general controls (e.g. controls for information processing facility, computer operations, access to programs and data, program development and program changes).

With regard to applying controls we remark that:
– Preventive controls prevail over detective and corrective controls;
– Automated controls prevail over manual controls; and
– A layered protection scheme (defense-in-depth) for critical components should prevail over singular distinct protection.
– Accepting the risk (e.g. costs outweigh benefit when implementing controls);
– Avoid the risk (e.g. by discontinuing a service); and
– Transferring the risk (e.g. opt for insurance coverage).

Risk assessment report
The results of the risk assessment should be formalized in a risk assessment report. This report will help to guide and determine the appropriate strategy to manage information security risks.
The IS steering committee should evaluate the risk assessment report and seek the Board of Managing Directors' approval for appropriate actions.

3.2 Ensure compliance
To ensure compliance with the institution's information security policy all relevant controls established by the information security policy and standards should be included in the risk assessment. Consequently, the assessor may also encounter topics, not covered by the information security policy, standards or procedures. In such cases appropriate steps should be taken to enhance the information security policy, standards or procedures.

3.3 Perform a risk assessment when implementing new information systems
Any change to the information system may introduce new threats and vulnerabilities. A risk assessment should be conducted before new information systems are implemented or important components of the information system are replaced.

3.4 Repeat risk assessments periodically
Risk assessments should be undertaken periodically to address any changes that might influence the risk assessments results. E.g. new threats can emerge; new vulnerabilities may be discovered; but also, security incidents may create new views on business impact.

Principle 4.
Financial Institutions should establish information security monitoring

The implementation of information security monitoring should be part of the ISM framework.

A static information security framework provides a false sense of security and will become increasingly ineffective over time. Information security monitoring and updating the information security framework is an essential part of the ongoing process of ISM. Therefore institutions should implement the daily and periodic operational execution of information security monitoring tasks (who, what, why, how, where, when).

Monitoring in this context should at least include:
– Log file analyses;
– Capacity management;
– Vulnerability management ; and
– Managing metrics data.

Log file analysis
The purpose of systems log analyses is to detect unauthorized processing activities and system defects. System logs record user activities, exceptions, and information security events.

Logs are emitted by network devices, operating systems, applications and all intelligent or programmable devices. Log file analysis must interpret messages within the context of an application, vendor, system or configuration in order to make useful comparisons to messages from different log sources.

System logs should be produced and kept to assist in future investigations and access control monitoring. The systems to analyze, the level of monitoring required, and the period to keep the log history available should be determined by a risk assessment.

It is advisable to direct log files to a centralized log file management software. Log file management software can assist to centrally collect, filter, analyze and alert on events. This improves the analysis process, because log files contain huge amounts of messages daily, which is a tedious task to interpret when done manually.

A global trend in log file analysis is to outsource the monitoring of intrusion detection (and protection) on the border firewalls[12]. Because of the specific technical knowledge to interpret outbound traffic and to implement effective controls increasingly organizations leave this task to companies who are specialized in this field. In such a case, the supervised institutions should very carefully select the outsourced company.

Capacity management
For each new and ongoing activity, capacity management requirements should be identified. System tuning and monitoring should be applied to ensure and improve the availability and efficiency of systems. Detective controls should be in place to indicate problems in due time. Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organization's information processing capabilities.
Capacity management can be divided into 'performance' and 'volume' measuring. In this respect, 'performance' is a factor for e.g.:
– Bandwidth of connectivity within and between network segments;
– Processing power of servers, desktops and other devices; and
– Network segments linkages (switches, routers, hubs, gateways, network cards).

[12] The border firewalls are located between the institutions network and the internet. It is the first point of access for outbound traffic after it is routed as incoming traffic.

And 'volume' is a factor for e.g.:
- Hard disks, tapes and other media;
- Database tables; files and other data containers;
- Amount of servers, desktops and other devices; and
- Available physical space.

It is advisable to automate capacity management processes as much as possible. In this regard, specialized network management software can assist to automate capacity management.

Vulnerability management
Supervised institutions should continuously gather and analyze information regarding new threats and vulnerabilities, actual attacks on their institution and others, and the effectiveness of existing security controls. As a result, the risk assessment process, the information security strategy and implemented controls should be updated appropriately.

Vulnerability management should at least include:
- The establishment of a process to gather information from external sources for vulnerabilities and threats regarding hardware and software;
- The implementation of patch management, including testing new patches in a test environment;
- Maintaining up-to-date anti-virus definitions and intrusion detection attack definitions;
- Communication with service providers and vendors to identify and react to new security issues; and
- The periodic assessment of hard and software vulnerabilities (vulnerability scanning/penetration testing). These activities are increasingly outsourced to companies specialized in this field.

Managing metrics data
Metrics is a system of measurement. As defined earlier the objective of the "ISM" is to:
- Maximize the protection of the supervised institution's information assets;
- Satisfy regulatory obligations; and
- Minimize potential legal liability and reputational exposures

in a cost effective manner.

Supervised institutions should define a system of measurement in order to confirm that the objectives of ISM are accomplished. In this regard, the establishments of metrics are important management and operational tools.

Key conditions to create effective metrics[13] are:
- Having a defined process;
- Having clear goals/performance requirements; and

[13] Metrics should be S-M-A-R-T (Specific, Measurable, Agreed upon, Realistic, Timely) See also: Appendix 3

– Having quantitative/qualitative measures for the process.

Metrics need to allow management to:
– Measure achievement;
– Drive performance; and
– Improve and realign towards goals.

Supervised institution should at least use the following types of measurements:
– Key Performance Indicators 'KPI' as measurement of performance; and
– Key Goal Indicator 'KGI' as a measurement of outcome.

Metrics may be introduced to measure performance and outcome, including but not limited to:
– **The organization** e.g. employee performance, budget and resource usage; timeliness of projects;
– **Security events** e.g. number of security incidents, open/closed issues, response time and remediation time;
– **Operations** e.g. timeliness of patch update schemas and anti-virus definitions, events due to improper capacity management
– **Business value** e.g. estimated vs actual costs of security controls, impact on employee productivity, total cost of ownership vs income generated from a business process;
– **Compliance** e.g. number of controls implemented/still open, number of policy exceptions applied for/granted.

Principle 5.
Supervised institutions should establish incident management and response

Incident management and response should be part of the ISM framework.

Reporting of information security events
Personnel, contractors and third party users should be instructed to report information security events and weaknesses as soon as observed to allow for timely corrective action. To allow for timely corrective actions formal event reporting and escalation procedures should be in place.

Establishment of formal procedures
Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents. Procedures should be established that cover amongst others:
– Handling of denial of service attack, viruses, worms, attack and other cyber incidents;
– Information systems failures and loss of services, and when to activate the institution's disaster recovery plan;
– Breaches of confidentiality and integrity;
– Misuse of information systems;
– Containment of forensic evidence; and

– Communication with those affected by or involved with the incident.

Actions to recover from security breaches and to correct system failures should be carefully and formally controlled to ensure that:
– Only clearly identified and authorized personnel are allowed to access production systems and data;
– All emergency actions taken are documented in detail; and
– Emergency actions are reported to management and completed in an orderly manner (based on the change management procedures).

Root cause analysis
Security incidents should be analyzed in order to identify the root causes of the incident. Only if the root cause of an incident is identified, effective corrective actions can be outlined to prevent the reoccurrence of the problem or event in the future.
In addition, the supervised institution should check if new threats or vulnerabilities have occurred in order to enhance the threat or vulnerabilities list of the risk assessment process. This can help to safeguard other information assets when performing risk assessments.
Furthermore, the information security awareness training can benefit from live examples of the organization to create a better understanding of security issues to personnel.

Security incident database[14]
Data about past incidents should be collected and stored for at least 5 years. Supervised institution should have mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored. The evaluation of security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrence (see also paragraph 2.5).

Principle 6.
Supervised institutions should protect the privacy of customer information

Controls to protect the privacy of customer information should be part of the ISM framework.

To meet the expectations regarding the privacy of customer information, supervised institutions should comply with existing applicable laws and regulations.

Furthermore, supervised institutions should at least:
1. Ensure the security and confidentiality of customer records and information;
2. Protect customers against any anticipated threats or hazards to the security or integrity of such records; and
3. Protect customers against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. As to the latter,

[14] See also the "CBCS Beleidsregel integere bedrijfsvoering bij incidenten en integriteitgevoelige functies" §3.2. Point 3 d) on page 4

customer information may not be sold to or shared with others[15] and may only be used for the purpose for which the data was originally recorded.

Principle 7.
Supervised institutions should provide information security training

Periodical information security training should be part of the ISM framework.

Personnel with specific information security tasks should be trained to become competent to perform such tasks.

A training that should be offered to all internal and long term[16] third party contractors is the security awareness training. The program should be updated and repeated at least every three years. New personnel should get this training within six months after employment.

The training program should include, but is not limited to:
- Explanation of the institution's information security policy, standards and procedures;
- Familiarization with their roles, accountabilities and responsibilities regarding information security;
- Explanation of current threats (e.g. phishing, viruses, worms, spyware, shoulder surfing, social engineering, piggy backing);
- Clean desk policy;
- Responding to an emergency situation;
- Significance of logical access in an IT environment; and
- Privacy and confidentiality requirements.

Principle 8.
Supervised Institutions should ensure the quality of all aspects of ISM by assessing independent audits

The planning and execution of audits should be part of the ISM framework.

Audits should provide independent, objective assurance and consulting service designed to add value and improve the institution's ISM Framework.

The auditor should review if the ISM Framework and plans are adequate and effective, and if the institution operates accordingly in a manner to ensure that:
- The institution's information security strategy is executed and in accordance with business requirements and applicable laws and regulations;
- There is a collective understanding of the institution's threat, vulnerability and risk profile;
- Risks are appropriately identified and managed;

15 E.g. selling customer e-mail addresses to a marketing company
16 Six month or longer

- Interactions with the various stakeholders occur as needed;
- Significant financial, managerial, and operating information is accurate, reliable and timely;
- Security practices are standardized;
- Policies, standards and procedures are continuously updated;
- Employees' actions are in compliance with policies, standards and procedures and tested for effectiveness;
- Security roles have sufficient and competent back-up staffing;
- 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 ISM 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 supervised institution's nature, size, scope of operations and the complexity of its business.

APPENDIX 1
Glossary/Definitions

Application controls	Application controls refer to transaction processing controls, sometimes called "input-processing-output" controls, specifically designed to ensure that integrity, confidentiality and business objectives are met.
Availability	Ensuring timely and reliable access to information sources.
Confidentiality	Preventing disclosure of information to unauthorized individuals or systems.
Four eyes principle	A control mechanism designed to achieve a high level of security for critical operations. Under this rule all access or actions requires the presence of two authorized people at all times.
Hardening (hardened systems)	The process of securing a system by reducing its surface of vulnerability such as: – Stopping/removing unnecessary software and services or closing down unnecessary ports of a firewall; – Installing necessary patches; – Deploying the latest versions of applications; – Implement least privilege principle rule; and – Using standardize configurations.
Information assets	Refers to all the infrastructural, organizational, technical components, data, documents and personnel, which assist in information processing.

Information Security Management Framework	A framework that defines the technical, operational, administrative and managerial components of ISM; the organizational units and leadership responsible for each component; the control or management objective that each component should deliver; the interfaces and information flow between components; and each component's tangible outputs.
Information processing facility	The computer room and support areas.
Integrity	The assurance that data is consistent, correct, not manipulated, and includes ensuring information on non-repudiation and authenticity.
Key Goal Indicator	Helps an organization define and measure progress toward organizational goals. Once an organization has analyzed its mission, identified all its stakeholders, and defined its goals, it needs a way to measure progress toward those goals. Key goal indicators are a measure of "what" has to be accomplished.
Key Performance Indicator	Key Performance Indicators are measures that tell management that an IT process is achieving its business requirements by monitoring the performance of that IT process. It is a measure of "how well" the process is performing.
Least privilege principle	Providing users only access to information or authorization to perform certain functions, which are absolutely essential to do his/her work.
Malware	Short for malicious software is software designed to infiltrate a computer system without the owner's informed consent.
Patch management	A patch is a piece of software designed to fix problems. Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.
Penetration testing	A simulation of a hacking attack on the organization's network to discover any potential vulnerabilities, which may result from poor or improper system configuration, known and/or unknown hardware or software flaws.
Piggy backing	When an authorized person allows (intentionally or unintentionally) others to pass through a secure door.
Phishing	Refers to the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

Standard builds	Standard builds allow one documented configuration to be applied to multiple devices in a controlled manner.
Shoulder surfing	Refers to using direct observation techniques, such as looking over someone's shoulder or placing a camera, to get information.
Social engineering	Refers to the act of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical hacking techniques.
Spyware	Refers to a type of malware that is installed on computers and that collects little bits information at a time about users without their knowledge.
Virus	A computer program that can copy itself and infect a computer.
Vulnerability scanner	A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications to identify weaknesses.
Worm	Refers to a self-replicating computer program. It uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention.

APPENDIX 2
Links to helpful websites

Organization	Website
FFIEC	http://ithandbook.ffiec.gov/it-booklets/information-security.aspx (Information Security Booklet)
ISACA	www.isaca.org/cobit.htm (Cobit)
ISO	http://www.27000.org/ (Information Security) http://www.iso.org/iso/catalogue detail?csnumber=43170 (Risk Management)
NIST	www.nist.gov http://csrc.nist.gov/index.html http://csrc.nist.gov/publications/PubsSPs.html (Special security publications)
SABSA	http://www.sabsa.org/the-sabsa-method.aspx
OGC	www.prince2.com/ (Prince2)
PMI	http://www.pmi.org/ (PMBok)
Octave	http://www.cert.org/octave/

Relevant Certification for Information Security Management

ISACA	www.isaca.org/cisa
	www.isaca.org/cism
ISC2	www.isc2.org/cissp

APPENDIX 3
SMART Metrics

Specific

A metric should be well defined. To set a specific metric one can use the six "W" questions:

*Who:	Who is involved?
*What:	What do we want to accomplish?
*Where:	Identify the location.
*When:	Establish a time frame.
*Which:	Identify requirements and constraints.
*Why:	Specific reasons, purpose or benefits of this metric.

Measurable

Metrics need to be formalized describing:

- Name of the metric;
- Description of what is measured and why;
- Stakeholders (Information collector, owner, customer)
- How is the metric measured;
- How often measurement takes place;
- Range of values considered normal for the metric (threshold);
- Best possible value for the metric; and
- Units of measurement.

Agreed upon

A metric should be agreed upon by all the stakeholders.

Realistic

Within the availability of resources, knowledge and time.

TImely

For KGI's specific target levels and timelines should be set. E.g. Phase Y of project X needs to be accomplished on Date Z using Q amount of resources delivering A,B,C deliverables. For KPI's the time frame should be defined to measure performance. E.g. Within one year we want 100% up time for all critical systems.

A good reference document is the NIST publication SP 800-55 http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

Provisions and Guidelines for Safe and Sound Electronic Banking

CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

I. Introduction

In its continuous effort to promote and ensure safe and sound banking practices on the islands of Curacao and Sint Maarten, the Centrale Bank van Curacao en Sint Maarten ("the Bank") hereby issues the "**Provisions and Guidelines for Safe and Sound Electronic Banking"(hereafter "Provisions and Guidelines**").

Ongoing innovations in information technology and competition among banking institutions, new market entrants, and mergers and acquisitions have contributed worldwide to a wider array of electronic banking ("hereinafter e-banking") products and services. The islands of Curacao and Sint Maarten have also experienced this development amongst its credit institutions, and the acceptance of e-banking services has grown rapidly.

E-banking carries benefits as well as risks to credit institutions. Because the characteristics of e-banking increase and modify banking risks and thereby influence the overall risk profile of banking, the Bank finds it important that these risks be recognized, addressed, and managed by the relevant credit institutions in a prudent manner.

Worldwide fraud, identity theft, money laundering, and terrorist financing also frequently are incline to move to countries where credit institutions provide e-banking products and services and which have inadequate risk management regarding e-banking. Therefore, the Bank recommends that credit institutions adopt relevant policies and stronger risk management including internal control to prevent these kinds of immoral activities.

These Provisions and Guidelines provide credit institutions, which are subject to the Bank's supervision, with guidance on the general principles for risk management of e-banking[1] and outline suggestions for consumer security and education. The Provisions and Guidelines should help credit institutions to expand their risk oversight policies and processes to cover their e-banking activities.

The "Provisions and Guidelines" are particularly derived from the principles and recommendations for e-banking outlined by the Basel Committee on Banking Supervisions ("The Basel Committee"), in the papers: "*Risk Management Principles for E-banking*" *and "Management and Supervision of Cross-Border E-banking Activities*"[2] issued in July 2003.

---

[1] See appendix 1 for definition.

[2] http://www.bis.org/publ/bcbs98.htm and http://www.bis.org/publ/bcbs99.htm

The Bank encourages credit institutions to read and understand the principles set forth in the abovementioned documents and to continuously monitor updated publications related to e-banking activities posted on among other places on The Basel Committee's website[3].

II. Legal base and scope

These Provisions and Guidelines 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).

The Provisions and Guidelines apply to all credit institutions that conduct e-banking activities in and/or from the islands of Curaçao and Sint Maarten and are licensed pursuant to the aforementioned National Ordinance. These institutions are hereafter referred to as "credit institutions".

III. Implementation

To ensure a high standard of e-banking risk management on the islands of Curacao and Sint Maarten, credit institutions are required to have implemented the "**Provisions and Guidelines for Safe and Sound Electronic Banking**" by the end of 2007.

The Bank recognizes that each credit institution's risk profile is different and will require:

1. a risk mitigation approach appropriate for the scale of the e-banking operations;
2. the materiality of the risk present; and
3. the true ability of the credit institution to manage these risks.

These differences imply that the risk management principles and recommendations presented and referred to in these Provisions and Guidelines are intended to be flexible enough to be implemented. However, each credit institution is required to implement a minimum of risk mitigating counter measures. The minimum required measures are stated in chapters VII, VIII, IX and X.

The Bank will verify the implementation of the Provisions and Guidelines during its offsite and onsite supervisions. Based on these examinations and its offsite reviews, the Bank will determine the adequacy of the credit institutions' risk management of e-banking. The Bank also may implement other monitoring processes to facilitate its ongoing supervision of e-banking.

IV. Supervisory approach

The Bank's supervisory objective is to establish and maintain a safe and sound environment for the development of e-banking activities in and/or from the islands of Curaçao and Sint Maarten.

[3] http://www.bis.org/

The general principle is that credit institutions are expected to implement the relevant risk management controls that are "fit for purpose", i.e., commensurate with the risks associated with the types, complexity, and amounts of transactions allowed, the electronic delivery channels adopted, and the risk management systems of individual credit institutions.

In developing these Provisions and Guidelines, the Bank has considered the supervisory approach and guidance by the Basel Committee in particular and those of other regulatory communities. The Bank emphasizes that these Provisions and Guidelines are not intended to prescribe uniform or all-inclusive principles and practices in managing the risks for all kinds of e-banking activities. The minimum required measures are stated in chapters VII, VIII, IX and X.

Credit institutions should take into account all relevant laws and provisions, policies, and guidelines issued by the Bank. They include but are not limited to:
- The National Ordinance on Identification of Clients when rendering Financial Services (N.G. 1996, no.23);
- The National Ordinance on Reporting of Unusual Transactions (NG.1996, no21);
- National Ordinance on Foreign Exchange Traffic (N.G. 1981, no.67);
- The BNA Corporate Governance Summary of Best Practice Guidelines;
- The BNA Provisions and Guidelines regarding Detection and Deterrence of Money Laundering and Terrorist Financing for Credit Institutions; and
- The BNA Policy rule for Sound Business Operations in the Event of Incidents and Integrity-Sensitive Positions.

The Bank may prescribe new rules and regulations to administer and carry out the purposes of this regulation, including rules and regulations to define or further define terms used in this regulation and to establish limits ore requirements other than those specified in this regulation.
The Bank reserves the right, in individual cases of (partially) non-compliance, to impose conditions or initiate consultations on a limitation of the e-banking activities.

V. Risk Management

The Board of Supervisory Directors (hereafter "the Supervisory Board") and senior management of credit institutions are responsible for managing the institution's risks. Its risk profile will become more complex if the institution provides e-banking transactions. Therefore, the Supervisory Board and senior management should be well involved in the development of the institution's e-banking business strategy and ensure that the risk characteristics are fully understood and operational and that security dimensions of the electronic activities are appropriately considered and addressed.

To mitigate the risks associated with all e-banking activities, credit institutions should have in place a comprehensive risk management process that assesses risks, controls risk exposure, and monitors risks. This comprehensive risk management framework should be integrated into the credit institutions' overall risk management framework. The risk management process should be supported by appropriate oversight by the Supervisory Board

and senior management or its designated committee. The process should be carried out by adequate staff with the necessary knowledge and skills to deal with the technical complexities of e-banking. As a result, the applicable risk management policies and processes and the relevant internal controls and audits should be enforced as required in the credit institutions risk management systems, and carried out as appropriate for the credit institution's e-banking services.

Credit institutions should implement at least the minimum required risk mitigating countermeasures as stated in chapters VII, VIII, IX, and X. However, to achieve a comprehensive risk management control regarding e-banking services, credit institutions should always take into account the 14 risk managementprinciples"or e-banking activities4 outlined by the Basel Committee.

These Provisions and Guidelines focus on the risks and risk management techniques associated with internet delivery channels. The principles are applicable to all forms of e-banking activities.

VI. E-banking related risks

E-banking does not open up new risk categories, but rather increases and modifies existing risks and creates new risk management challenges. Because of rapid changes in information technology, no description of such risk categories can be exhaustive. However, the Bank has identified below a number of risks specifically associated with e-banking for bank supervision purposes. The board of supervisory directors and senior management must recognize these risks and should ensure that the risk management controls and systems have been reviewed and modified where necessary to address specific risk management challenges associated with e-banking.

Strategic risk

This is the current and prospective risk arising from amongst other things, from adverse business decisions or improper implementation of decisions. Senior management must fully understand the strategic and technical aspects of e-banking. Spurred by competitive and peer pressures, credit institutions may seek to introduce or expand e-banking activities without an adequate cost-benefit analysis. In managing the strategic risk associated with e-banking services, credit institutions should develop clearly defined e-banking objectives by which the institution can evaluate the success of its e-banking strategy.

Transaction/operations risk

This is the current and prospective risk arising from among other things fraud, processing errors, systems descriptions negligence, and the inability to maintain expected service levels. It includes failure of communications, breakdown of data transport or processing, internal control system deficiencies, and management failure. Offering innovative services that have not been standardized increases the complexity of an institution's activities and the quantity

[4] The 14 risk management principles and recommendations for e-banking activities are explained in the document "Risk Management Principles for E-banking" available at: http://www.bis.org/publ/bcbs98.htm

of this risk. A high level of transaction/operations risk may exist with e-banking products, because of the need to have sophisticated internal controls and constant availability. The level of transaction/operations risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology. Credit institutions should make certain that customers who transact on the internet cannot later deny having originated the transactions. Third-party providers also increase transaction/operations risks, since the credit institutions do not have full control over a third party. Without seamless process and system connections between the bank and the third party, there is a higher risk of transaction errors. The key to controlling transaction/operations risk lies in adapting effective policies, procedures, and controls to meet the risk exposures introduced by e-banking. Basic internal controls such as segregation of duties and dual controls remain important. Credit institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level.

Compliance/legal risk
This is the failure to comply with statutory or regulatory obligations or contractual agreements such as laws, rules and regulations and the violation of ethical standards. Compliance/legal risk may lead to diminished reputation, reduced business opportunities, and actual monetary losses. Conflicting laws, tax procedures, and reporting requirements across different jurisdictions add to the risk. The need is to keep customer data private and to seek customers' consent before sharing the data, unless allowed otherwise by law, such as the reporting to the FIU/MOT (Meldpunt Ongebruikelijke Transacties). FIU also adds to compliance/legal risk. Credit institutions need to understand and interpret existing laws, regulations, and ethical standards that apply to e-banking and ensure consistency with other channels such as branch banking.

Reputation risk
This is the current and prospective risk arising from negative publicity regarding the credit institution's business. A bank's reputation can be damaged by e-banking services that are poorly executed (e.g., limited availability, buggy software, poor response, the use of inadequate point of sale devices). To meet customers' expectations, credit institutions should have effective capacity, business continuity, and contingency planning. Credit institutions should also develop appropriate incident response plans, including communication strategies, which ensure business continuity, control reputation risk, and limit liability associated with disruptions in their e-banking services.

Information security risk
Information security includes protecting information and/or information systems from unauthorized access, use, disclosure, disruption, modification, or destruction, to provide integrity, confidentiality, and availability. Information security risk arises out of lax information security processes', and may expose the institution to malicious hacker or insider attacks, viruses, denial-of-service attacks, data theft, data destruction and fraud. The speed

of change of technology and the universal accessibility of the internet channel makes this risk especially critical.

Contingency/technological risk
Contingency/technological risks are risks related to any adverse outcome, damage, loss, disruption, violation, irregularity, or failure arising from the use of or reliance on computer hardware, software, electronic devices, and online networks and telecommunications systems. These risks can also be associated with among other things application security, systems failures, processing errors, software defects, operating mistakes, hardware breakdowns, capacity inadequacies, network vulnerabilities, control weaknesses, security shortcomings, malicious attacks, hacking incidents, fraudulent actions, and inadequate recovery capabilities.

VII. Risk mitigating counter measures
The risk management controls and policies related to e-banking should cover, at a minimum, the following risk mitigating countermeasures:

Authentication of customers
Credit institutions should select reliable and effective authentication techniques to validate the identity and authority of their e-banking customers. Single-factor authentication[5], as the only control mechanism, is insufficient and not accepted by the Bank for transactions involving access to customer information or the movement of funds to other parties. Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods. Consequently, multifactor authentication[6] methods (such as two-factor authentication[7]) are more reliable and provide stronger assurance in authentication. Credit institutions should ensure that customers are verified and their identities established before conducting business over the internet. Password generating devices, biometric methods, challenge-response systems, and public key infrastructure are some ways of strengthening the authentication process, as indicated in our letter of July 27, 2006, with reference CE/nl/2006-10.581.

Current examples of the proper use of multi-factor authentication are:
- Internet banking websites using a user id and password in combination with a token device to connect to the on-line banking application;
- POS at the supermarket requires an ATM card and a pin code for access and authentication before completing a transaction; and
- ATM machines require an ATM card and a pin code for access and authentication before collecting money from the ATM machine.

5 Single-factor authentication involves the use of one factor to verify customer identity, namely user id and password.
6 Multifactor authentication utilizes two or more factors to verify customer identity.
7 Two-factor authentication involves the use of two factors, e.g., a password-generating device along with the user id/password, ATM card and pin code, user id/password and token device.

Current examples of the improper use of access and authentication are:
– Internet banking websites using only a user id and password to connect to the online banking application; and
– POS machines at gasoline stations allowing only an ATM card input to complete a transaction to fill up the fuel tank.

Credit institutions are required to use multi-factor authentication for internet banking:
– When the user logs on to the banking system; and
– When the user wants to make a transaction.

Confidentiality and integrity of information
E-banking services entail transmission of sensitive information over the internet and credit institution's internal networks. Therefore, credit institutions should therefore implement appropriate technologies to maintain confidentiality and integrity of sensitive information while it is being transmitted over the internal and external networks and also when it is stored inside database systems. The use of cryptographic technologies is required to protect the confidentiality of sensitive information. Credit institutions should choose cryptographic technologies appropriate to the sensitivity and importance of information and the extent of protection needed. They must ensure that all intelligent electronic devices that capture information do not expose/store information such as the PIN number or other information classified as confidential and must also ensure that a customer's PIN number cannot be printed for any reason whatsoever. In addition, credit institutions must provide safe- to- use intelligent electronic devices and ensure that customers are able to make safe use of these devises at all times.

Application security
Inadequate application security in e-banking systems increases the risk of intruders exploiting the system. Credit institutions should ensure an appropriate level of application security in their e-banking systems. When credit institutions select system development tools or programming languages for developing e-banking application systems, they should evaluate the security features that can be provided by different tools or languages to ensure that effective application security can be implemented. In the case of selecting an e-banking system developed by a third party, credit institutions should take into account the appropriateness of the application security of the system. Credit institutions are required to test new or enhanced applications thoroughly using a general accepted test methodology in a test environment.

E-Banking applications should protect against common techniques that fraudsters use to break into the credit institution's server by misleading its application.
E.g.:
– SQL injection;
– cookie poisoning/tempering;
– cross site scripting; and
– entering programming code into fields that lack input validation.

Credit institutions should make reasonable effort to ensure non-repudiation of e-banking transactions using strong authentication mechanisms and application security.

Internet infrastructure and security monitoring
Credit institutions should establish an appropriate operating environment that supports and protects their e-banking systems. Credit institutions should proactively monitor their e-banking systems and internet infrastructure on an ongoing basis to detect and record any security breaches, suspected intrusions, or weaknesses. Credit institutions should ensure that adequate controls are in place to detect and protect against unauthorized access to all critical e-banking systems, servers, databases, and applications.

This includes, but is not limited by:
- A formal[8] information security policy;
- A formal server security policy;
- A formal physical security policy;
- A formal disaster recovery plan;
- A formal backup and recovery procedure;
- A formal change management procedure;
- A formal patch management procedure;
- A formal security monitoring procedure;
- A formal virus update procedure;
- Placement of external accessible servers placed in a De-militarized zone (DMZ); and
- Protecting critical hosts with intrusion detection systems.

Outsourcing
Credit institutions may rely on an outside service provider to operate and maintain IT systems or business processes that support their e-banking services. In such cases, credit institutions should exercise appropriate due diligence in evaluating their reputation, credit status, and viability. Credit institutions must ensure that the service providers and vendors can perform as promised and that they are capable of keeping abreast of new or changing technology. When contracting for e-banking services, credit institutions must carefully consider how they intend to use third parties to design, implement, and support all or part of their e-banking systems. A credit institution's contracts with technology providers should ensure that the provided activities match applicable legal and policy standards. Credit institutions should maintain control through a Service Level Agreement over the services and products provided by third parties and ensure that the outsourced service is subject to independent assessment and the customer data are kept confidential.

A global development is buying through telephone services. Credit institutions rely on the telecommunication businesses (e.g., UTS) to handle part of the transaction between the retail business and the credit institution or the consumer and the credit institution. Credit

[8] Formal means "in writing and approved by management"

institutions are responsible for adequately controlling these new types of payment services and should take into account abovementioned risk mitigating countermeasures.

Internet banking
Credit institutions should put in place procedures for maintaining the credit institution's web site, which should ensure at least the following:

1. Only authorized staff should be allowed to update or change information on the web site;
2. Updates of critical information (e.g., interest rates) should be subject to dual verification;
3. Web site information and links to other websites should be verified for accuracy and functionality;
4. Management should implement procedures to verify the accuracy and content of any financial planning software, calculators, and other interactive programs available to customers on an internet websites or other e-banking service;
5. Links to external web sites should include a disclaimer that the customer is leaving the financial institution's site and provide appropriate disclosures, such as noting the extent, if any, of the bank's liability for transactions or information provided at other sites;
6. Credit institutions must ensure that the Internet Service Provider (ISP) has implemented a firewall to protect the financial institution's website where outsourced;
7. Credit institutions should ensure that installed firewalls are properly configured and institute procedures for continued monitoring and maintenance arrangements are in place; and
8. Credit institutions should ensure that summary-level reports showing website usage, transaction volume, system problem logs, and transaction exception reports are made available to the institution by the web administrator.

VIII. Internal control

The risk management controls and policies related to e-banking should also cover, at a minimum, the following risk mitigating countermeasures:

Segregation of duties
As in any traditional process, segregation of duties is a basic internal control measure designed to reduce the risk of fraud in operational processes and systems. The credit institution's management must identify and mitigate areas where conflicting duties create the opportunity for insiders to commit fraud. Credit institutions should ensure that appropriate measures are taken to protect the data integrity of e-banking transactions, records, and information. No one employee should be able to process a transaction from start to finish.

Recordkeeping
All e-banking transactions should generate clear audit trails, which should be archived and kept for 10 years. ATM video surveillance recordings should be archived for at least one year. It is also vital to generate and protect records of customer instructions in a legally acceptable format. Credit institutions should strengthen information security controls to preserve the confidentiality and integrity of customer data. Firewalls, ethical hacking tests,

physical and logical access controls are some of the methods available. Recordkeeping requirements should be based upon the level of activity and risk.

Dual controls
Some sensitive transactions necessitate making more than one employee approve the transaction before authorizing the transaction. Large electronic funds transfers or accesses to encryption keys are examples of two e-banking activities that should warrant dual controls.

Reconcilements
E-banking systems should provide sufficient accounting reports to allow employees to reconcile individual transactions to daily transaction totals.

Monitor suspicious activity
Credit institutions should establish fraud detection controls that could prompt additional checking of suspicious activity. Some potential concerns to consider include false or erroneous application information, large check deposits on new e-banking accounts, unusual volume or size of funds transfers, multiple new accounts with similar account information or originating from the same internet address, and unusual account activity initiated from a foreign internet address.

Incident response
Credit institutions should put in place formal incident response and management procedures for timely reporting and handling of suspected or actual security breaches, fraud, or service interruptions of their e-banking services. The incident response and management procedures should allow credit institutions to quickly identify the origin of the weakness and contain the damage and assess the potential scale and impact of the incident. Credit institutions should also identify and notify affected customers and collect and preserve forensic evidence as appropriate to facilitate the subsequent investigation and potential prosecution of suspects and intruders. Furthermore, the incident response procedures should include strategies for dealing with adverse media and customer reactions in a timely way. In the event of an incident as described above, the credit institutions should notify the Bank immediately.

Error checks
E-banking activities provide limited opportunities for customers to ask questions or clarify their intentions regarding a specific transaction. Institutions can reduce customer confusion and the potential for unintended transactions by requiring written contracts explaining rights and responsibilities, by providing clear disclosures and on-line instructions or help functions, and by incorporating proactive confirmations into the transaction initiation process. On-line instructions help features and proactive confirmations are typically part of the basic design of an e-banking system and should be evaluated as part of the initial due diligence process. On-line forms can include error checks to identify common mistakes in various fields. Proactive confirmations can require customers to confirm their actions before the transaction is accepted for processing. For example, a bill payment customer would enter the amount and date of payment and specify the intended recipient. But, before ac-

cepting the customer's instructions for processing, the system might require the customer to review the instructions entered and then confirm the instruction's accuracy by clicking on a specific box or link.

Alternate channel confirmations
Credit institutions should consider the need to have customers confirm sensitive transactions like enrollment in a new on-line service, large funds transfers, account maintenance changes, or suspicious account activity. Positive confirmations, or sensitive on-line transactions provide the customer with the opportunity to help catch fraudulent activity. Financial institutions can encourage customer participation in fraud detection and increase customer confidence by sending confirmations of certain high-risk activities through additional communication channels such as the telephone, e-mail, or traditional mail.

Customer data protection
Misuse or unauthorized disclosure of confidential customer data may expose a financial institution to customer litigation. The general requirements and controls that apply to paper-based transactions also apply to electronic financial services. To meet expectations regarding the privacy of customer information, credit institutions should ensure that their privacy policies and standards comply with existing applicable regulations.

Furthermore, credit institutions should at least:
1. ensure the security and confidentiality of customer records and information;
2. protect customers against any anticipated threats or hazards to the security or integrity of such records; and
3. protect customers against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

IX. Cross-border e-banking activities

Before engaging in cross-border e-banking transactions, credit institutions should ensure that adequate information is disclosed on their websites to allow potential customers to make a determination of the credit institution's identity, home country, and whether it has the relevant regulatory license(s) before they establish the business relationship. This information will improve transparency and minimize legal and reputation risk associated with cross-border e-banking activities. By engaging in cross-border e-banking activities, credit institutions should ensure that they are complying with the Provisions and Guidelines regarding Detection and Deterrence of Money Laundering and Terrorist Financing and Foreign Exchange Regulations.

To achieve a comprehensive risk management control policy for cross-border e-banking, credit institutions should, in addition to implementing the 14 risk management principles for e-banking activities, also implement, where necessary, the 2 principles and recommendations for cross-border e-banking activities[9] outlined by the Basel Committee.

[9] The principles and recommendations for cross-border e-banking activities can be found on the BIS website at http://www.bis.org/publ/bcbs99.htm

X. Customer security, education, and transparency

An important aspect of customer security and risk management is customer education. Therefore, credit institutions should pay special attention to the provision of easy-to-understand and prominent advice to their customers on e-banking security precautions.

At a minimum security precautionary advice for customers should cover the following issues:

- Password and user ID selection and protection, e.g., not to select passwords incorporating such info as birthday and to avoid using the same password for accessing other online services;
- Not to disclose their personal information to unauthorized persons or to any doubtful websites;
- Never to write down their PIN number;
- To cover their hands when typing at POS systems;
- To be aware of phishing e-mails; and
- To ensure that their pc's are securely configured and adequately protected from malicious programs and viruses, e.g., regularly updating their anti-virus software.

Credit institutions should use effective methods and channels to communicate with customers on security precautions. Such channels can include websites and messages printed on customer statements.

Fee disclosure

Automated Teller Machine (ATM) and Point of Sale (POS) operators who impose a fee on consumer for providing host transfer services should notify the consumer in advance that a fee is imposed for providing the service and the amount of any such fee.

The notification should be placed in a prominent and conspicuous location on or at the ATM and/or the POS where the consumer initiates the electronic fund transfer.

APPENDIX 1
Glossary/Definitions

Authentication

The techniques, procedures, and processes used to verify the identity and authorization of prospective and established customers.

Board of Supervisory Directors

The governing body of an institution, elected by the shareholders, to oversee and supervise the management of the institution's resources and activities. This body is ultimately responsible for the conduct of the institution's affairs, and controlling its direction and, hence, it's overall policy.

Cross-border e-banking activities

The provision of transactional on-line banking products or services by a bank in one country to residents of another country.

E-banking
The automated delivery of new and traditional banking products and services directly to customers through electronic and interactive communication channels. E-banking includes the set up, maintenance, internal control, and other aspects of the systems that will enable credit institution customers and/or other persons to access accounts, transact business, or obtain information on financial products and services through the above channels and a private or public network, including the internet. Customers access e-banking services using an intelligent electronic device, such as a personal computer (PC), personal digital assistant (PDA), automated teller machine (ATM), point of sale devices (POS), Kiosk, or Touch Tone telephone.

Identification
The procedures, techniques, and processes used to establish the identity of a customer when opening an account.

Meldpunt Ongebruikelijke Transacties (MOT/FIU)
Pursuant to article 11 of the National Ordinance on the reporting of Unusual Transactions (N.G. 1996, no. 21), any (legal) person who provides a financial service is obliged to inform the MOT "Meldpunt Ongebruikelijke Transacties" of an unusual transaction that is contemplated or has taken place.

Risk management
The ongoing process of identifying, measuring, monitoring, and managing potential risk exposures.

Senior management
Comprises the individuals entrusted with the daily management of the operations to achieve the institution's objectives.

Policy Memorandum: Management of Computer Risks

CENTRALE BANK VAN CURACAO EN SINT MAARTEN
(Central Bank)

I. Introduction

The application of computer and telecommunication technology is currently a wide-spread phenomenon in the financial industry. The trend towards increasing automation is likely to continue for many years. The success of an organization will thus depend to a considerable degree on the quality of its computer and telecommunication systems, and the extent to which it develops these systems to match the evolving needs of its business and its customers. Deficiencies in security and control procedures within those systems can pose a significant threat to the continuity of operations.

The purpose of this memorandum is to provide Senior Management with a firm basis for an evaluation of the risks inherent to the use of computer technology and to increase Senior Management's awareness of the general control elements that may be effective in safeguarding the institution's operations against such risks. The memorandum is also an aid to identify the automation related risks that threaten the effectiveness and continuity of an institution's operations and in understanding their potential consequences, which might be as extreme as prolonged closure.

This memorandum is not aimed at addressing all the detailed questions that are relevant to computer security and control in every installation, and so will not necessarily identify all vulnerabilities which may exist. The subject is technically complex and in each institution there are considerable variations in vulnerabilities and control techniques among different types of systems and equipment. Use of the memorandum cannot replace a detailed review by a computer security audit specialist, whether in house or external. However, by focusing on those controls which can make the greatest contribution to protecting operations, the memorandum provides a firm basis for a global evaluation of the computer security and control procedures in the electronic data processing environment of an institution.

Viewing the contents of this Memorandum one notes that a general introduction to the nature of business risks resulting from the use of computer and telecommunication systems is being presented in a policy framework. It describes the types of control which can be used to minimize potential risks and to ensure that systems are reliable and meet the needs of their business.

Throughout this memorandum, the term "institution" is frequently used as a shorthand for supervised institutions, and the general term "computer" for computer, microcomputer or telecommunication systems, including the applications being used.

II. Managing Computer Risks to Banking Operations

The successful management of computer and telecommunication risks requires effective mechanisms for identifying risks and assessing their consequences. Security and control procedures should then be compared and evaluated in terms of cost and the extent to which they reduce the risks of serious loss arising from inadequacies or failures in the computer systems.

In certain cases it may be possible that certain procedures which are appropriate for a large institution with substantial numbers of data processing staff are inappropriate for a small institution. In general, however, the nature of computer and telecommunication risks is very similar in both large and small organizations and effective security and control procedures are necessary in both cases.

In section III we will address the nature of computer risks and identify five (5) categories of computer risks that may pose significant threats for the institutions if left uncovered.

In order to protect the institution against undue risks, certain controls are described in section IV of this memorandum. These control measures represent a general framework of controls that must be in place to provide protection against computer risks.

III. Nature of Computer Risks

All institutions are exposed to losses resulting from errors and fraud. While it is arguable whether computers have changed the types of risks which exist, it is clear that they have changed the scale of those risks and the ways in which they can arise, as well as the types of security and control procedures necessary to contain those risks to acceptable levels.

This memorandum addresses the following areas which are related to certain types of risks:

1. Development risks;
2. Risk of errors;
3. Risk of business interruption;
4. Risk of unauthorized disclosure of confidential information and
5. Risk of fraud.

III-1 Development risks

Efficiency and quality of services are nowadays so dependent on computer systems that any failure in planning, controlling or developing new systems may have significant commercial consequences.

Major delays in implementing key systems may place an institution at a serious disadvantage in its competitive environment. Failure to anticipate advances made by competitors in their use of technology may lead to inappropriate systems being developed or to operational systems becoming economically obsolete.

The following aspects of computer development require particularly close attention by senior management: long term (strategic) planning of computer systems and equipment, feasibility studies, specification of system requirements, selection of equipment and software

suppliers and project control by those in charge with implementation of computer projects (costs, duration and quality). Lack of attention to one or more of these aspects can lead to serious development delays, increased costs, failures of computer projects or inadequate operation of implemented systems.

It is important that all security and control requirements in a new system are immediately taken into consideration when the system is being specified and designed. Otherwise, new systems may be unreliable from the outset. Internal inspection and audit departments can often make a significant contribution in achieving good controls if they are consulted sufficiently early in the systems design process.

Those institutions which do not employ inspection or audit staff with the appropriate skills may find that their external auditors or outside consultants can assist. However, even in these cases proper awareness of the above mentioned aspects of computer development continues to be required for Senior Management.

III-2 Risk of errors

Errors can arise in a variety of ways and can affect customer service, operational efficiency and management and supervisory control. These errors frequently occur during the entry of data by terminal operators and during the development and amendment of computer programs. Significant errors can also occur, however, during the systems design process, during routine system maintenance procedures and when using special programs to correct errors. The cause is usually human failure. It is relatively rare for failure in electronic or mechanical components to be the cause of errors in computer data.

The complexity of computer systems may contribute significantly to the occurrence of errors. Most computer programs contain so many instructions that it is impracticable to test every logical path through them. Even when programs are well tested, errors can remain that may lie dormant for months or years until a particular set of circumstances occurs. When this happens, the results can be unpredictable. Often new errors are introduced during successive system changes.

Errors may also be introduced into standard software packages when these are "customized" i.e. tailored to meet the needs of a particular institution or user. This may pose a significant problem, which may grow as maintenance is carried out. When purchasing standard software packages the aim should therefore be to keep the number of changes to a minimum.

Based on the above, institutions are required to maintain good standards of error control in order to maintain accurate transaction balances and management information. Senior Management must at least be aware of the measures taken by operational management and staff to control the occurrence of errors.

III-3 Risk of business Interruption

Nowadays, once computers have been introduced few institutions can continue to operate for long without their computer systems. Computer systems consist of large numbers of

individual equipment and software components, which may bring down the system if they fail. In most organizations, a considerable proportion of these components are centered in one place. Computer systems are therefore particularly vulnerable to breakdown, accidents and malicious damage.

Once the systems are out of function, the damaging effects on services, particularly for those institutions using on-line real-time systems, can increase rapidly. In some banks for instance, customers may be affected immediately as links to automated teller machines (ATM's) or other electronic networks fail. Processing backlogs develop quickly and, after a breakdown lasting several hours, these may take days to clear if there is insufficient processing capacity to cope with the additional load.

If its systems are out of action for several days or more, an institution may have to suspend its business unless adequate contingency plans have been specified and tested beforehand. The consequential costs of a serious system failure, therefore, can far exceed the costs of replacing damaged equipment, data or software.

The particular importance of protecting an institution's software and data should be kept in mind by Senior Management at all times. Equipment can eventually be replaced, but if, in an accident, all copies of programs and data were to be destroyed, considerable time might elapse before normal operations could be resumed. Total destruction of unique software could require substantial efforts to replace. Similarly, loss of copies of data may cause severe disruption for a considerable period. At worst, a total loss of data or software could cause the prolonged closure of the institution. This event could occur if inadequate steps had been taken to protect the software and data against fire, other calamities or malicious damage.

Institutions must therefore protect their computer resources effectively against physical threats and have adequate backup and recovery procedures or standby arrangements in place and tested, to call on when events occur which cause computer systems to fail. These backup and recovery procedures should be maintained and adapted to changing circumstances as the computer systems evolve.

III-4 Risk of unauthorized Disclosure of Confidential Information

Much of the information stored in an institution's computer systems or transmitted through telecommunication lines is confidential and could damage customer relations and the reputation of the institution, as well as give rise to claims for damages, if it was to fall into the wrong hands. Word processing systems may contain records of customer correspondence and the institution's strategic business plans. Often confidential details of profit forecasts, staff salaries and personnel records are also stored in the computer. In this context, particular attention needs to be paid to private data relating to customers as well as employees.

Confidential information stored in computer systems can be accessed and read in a variety of ways. Potential avenues of unauthorized access include normal terminal inquiry facilities, use of special programs to read data files, physical removal of computer files or printouts from the institution's premises and the tapping of telecommunication lines.

A person may not have to move from his or her normal place of work to access the information and there may be no trace of unauthorized access having occurred. Compared with manual systems, much larger quantities of information can often be removed in a more convenient and processable form (e.g. on tapes or disk).

As with the other categories of risk already described, good security and control procedures are necessary to protect the institution.

These include effective physical security over computer files and good password control systems to allow different levels of access to different users. It may be necessary to encrypt highly confidential information, so that if it is stolen or intercepted, it cannot be deciphered and understood or manipulated.

III-5 Risk of fraud

Losses through fraud in computer systems can be considerable. Many of the computer records contained in these systems represent assets or instructions which ultimately move assets. The wide variety of ways in which computer records can be accessed creates many possibilities for fraud. The increasing dependence of internal control procedures on computer programs and the speed with which assets can be transferred using electronic payment and message switching systems complicates the task of fraud prevention.

There are several ways in which fraudulent transactions in computer systems can be generated. For example:

a) Unauthorized amendments to payment instructions can be made prior to their entry into the computer system;
b) Unauthorized transactions can be entered directly through terminals;
c) Unauthorized changes to programs can be made during routine development or during maintenance which may cause the program to generate fraudulent transactions automatically, to ignore control checks on selected accounts or to remove records of specified transactions;
d) Special programs can be used to make unauthorized changes to computer records in a way that bypasses the normal control and audit-trail facilities built into the computer systems;
e) Computer files can be removed physically from a computer installation, amended elsewhere by the insertion of fraudulent transactions or balances and returned for processing;
f) Transactions can be introduced or intercepted and amended fraudulently whilst being transmitted through telecommunication networks.

Most computer systems contain control facilities and produce reports designed to assist in the prevention or detection of these types of fraud. These too, however, may be vulnerable to manipulation by persons with access to computer terminals or files.

Before effective controls to prevent fraud can be implemented, care must be taken to identify all the vulnerable points and areas in each system. Potentially vulnerable records and programs must then be protected against unauthorized changes.

In this respect it should be noted that testing programs and systems, although an effective means of detecting most of them may not detect all unauthorized changes. This is because manipulations to programs can be made in such a way that they do not come into operation until long after testing has been completed, perhaps triggered by a particular date having been passed or by a particular transaction being entered into the system.

Senior Management must be properly aware of the risks of fraudulent transactions through the use of computers and actions should be taken by operational management in the prevention of computer fraud.

IV. Nature of Controls

It is senior management's responsibility to ensure that operations are adequately protected against the risks described under section III above. Management therefore needs to understand not only the nature of computer risks but also the techniques at their disposal to manage these risks. These techniques may be classified broadly as;

- Preventive controls;
- Containment controls;
- Insurance and
- Audit.

IV-1 Preventive Controls

Preventive controls are those designed to ensure that events which threaten operations occur only very infrequently. Examples are the careful design and setting of computer centers, data input controls, security devices to prevent unauthorized access to computer equipment, passwords designed to restrict access to computer programs and data, and authentication of telecommunication messages. Other examples are the procedures used to ensure that systems specifications reflect the institution's needs, projects are properly controlled, systems are well tested before implementation and to ensure that documentation is accurate and physically secured. These types of control are essential to the effectiveness, integrity and reliability of computer systems. Preventive controls, however, are vulnerable to human failure and can never be totally reliable. Therefore, additional measures are required to ensure that potentially damaging events do not cause significant losses or cause operations to fail.

IV-2 Containment Controls

On top of preventive controls, some containment controls must exist. Containment controls are essential to protect institutions from the consequences of events which bypass preventive controls. They are designed to detect and limit the effect on the business of events which occur and threaten operations.

Examples are fire detection and extinguishing equipment, dual capacity in telecommunication and computer networks to limit the consequences of breakdowns of individual com-

ponents, reconciliation procedures designed to detect errors quickly and contingency plans to aid recovery if the computer center was to be disabled by any calamity (calamity plan).

IV-3 Insurance

Some of the risks referred to in this memorandum can be insured, such as fraud by employees and the costs of replacing data, software and equipment. It may also be possible to insure against the consequential losses for an institution following damage to computer resources and consequent business interruption. Because neither preventive nor containment controls can ever be foolproof, it is usually prudent to obtain insurance coverage appropriate to the particular risks within the institution. Insurance, however, cannot be regarded as a substitute for good preventive and containment controls. To determine the scope of the insurance, particular care should be taken to identify and understand the types of losses which are not recoverable under insurance policies and the limitations imposed by the policies.

IV-4 Inspection and Audit

Even soundly designed security and control systems can fail and leave an institution exposed to losses if the procedures they lay down are not followed in practice. A regular program of independent tests of security and control procedures by inspectors, auditors or consultants should help to identify lapses in control before they put operations at serious risk. Conversely, without regular audit testing, any new or unidentified exposures which exist might not be detected for a considerable period.

Generally the frequency and depth of audit tests conducted in any area should reflect the level of risk to the institution if the security and control procedures in that area fail. With any audit program, either internal or external, it is important to establish the scope of the audit by class of risk and type of control.

Apart from regular audit checks on existing systems, Internal or External Audit involvement at an early stage in the specification and design of new systems can contribute significantly to the quality and effectiveness of security and control procedures to be developed.

V. Conclusion

Supervised institutions can normally achieve effective, secure and reliable computer systems only through an appropriate balance of all the control techniques described in this memorandum. The selected controls will vary from institution to institution, reflecting the particular risks within each institution and the costs of related security and control procedures.

Computer security and control procedures must form an integral part of the system of internal control within an institution. Therefore, it is important for Senior Management to understand the relationship that exist between the computer security and control procedures addressed in this memorandum and the total system of controls within the institution. Discussions with computer security and audit specialists as to the use and interpretation of this memorandum may assist Senior Management to achieve this understanding.