CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN (Central Bank)

IT Framework Memorandum

For

Supervised Institutions

WILLEMSTAD, Updated version April 2011

IT Framework Memorandum for Supervised Institutions

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.

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

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.

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.

[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. 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.

V. 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.

VI. 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:

- <u>Asset Management:</u>
To achieve and maintain appropriate protection of the institution's assets;
- <u>Human resource security:</u>
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;
- <u>Physical and environmental security:</u>
To prevent unauthorized physical access, damage, and interference to the the institution's premises and information;
- <u>Communications and operations management:</u>
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] 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 auditted by the IT Auditors

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.

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 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.

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)