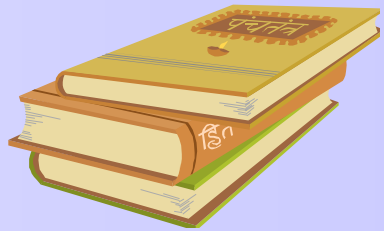
Provisions and Guidelines for IT Service Management

Dhr. C. Walters

November 27, 2014

Why IT regulations?



Information Technology has become increasingly complex

- Distributed environments;
- Layered applications;
- Integrated applications;
- Version control, patch management;
- Array of computer operating platforms;
- Mix of devices (firewalls, routers, switches);
- Connectivity to the internet (public network);
- Cloud computing; and
- Security monitoring and prevention tools.

As the complexity of technology grows, information systems and networks are faced with control weaknesses.

Objectives of IT regulations

In 2009 the Central Bank issued the
IT Framework Memorandum for Supervised Institutions

Objectives:

- Streamline the level of competence on IT governance;
- Provide clarity amongst stakeholders;
- Improve the maturity level by implementing safe and sound practices;
- Improve the security, stability and resilience of IT systems;
- Improve the professionalism of IT staff ; and
- Supply internal and external auditors with a framework to audit IT processes.

By complying to the IT Regulations each supervised institution will be

- *contributing to maintain a stable financial sector; and*
- *raising its own maturity level for IT processes.*

What is issued?

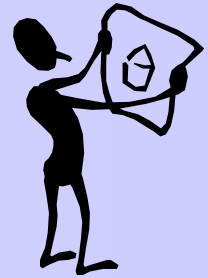
Until today:

- Provisions and guidelines for E-Banking – 2007
- IT Framework Memorandum - 2009
- Supervised Institutions IT Questionnaire -2009
- Provisions and guidelines for BCM – 2010
- Supervised Institution Simplified IT Questionnaire-2011
- Provisions and guidelines for ISM – 2011
- Provisions and guidelines for IT Service Management -2014

Planning to issue – Provisions and guidelines for:

- IT Governance
- IT Development and Acquisition

CBCS Timeline



Scheduled work:	Complete by:
Business Continuity Management	1 July 2011
Information Security Policies	31 Dec 2011
Initial Inf.Sec. Management Plan	1 April 2012
Implement a formal Inf.Sec. Risk Assessment methodology	1 July 2012
Comply with ISO 27002 Control Objectives	31 Dec 2012
Implement technical security standards	1 July 2013
Implement security monitoring	31 Dec 2013
Full compliance with Inf.Sec.Man Regulation	1 July 2015

CBCS Philosophy

- The IT regulations set out **what** principles need to be carried out.

- The supervised institution decides **how** to implement the regulations and **to which extent** inherent information technology risks are mitigated.

- The supervised institution should implement controls to mitigate risks **proportionate** to the operational risk
  and
  tailored to the nature, size and scope of the operations and complexity of the business.

- The institution's internal and external auditors will verify:
  - if the principles provided in the regulations are adhered to and
  - if controls are in place to ensure that inherent information technology risks are managed adequately.

CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN

Provisions and Guidelines for IT Service Management

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 IT service management.

The object of this principle is to set the tone at the top.

By establishing ITSM policies, management sets out:

- The organization's aims, principles, and approach to ITSM;
- The importance of fulfilling business requirements with the use of IT;
  - Ensuring that risks to services are identified, assessed and managed;
  - Examining new possibilities for IT and ITSM;
  - How to resolve incidents and problems and how to implement changes in the IT environment;
- Implementing key roles and responsibilities for the ITSM process; and
- How ITSM will be governed and reported upon, including key performance indicators and key goal indicators.

Principle 2.

Supervised Institutions should define the level of service required for critical business functions.

The object of this principle is to align IT services with business requirements.

Per critical business process we should answer :

- Does IT provides the service that I need to run my business?
- What level of service is important to the business and its customers during normal circumstances?

Principle 3.

Supervised Institutions should set up the support and delivery functions for IT services.

The objective of this principle is to ensure that current, changed and new services will be delivered and managed according to the service levels required by the business functions.

IT should set up the processes and controls for the support and delivery functions of IT services, which are:

- IT Support services & Incident management;
- Problem management; and
- Change management.

Any change in the IT environment should be under control of change management procedures.

Principle 4.

Supervised Institutions should manage IT assets and configuration information.

The objective of this principle is to accommodate financial, insurance, contractual, risk assessment, inventory and incident management functions. Assets in this regard include all elements of software and hardware that are needed to run business processes in a safe and sound manner.

Includes:

- Keeping the inventory of IT assets (Hardware and software);
- Labeling of assets;
- Inventory review (Hardware and software);
- Procurement of IT assets; and
- Disposal of IT assets.

Principle 5.

Supervised Institutions should protect the physical computer environment to guarantee IT services.

The objective is to prevent unauthorized physical access, damage, theft and interference to the organization's computer environment.

Includes:

- Site Selection and Layout;
- Physical Security Measures;
- Physical Access; and
- Physical Facilities Management.

Principle 6.

Supervised Institutions should monitor the IT infrastructure in order to ensure continuous service on the network.

The objective of network monitoring is to detect problems and optimize the performance of IT infrastructure, resources and capabilities.

Includes:

- Define and implement procedures to monitor the IT infrastructure and related events;
- Assess current performance and capacity of IT resources to determine if sufficient capacity and performance exist to deliver against agreed-upon service levels;
- Conduct performance and capacity forecasting of IT resources at regular intervals; and
- Continuously monitor the performance and capacity of IT resources.

Principle 7.

Supervised Institutions should implement a backup/restore procedure to comply with business needs and legislation.

The objective of backup/restore procedure is to create a safety net to recover from computer deflects, major incidents, and to comply with legislation.

Includes:

- Awareness and compliance with legislation with respect to data retention;
- The grandfather/father/son principle with three cycles of backup:
  - Daily;
  - Monthly; and
  - Yearly.
- Transportation of backup media; and
- Restore testing.

Principle 8.

Supervised Institutions should manage third party services.

The objective of this principle is to govern third party services. Services obtained from third parties should be in line with the third party service level agreement/contract.

Includes:

- Investigating third parties before entering a long term relationship.
- The security controls, service definitions and delivery levels included in the third party service level agreement/contract; including daily IT Operation management, such as
  - Patch and anti-virus management;
  - Backup and restore management;
  - Operating System fine-tuning;
  - Log analysis;
  - Network monitoring;
  - User account management for the network;

Principle 8 (continued).

Supervised Institutions should manage third party services.

In case a model is used where the application and data is stored at the third party the following needs to be part of the third party service level agreement/contract:

- The supervised institution should be owner of its own data;
- Data must be stored encrypted;
- Encryption key is only known to the supervised institution, where the third party cannot access the data in a readable format;
- The CBCS should have the right to audit the third parties IT infrastructure (including computer facilities, hardware, operating environment, application and database);
- For critical outsourced financial systems:
  An independent audit firm should yearly review (using the ISAE3402 /SSAE16 standards).

  If there are any uncertainties about this or other principles for your specific environment please contact the central bank.

Principle 9 - 11

Principle 9:
Supervised Institutions should standardize IT financial management.
Cobit 5.0 has made a big improvement by introducing
APO06 'Manage Budget and Costs'.

Principle 10:
Supervised institutions should continuously educate and train IT personnel and users.

Principle 11:
Supervised Institutions should ensure the quality of all aspects of ITSM by assessing independent audits.

Principle 12:
Supervised Institutions should inform the Bank when critical IT systems are being replaced or innovative products will be introduced.

Why would we want to comply?

Do not think of it as a necessary evil.

Compliance will improve the maturity level of the company by:

- Better alignment of the Business and IT;
- Providing clarity on key organizational risks;
- Increasing responsibilities and accountability;
- Improving decision making within the company;
- Improving controls efficiency; and
- Increasing the level of competence.

Any feedback/comments/errors detected please contact c.walters@centralbank.cw

Questions ?