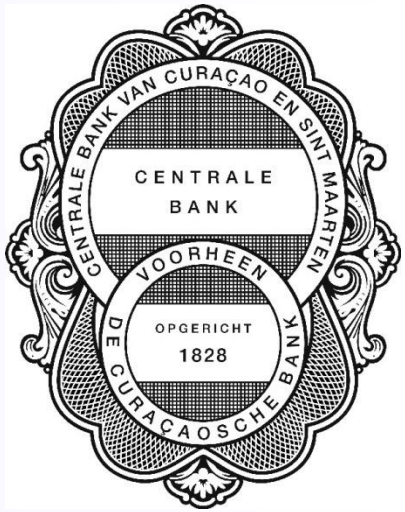
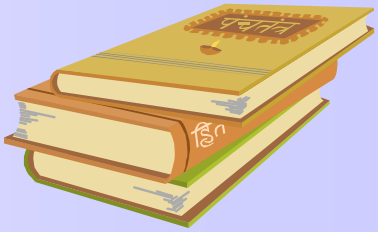
Provisions and Guidelines for Information Security Management

Dhr. C. Walters



June 8, 2011

Why impose rules for Information Security Management ?



- Supervised institutions have been requesting rules;
- Rules promotes clarity amongst all stakeholders;
- Rules supports safe and sound practices; and
- Promotes the maturity level.

Which supervised institutions should comply?

- All institutions supervised by the CBCS should comply to the new rules;
- However, the rules set out only high level principles supervised institutions need to adhere to;
  - The CBCS does not imply how much money should be invested; or
  - What systems need to be bought; or
  - What physical security features should be in place.

Responsibilities for stakeholders

- The extent to which 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 ISM are adhered to and if controls are in place to ensure that inherent risks are managed adequately.

Principle 1


Grand canyon skywalk

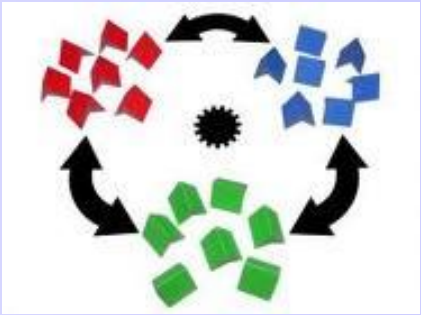
- **The Board of Supervisory Directors and the Board of Managing Directors should establish effective management oversight with respect to potential events that threatens the security of information assets of the supervised institution.**

Principle 2

- **Supervised Institutions should design, implement and maintain an ISM framework.**

This includes:

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



ISM framework is designed to provide 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;
- Information security processes are monitored and reported on to ensure that objectives are achieved and undesirable events are prevented or detected and corrected;
- Responsibilities of information security are clearly assigned, managed and enforced.

How do we get there?

- Adapt to ISO/IEC 27002
- Collect, document, analyze and prioritize information security requirements
  - Create an ISM work group
  - Perform a quick scan/gap analyses
- Create a written ISM program

Examples topics for an ISM program

- Setup of information security governance (e.g. establishing an IS steering committee, determining IS ownership and responsibilities, appointing an Information Security Manager);
- Setup of the information security policy, standards and procedures;
- Short term risk mitigating actions for high risk situations (exposed as a result of the quick scan);
- 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);
- Physical and environmental security;
- Outsourced services risk review;
- Customer, retailers and business partners risk review;
- Setup of security baseline configurations for devices, DBMS and software;
- Legal security requirements regarding country or international law and contracts with external parties;
- Software and user license management;
- Network security assessment;
- Vulnerability management;
- Information security awareness training;
- Intrusion Detection / Intrusion Protection; and
- Log analyses and network monitoring.

Principle 3

- **Supervised Institutions should maintain an ongoing information security risk assessment program**

Principle 4

- **Financial Institutions should establish information security monitoring**
  - **Log file analyses;**
  - **Capacity Management;**
  - **Vulnerability management; and**
  - **Managing metrics data (NIST 800-55).**

Principle 5

- **Supervised institutions should establish incident management and response**

Principle 6

- **Supervised institutions should protect the privacy of customer information**

  - Ensure the security and confidentiality of customer records and information;
  - Protect customers against any anticipated threats or hazards to the security or integrity of such records; and
  - 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, customer information may not be sold to or shared with others and may only be used for the purpose for which the data was originally recorded.

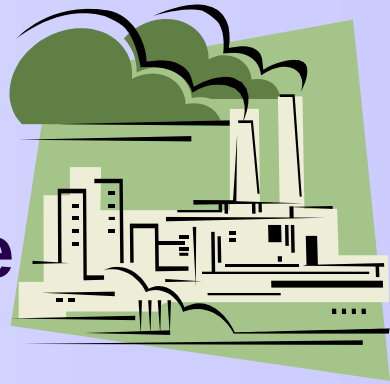
Principle 7

- **Supervised institutions should provide information security training**

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**

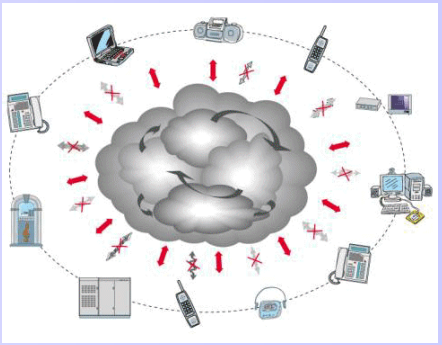
The auditor should review if the ISM Framework and plans are adequate and effective, and if the institution operates accordingly in a manner to ensure that:

- 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;
- Interactions with the various stakeholders occur as needed;
- Significant financial, managerial, and operating information is accurate, reliable and timely;
- Security practices are standardized;

Principle 8 - Continued

- 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.

Summary



- Why impose rules for Information Security Management?
- Which supervised institutions should comply?
- The principles for Information Security Management

Implement the initial ISM Program within four years

Scheduled work	Must be completed by:
Business Continuity Management	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

Provisions and guidelines for Information Security Management

The provisions for ISM will help us all!

Questions ?