CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN
(Central Bank)

Provisions and Guidelines

For

Information Security Management

WILLEMSTAD, Updated version April 2011

Provisions and Guidelines for Information Security Management

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, 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.

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

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.

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

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 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.

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) non-compliance, 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;

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

- *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.

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.

[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
[7] We will only refer to "ISM 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".

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;
- 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.

[8] See appendix 2 for an overview of helpful websites

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 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);

[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.

- 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.

[10] For further reference see appendix 2

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

[11] See Provision and Guidelines for Business Continuity 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

[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.

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).

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
- 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,

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

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).

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

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, 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.

[15] E.g. selling customer e-mail addresses to a marketing company

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.

[16] Six month or longer

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;
- 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