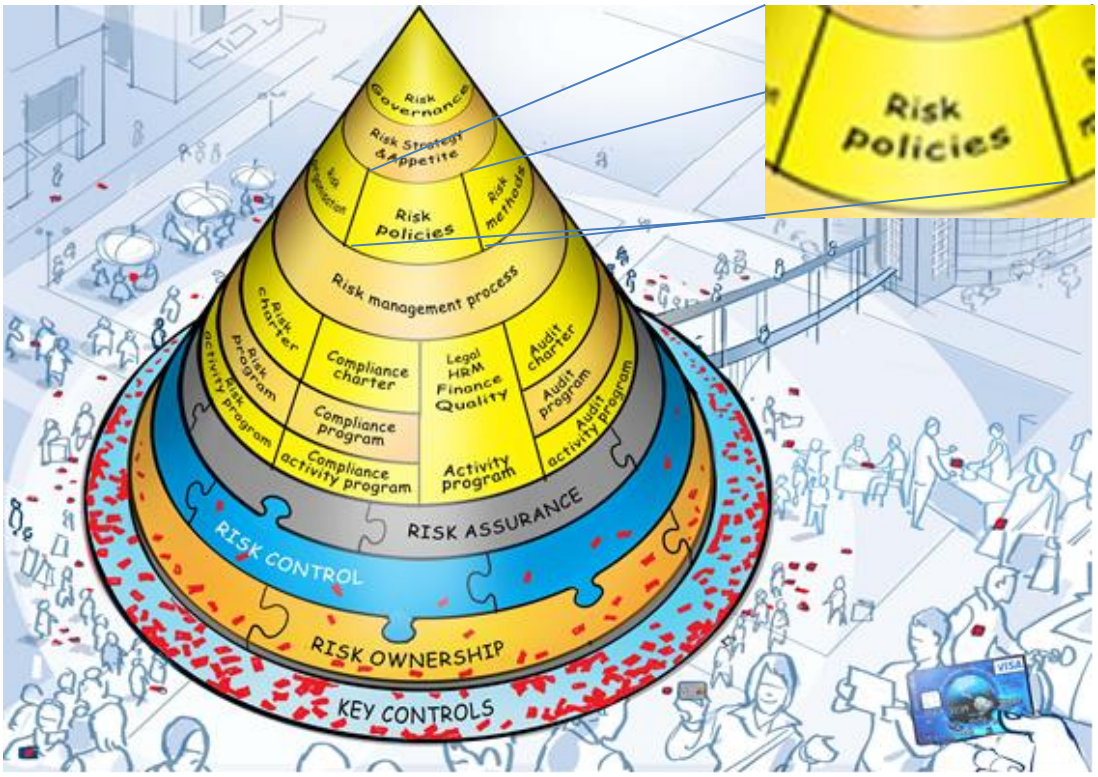
Information Security Standard



By: Risk

Version: 1.0

Date: 16-11-2017

Contents

1. Introduction

1.1. Information security defined

Information security is focused on protecting information against a wide range of threats in order to ensure business continuity and to minimise business risks. In line with ISO/IEC 27000 and ABN AMRO, ICS has defined information security as the "preservation of Confidentiality, Integrity and Availability (CIA) of information".

Information security is the process of protecting information and its associated assets, e.g. computers, paper files, from accidental or intentional breaches of:

- Confidentiality: ensuring that only authorised users have access to information and associated assets
- Integrity: safeguarding the accuracy, completeness and timeliness of information and information processing
- Availability: ensuring that authorised users have access when required to information and associated assets.

Information assets include:

- Data
- Storage media
- Applications
- Data communication networks
- IT infrastructure, systems, processing facilities

The value of information assets for the business is leading when identifying security measures to be implemented.

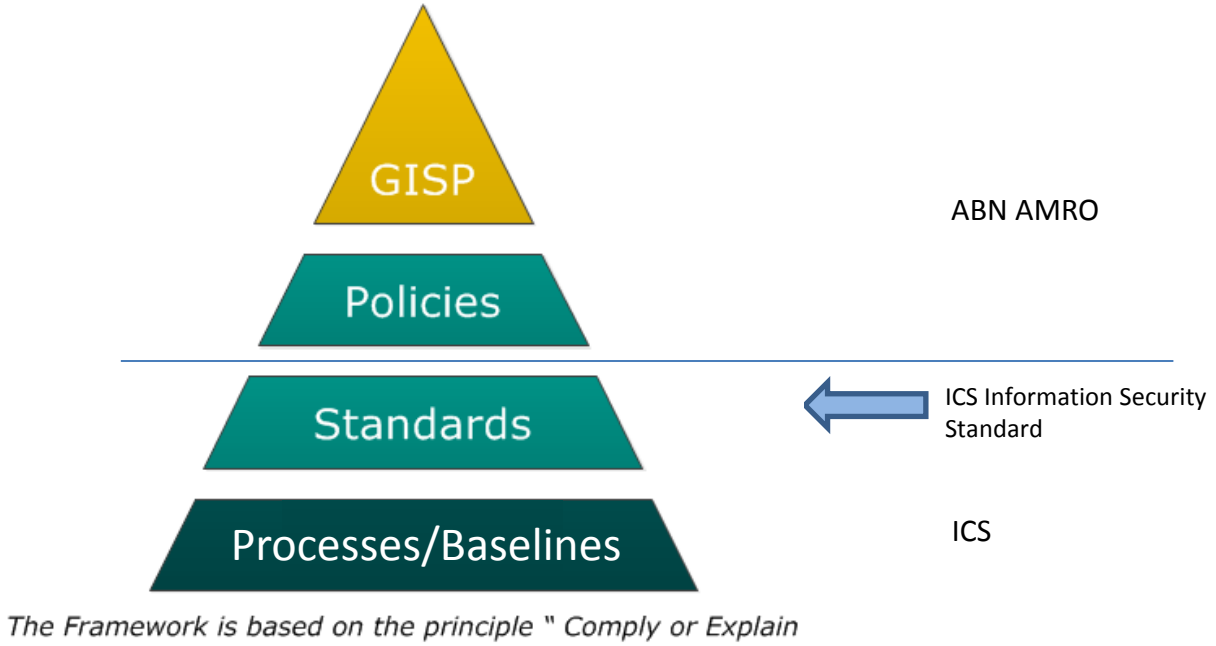
1.2. Purpose and scope

ICS fully adopts the Information Security Policy of ABN AMRO (AIM number: 108-49-00).

Purpose of this standard is to set guidelines on how to manage Information Security issues in a uniform, structured manner. This document sets requirements for Information Security and describes the activities and responsibilities for Information Security within ICS. In the standard, an explicit relation is established with the baselines available within ICS.

This standard follows the structure of the ABN AMRO Information Security Policy. Not only because the structure is in line with the ISO 27001 standard, but als for policy adherence reasons.

The following image shows the place of this standard in the document structure of ABN AMRO.



Scope: the Information Security Standard of ICS and the measures following from it apply to all ICS locations and staff, including students on a work placement, temporary workers and hired-in employees of third parties, as well as personnel dealing with management and maintenance of the resources used.

The Information Security Standard relates to the various processes within ICS where data processing and provision of information takes place. This concerns ICS data, customer data, employee data, card data, partner data, cobrander data and shareholder data. Outsourced data fall under the scope of this policy as well. Therefore, ICS is responsible for the measures to be taken by the outsourcing partner and the monitoring thereof.

1.3. The importance of information security

As already specified in the above paragraph, International Card Services processes lots of valuable data and information. ICS depends on this information and on information processing technology. These valuable and vulnerable company assets must be protected against loss and threats to availability, integrity and confidentiality at all times. Next to this ICS must ensure compliancy with external laws, regulations and guidelines with regard to this information.

Quote from the ABN AMRO Information Security Policy:
"Information is one of the bank's most valuable assets. Securing the confidentiality, integrity and availability of information and information systems is essential for ABN AMRO's reputation as a highly trusted business partner and thus for ABN AMRO's continued growth and success."

Incidents that affect the Confidentiality, Integrity and Availability (CIA) of customer or bank information can have a high negative impact on the reputation of the bank and its clients. This may result in substantial financial or reputational damage, such as direct financial losses, decrease in business, sanctions by regulators or legal claims.

2. Framework for information security

To ensure that Information Security is implemented in a structured way, ICS has fully adapted the international standard for information security: ISO 27001:2013. The principles mentioned in the policy are fully mapped with the objectives mentioned in this standard.

In addition, related to card holder data, ICS follows the principles of the Payment Card Industry Data Security Standard (PCI/DSS).

ISO 27001:2013 objectives are translated in controls, measures and guidelines. The controls have been implemented across ICS and are monitored and tested in accordance with the ICS Control Monitoring and Testing Procedure.

The directives and principles for the elaboration of IT Security are included in the Beleid IT Risk Management .
.

The set up IT Security focuses on "zero trust". This is supported by the following principles:
1. Increase in security awareness is embedded in daily activities
2. Measures are always aimed at protecting information
3. Do not trust the network, endpoint, user or application
4. Respect the privacy laws and regulations
5. Checking is better than trust
6. Security measures are confidential

For some subjects, further specific guidance is required. This is documented in the Baseline Security Management.

2.1. Information Security Awareness

Awareness of all staff members is key in managing Information Security. Because of the importance of the subject, the CEO of ICS is accountable for information security awareness.
The Manager Information Risk & Security is responsible for increasing the level of awareness.
Key in improving awareness is the Team Information Security (TIS). The TIS is organized and chaired by Manager Information Risk & Security. Participants are Investigations, BISO, Risk, Compliance, Technical Application Management, Security Architect, Facility Services, Privacy Officer and Operational IT Risk, other participants on invitation.
See baseline Information Security Awareness for details

2.2. Governance

- Risk is responsible for 'translating' the ABN AMRO Information security policy to an ICS Information security standard
- Information security policies and standards are approved by the Enterprise Risk committee (ERC). Information security baselines are approved by the CIO.
- Risk is responsible for maintaining the consistency of the information security policy framework and will initiate and support actions for topics covered in other second-line support functions
- Information Risk & Security monitors the coverage of the ISO/IEC 27000 family by ICS policies and will initiate and support actions for topics covered within Information Technology & Business Support

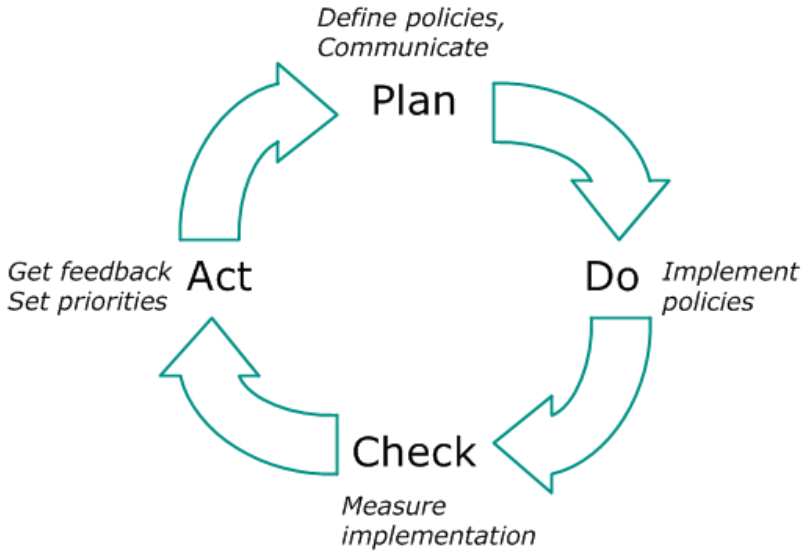
See baseline Security Management for the operational implementation.

3. Information security management

This chapter describes how information security management is organised within ICS as a whole. This is generally referred to as the Information Security Management System (ISMS) and is fully aligned with the standard policy management cycle as well as the Baseline used (Baseline Security Management).

3.1. ISMS description

Key in information security management is continuous improvement. The following diagram reflects this process. Over time, this will result into a higher maturity level of information security.



Plan
Information security standards, IT policies and baselines are drafted, approved and published. The publication of new and updated documents is communicated to those who need to know. See Baseline Security Management for details.

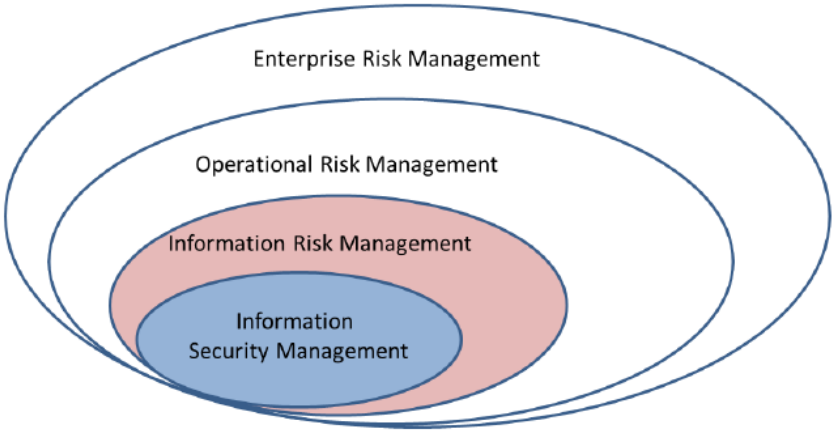
Do
After publication, policies have to be implemented within the organisation. The actual implementation of information security measures is the responsibility of the departments in the 1st line. Information Risk & Security supports implementing information security measures.

Check
Measure and report the effectiveness of controls and the level of compliance with existing information security policies and standards. Check are performed by use of assessments an (key control) testing.

Act
The level of implementation of security measures must be adjusted to the actual risks. Input triggers, such as results of assessments, MC&T results, audit findings, feedback on existing policies or external developments like new security threats or changes in laws or regulations, are used to set priorities for the policy, standard or baseline maintenance plan.

3.2. Context ISMS

Within ICS the ISMS is positioned as part of Information risk management, which is regarded as an operational risk.



See Baseline Security Management for details.

3.3. Three lines of defence

ICS has adopted the three Lines of Defence model. This model supports ICS in clarifying which role each function plays in managing our risks.

Line	Who	Role	Responsibilities
1st Line	ICS Line Management Information Risk & Security	Risk Owner	• Take risk decisions • Determine and mitigate risks • Measure risks • Monitor risks • Report risks
2nd Line	Risk Legal Compliance	Risk Control	• Support 1st Line • Challenge the mitigating actions (Design of Control)) • Tests the working of risk control framework (Working of Control) • Report risks, control and related issues
3rd Line	Internal Audit	Risk Assurance	• Reviews and evaluate the working of 1st and 2nd Line of Defence • Confirms if controls are working as intended

4. Generic information security rules

In this chapter the generic policy rules have been elaborated to ICS standards. These policy rules are grouped following the ISO/IEC 27002 clauses. For each clause, the most relevant policies and/or baselines are specified.

The policy rules are mandatory and are formatted in **bold**.

4.1. Organisation of information security

Objectives

- To manage and control information security within ICS
- To create a risk aware culture

Information security policy rules

Information security responsibility (1st line of defence)

1. **Personnel at all levels are responsible for information security.**
   All personnel have information security responsibilities for the following:
   1. Use of information, information systems and other information assets in line with job role and responsibilities, their intended purpose and applicable policies, standards and guidelines
   2. Exclusive use of the assigned user ID and thus responsibility for all actions performed under the user ID and for the security of the applicable authentication means, e.g. password, security token. These requirements are defined in Beleid Identity Management at ICS and Baseline Wachtwoorden en Authenticatiemiddelen.
   3. Immediate reporting of known or suspected vulnerabilities and security incidents to the line manager and/or Information Risk & Security, in accordance with the Baseline Incident Management
2. **Line management of each business line is responsible for the implementation of information security policy rules, standards and baselines in business activities**
   Line managers have information security responsibilities for the following:
   a. Clear assignment of information security roles and responsibilities, taking into account the principles of a proper segregation of duties and ensuring that high-risk functions are manned by qualified personnel
   b. Communication of relevant information security policies, standards and guidelines to new personnel, with at least an annual update for current personnel to keep them informed and aware
   c. Ensuring that personnel access rights are in line with the job role and responsibilities
   d. Timely and effective response to reported vulnerabilities and security incidents
   e. Setting a good example by complying with information security policies, standards and guidelines
   f. Monitoring compliance of personnel, with appropriate follow-up

For details see policy IAM. Beleid Identity_Management at ICS and baseline Proces Identity & Access Management.

3. **Line managers must monitor and report compliance with approved group information security policies and standards within their area of responsibility**
   Compliance to the policy, standards and baselines must be reported to Information Risk & Security. Line managers can delegate expert tasks such as information security assessments or security monitoring to Information Risk & Security, Risk or other parties.
   If the information asset has been outsourced to a third party, the contract owner is responsible for ensuring and verifying third-party compliance. For more requirements refer to ICS Outsourcing Policy.
4. **Line management must appoint an information security officer who co-ordinates all information security activities within the cluster**
   Within ICS all information security activities are coordinated by department Information Risk & Security.
5. **Line management must document how information security is organised within their cluster**
   Documentation of information security is delegated to Information Risk & Security. See baseline Security Management.

Information security oversight (2nd line of defence)

To support information security, line management must ensure that information security goals are identified.

1. **The co-ordination and oversight of information security for ICS is the responsibility of Information Risk & Security in close co-operation with Risk**

4.2. Information asset management

Objectives

- To ensure that all information assets are accounted for and have a formal owner
- To achieve and maintain appropriate protection of all information assets according to their classification
- To maintain an inventory of all information assets, which helps to ensure that effective information asset protection takes place

Software Asset Management within ICS is aimed at administering, monitoring and verifying the use of software and licenses. This prevents the use of software from inadequate licenses, licensing, or software being illegally obtained within the organization. This helps SAM contribute to the compliance of the organization.
The department Solutions Architectuur is responsible for the overview of all applications. All hardware is recorded in Topdesk under responsibility of Business Support.

Information security policy rules

1. **Every information asset must have an owner, who is accountable for the security of the information asset**
   The responsibilities of the asset owner are described in Beleid Eigenaarschap.

2. **Business process owners must ensure that an inventory is maintained of the information assets that support their business processes**
   Business process owners are supported by Solutions Architectuur.
3. **Owners of information assets must ensure that each of their information assets is assigned a classification label that properly indicates its business value and criticality to the organisation**
   A CIA rating is assigned as an indication of the value of the information assets. The department Solutions Architectuur is responsible for assigning CIA ratings.
   Every year, for all business processes, information systems / applications, technology infrastructure and data the CIA Ratings is revised.
   The owner of the information asset is also owner of the CIA rating and responsible for the realization of the correct measures to comply with the CIA rating of the information asset.

   An overview of the measures that are necessary for the different CIA ratings is listed in Bijlage I van IT beleid CIA rating & dataclassificatie: Tactische maatregelen CIA (9-vlaksmodel).

   See Baseline CIA Rating & Data Classificatie for details.

4.3. Risk assessment and treatment

Objective

- To manage information security risk profile to an acceptable level of control in an efficient and cost effective way.

Information security policy rules

1. **Business owners must ensure that information security risk assessments are performed on new or significantly changed information assets**
   Initiation of an ISRA is the responsibility of the business owner. ISRA's are performed by Information Risk & Security, if necessary in cooperation with Risk.
2. **For existing information assets a re-assessment is periodically performed based on their classification**
   As the environment might change over time, operational information assets must be periodically re-assessed, in line with business priorities. This is the responsibility of the business owner.
3. **For all identified risks approval is obtained for recommended actions and acceptance of any residual risks**
   It is important that the agreed security levels are properly maintained. As the environment might change over time, operational information assets must be periodically re-assessed, in line with business priorities and the current change process within ICS.
4. **The information asset owner is accountable for monitoring the registration and timely resolution of all identified IS risks**
   Follow up for the implementation of the mitigation plan must be within the agreed timelines. This must be adequately monitored to make sure that all identified risks are effectively managed
5. **Security testing, penetration test and/or code review, must be performed on systems with a high risk profile**
   For systems with a high-risk profile, systems that are C, I or A critical e.g. systems that are subject to fraud, additional security testing is required. Security testing is part of the

responsibility of the scrum teams.
The type of test is determined during the information security risk assessment**.**

4.4. Human resources security

Objectives

- To manage the human resource aspects of information security in a way to prevent the risk of theft, fraud or misuse of information and facilities
- To ensure that employees, contractors and third party users enter and exit the organisation or change employment in an orderly manner (joiner/leaver process)

Information security policy rules

1. **Pre-employment screening on all candidates for employment, contractors, and third party users must be carried out according to HR procedures**
   Pre-employment screening is a shared responsibility. Human Resources is responsible for this step to be started. Investigations is responsible for the actual screening.
   It is the responsibility of the managers that hire new staff (internal or external), contractors or third party users to report changes in staff to HR.
2. **The terms and conditions of employment contracts must include the employees and the organisation's responsibilities for information security**
   The contracts must explicitly refer to applicable regulations, such as the personnel and the sanction regulations.
   ICS stated a Code of Conduct on Information Security. The rules of conduct are extensively described in the information security brochure which is handed over to all new employees during the 'Introductiecursus'.
3. **Line management ensures that all personnel joining, leaving and changing job positions is handled**
   Line management ensures that for all personnel changing job positions within ICS, both physical access rights and access rights to information are changed in accordance with the requirements of the new job position. Also, any equipment that is unnecessary for the new job position is returned. Access right are changed according to Baseline Identity & Access Management and specific Access control Procedures.
4. **New and current personnel must be properly informed and trained about their information security responsibilities, policies and standards and where these policies and standards are published**
   The HR Centre of Expertise is responsible for a yearly e-learning on Information Security. The departments Risk and Information Risk & Security are responsible for the content.

4.5. Physical and environmental security

Objectives

- To prevent loss, damage, theft or compromise of assets via unauthorised physical access and environmental threats to premises and information assets

Information security policy rule:
Information processing facilities and assets that process sensitive or critical information are housed in secure areas and protected by physical security perimeters.

Physical access to the ICS building is the responsibility of the Business Support manager.
For details see Baseline Fysieke Beveiliging

Except for the telephone exchange all business process related hardware is placed in external secure computer centers (Tieto and KPN). Physical security matters including protection from power failures and other disruptions caused by failures in supporting facilities are part of the contracts with the service suppliers.

Telecommunications cabling carrying data or supporting information services are protected from interception or damage according to Baseline Informatie Transport.

Work palaces are secured according to Baseline IT Werkplekbeveiliging.

4.6. Communications and operations management

Objectives

- To ensure the correct and secure operation of information processing
- To implement and maintain the appropriate level of information security and service delivery in line with delivery agreements
- To ensure the secure communication of information in networks and the protection of the supporting infrastructure
- To detect unauthorised information processing activities
- To prevent unauthorised disclosure, modification, removal or destruction of assets, and interruption to business activities

Information security policy rules

1. **Management ensures that all information processing facilities are operated in a secure manner**
   The responsibility of business owners for information processing facilities is described in beleid-eigenaarschap.. More specific responsibilities of management are described in Beleid IT Risk Management.
2. **Every information processing facility has a formal change management procedure in place**
   The change management procedure must include a security impact assessment and business sign-off. For details see Baseline Change Management.

3. **Information systems must be installed, configured, maintained and decommissioned following agreed configuration management procedures**
   Within ICS department IT Service Operations is responsible for controlled installation, configuration, maintaining and decommissioning of information systems.
   relevant baselines are:
   - Baseline Configuration Management
   - Baseline Functional Application Management
   - Baseline Incident Management
   - Baseline Capacity Management
   - Baseline IT Infrastructure Management
   - Baseline Logging and Monitoring
   - Baseline Network Security
   - Baseline Key Performance Indicators IT&BS
4. **A back-up is made regularly of all relevant business information. Electronic back-ups are periodically tested and stored securely**
   The back-up procedure is the resonsibility of IT Service Operations. For details see Baseline Back-up & Recovery.
5. **Management ensures that proper measures are taken to protect information that is exchanged either internally or externally**
   See Baseline Informatie Transport .
6. **Information security controls are agreed between ICS and external parties**
   All contracts with external parties are managed by a standard process. The owner of the process outsourced to an external party is responsible for starting the process. Department IT Staff is responsible for the process itself and monitoring of service level agreements.
   See ICS Outsourcing Policy
   Managing the services is the responsibility of the IT Service Operations Manager. See Baseline Service Delivery Management for details.
7. **Management ensures that detection, prevention and recovery controls are implemented to protect information assets against internal and external threats**
   Protection of information assets against internal and external threats is the responsibility of IT Service Operations. For details see:
   - Baseline CIA Rating & Data Classificatie
   - Baseline Security Management
   - Baseline Malware Protectie
   - Baseline IT Vulnerability Management
   - Baseline Cryptografie Key Management
   - Baseline Fysieke Beveiliging
   - Baseline IT Werkplekbeveiliging
   - Baseline Identity & Access Management
   - Baseline Wachtwoorden en Authenticatiemiddelen
   - Baseline Remote Access
   - Baseline Logging and Monitoring
   - Baseline Network Security
   - Baseline Security Patch Management
   - Baseline Key Performance Indicators IT&BS
   - Baseline Verwijderen en Vernietigen van Data & Media

4.7. Access control

Objectives

- To control logical access to information assets
- To ensure only authorised users can access or change information assets

Information security policy rules

1. **All users of ICS systems must be uniquely identifiable.**
   Every individual within ICS gets its own unique user id, so all activities can be traced back to a user ID and subsequently to an identified person. For details see Baseline Identity & Access Management
2. **All users must be authenticated by means of appropriate authentication methods.**
   The standard authentication method is the use of user id and password. See Baseline Identity & Access Management.
3. **Authorisations must be granted based on the responsibilities and roles that employees have within their business line in accordance with agreed policies and procedures.**
   Authorisation is granted based on the principle of role-based access control, a mechanism that determines what application/data a user has access to, based on the roles a user has and the function that the usere is performing. Line management is accountable for granting access rights. See Baseline Identity & Access Management.
4. **Management must actively review the assigned users access rights regularly using a formal process, both for infrastructure as well as for business applications.**

   The review covers personal users, non-personal generic accounts, non-personal service accounts, and accounts under the Red Envelope Procedure.

   For details see:

   - Procedure Manage Profiles - Authorisation Matrix

   - Red_Envelope_Procedure_Identity&Access_Management

   - Specific Access Control Procedures

4.8. Information systems acquisition, development and maintenance

Objectives

- To ensure that only information assets are acquired or developed that meet the bank's security requirements
- To prevent errors, loss, unauthorised modification or misuse of information in applications
- To maintain the security of application system software and information

Information security policy rules:

1. **The owner of an information asset is accountable for specifying and maintaining the information security requirements for that asset**
   Ownership of information assets is defined in policy beleid-eigenaarschap.
2. **The information asset owner ensures that application controls are implemented to prevent the loss, alteration and misuse of data**
   The owner of the asset is responsible. For details see Baseline Identity & Access Management and Baseline Software Asset Management.

3. **Development, test, acceptation and production facilities must be separated to reduce the risks of unauthorised access or changes to operational information**
   All software developed within ICS is put into service according to OTAP and change management principles. See Baseline Development Management and Baseline Change Management.
4. **The asset owner makes sure that an information system meets all security requirements and that the security controls are tested before the system is taken into production**
   Activities are described in Baseline Software Asset Management and Baseline Test Management.

5. **The use of cryptography in order to protect information assets must be managed in a controlled way**
   Cryptography is important for the services of ICS. For details see Baseline Cryptografie Key Management

4.9. Information security incident management

Objectives

- To ensure information security events and weaknesses associated with information systems are recorded and communicated in a manner allowing timely corrective action to be taken
- To ensure a consistent and effective approach is applied to the management of information security incidents

Information security policy rules

1. **A ll internal and external employees are obliged to report all weaknesses and information security incidents they observe in the information security controls to their management without delay**
   ICS stated a Code of Conduct on Information Security which includes the obligation of reporting weaknesses. The rules of conduct are extensively described in the information security brochure which is handed over to all new employees during the 'Introductiecursus'.
2. **Management has established responsibilities and implemented procedures for effectively handling information security incidents and weaknesses**
   The procedure is part of the IT Risk Management policy and is an exception to the incident process. See Procedure Security Incidenten .
3. **All information about security incidents must be retained and be available**
   According to legal requirements, operational risk losses information must be retained. Therefore, information security incidents must also be retained. When damage occurs as a result of an information security incident, the loss is properly documented, registered in the ORM database and reported to ORM as described in the Risk Event Management Policy.
4. **ICS informs the appropriate judicial authorities when criminal or fraudulent activity is suspected**
   Informing appropriate judicial authorities is mainly the responsibility of the Fraud department and Compliance. They determine in consultation with the relevant parties whether notification is necessary.

4.10. Business continuity management

Apart from Information Security, Business Continuity Management exists as a separate discipline within ICS. For further information refer to the Business Continuity Management Policy. BCM at ICS is designed in accordance with this policy

Objectives

- To counteract interruptions to business activities and to protect critical business processes from the effects of major information systems failures

Information security policy rules:

1. **As part of the overall BCM implementation the business lines must identify critical information systems and critical information**
   Description of critical information systems and critical information is the responsibility of Solutions Architecture.
2. **Consequences of security failures must be identified and mitigating actions must be defined as part of the overall BCP of the business line**
   Risk is responsible for the general set up of business continuity within ICS. See BCP Q1 2017 for details.

4.11. Compliance

Objectives

- To ensure compliancy with applicable laws, with statutory, regulatory and contractual obligations with respect to the protection of information associated assets

Information security policy rule

1. **Information security policies must cover all relevant local statutory, regulatory and contractual requirements for information security**
   The inclusion of relevant local statutory, regulatory and contractual requirements is primarily the responsibility of the business owners. See beleid-eigenaarschap.
   The Legal departments supports by translating legal requirements to business requirements. Standards on topics like protection of personal data and privacy are the responsibility of Compliance. See the policy on personal Data in the Policy House.

5. Related documents

For this policy the following supporting documents exists:

- ISO 27001 (http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)
- ISO 27002 (http://www.iso.org/iso/home/standards/management-standards/iso27001.htm)
- Payment Card Industry Data Security Standard (https://www.pcisecuritystandards.org)

6. About this document

6.1. Responsibilities for this standard

Responsibilies	Function/ Department
Accountable	CEO
Responsible	Manager Information Risk & Security (LISO role)
Consulted	MIR&S, Legal, Compliance, Audit
Informed	Enterprise Risk Committee

The accountable person is responsible for determining if a change should be included in this standard or in any other related procedure, standard, work instructions or other document.

6.2. Version history

Version	Date	By whom	Reason for amendment	Status
0.1	02-09-2017	Rob van Gent	First draft	Draft
0.2	09-11-2017	Rob van Gent	Second draft	Draft
0.3	13-11-2017	Rob van Gent	Final draft	Draft
1.0	16-11-2017	ERC	Goedkeuring	Final

6.3. Next revision period

Q4 2018