
Financial services — Information security guidelines

Services financiers — Lignes directrices pour la sécurité de l'information



Reference number
ISO/TR 13569:2005(E)

AVA Documents
Document Sharing Hub
© ISO 2005

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

© ISO 2005

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents		Page
Foreword.....		iv
Introduction		v
1	Scope	1
2	Normative references	1
3	Terms and definitions.....	2
4	Symbols and abbreviated terms	10
5	Corporate information security policy.....	11
6	Management of information security — Security programme	18
7	Organization for information security	20
8	Risk analysis and assessment	24
9	Security controls implementation and selection.....	25
10	IT systems controls	29
11	Implementation of specific controls	32
12	Miscellaneous	36
13	Follow-up safeguards	40
14	Incident handling	41
Annex A (informative) Sample documents		43
Annex B (informative) Web services security analysis example		52
Annex C (informative) Risk assessment illustrated.....		57
Annex D (informative) Technological controls.....		66
Bibliography		72

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In exceptional circumstances, when a technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide by a simple majority vote of its participating members to publish a Technical Report. A Technical Report is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/TR 13569 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This third edition cancels and replaces the second edition (ISO/TR 13569:1997), which has been technically revised. It also incorporates ISO/TR 13569:1997/Amd 1:1998.

Introduction

Financial business practices have changed with the introduction of computer and network-based technologies. Increased reliance on electronic transactions has heightened the need to manage the security of information and communications technology. Huge amounts in funds and securities are transferred daily by electronic communication mechanisms controlled by security practices based on business policies.

The high value and sheer volume of such transactions within an increasingly connected, open environment exposes the financial industry to potentially severe consequences. Interconnected networks and the increased number and sophistication of malicious adversaries compound this risk with the potential to impact banks and their customers. And when financial transactions involve systemically important payment systems, these consequences may adversely affect national and global financial markets.

The necessity to expand business operations into these environments and to manage risk, demands a strong and effective enterprise information security programme. Financial institutions must manage these programmes in a comprehensive manner, just as they manage risk through well-established business practice and agreements, careful outsourcing of functions, insurance and the use of appropriate security controls. Also they must architect their security programmes to address the changing risks and requirements imposed by an expanding national and international legal and regulatory environment.

As the Basle accords warn us, operational, legal and regulatory risks can cause or exacerbate credit and liquidity risks. The management of these risks has become central to the information security programme of a financial institution. Each institution must interpret these risks in terms of its own business activities in order to understand its exposure. Careful consideration must be given to operational risks, including fraud and criminal activities, natural disasters and acts of terrorism. Low probability events, such as the tsunami that struck Asia in December 2004 and the September the eleventh, 2001 terrorist attacks on the financial services in New York City, do happen and must be planned for.

This Technical Report is intended for use by financial institutions of all sizes and types that need to employ a prudent and commercially reasonable information security management programme. It also gives useful guidance to providers of services to financial institutions, and may serve as a source document for educators and publishers serving the financial industry.

The objectives of this Technical Report are:

- to define the information security management programme;
- to present programme policy, organization and necessary structural components;
- to present guidance on the selection of security controls that represent accepted prudent business practice in financial applications;
- to inform financial services management of the need to systematically address legal and regulatory risks in their security information management programme.

This Technical Report is not intended to provide a single generic solution for all financial service institutions. A risk analysis must be performed by each organization and appropriate actions selected. This Technical Report provides guidance for conducting that process, not specific solutions.

Copyright International Organization for Standardization

Financial services — Information security guidelines

1 Scope

This Technical Report provides guidelines on the development of an information security programme for institutions in the financial services industry. It includes discussion of the policies, organization and the structural, legal and regulatory components of such a programme. Considerations for the selection and implementation of security controls, and the elements required to manage information security risk within a modern financial services institution are discussed. Recommendations are given that are based on consideration of the institutions' business environment, practices and procedures. Included in this guidance is a discussion of legal and regulatory compliance issues, which should be considered in the design and implementation of the programme.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9564 (all parts), *Banking — Personal Identification Number (PIN) management and security*

ISO 10202 (all parts), *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards*

ISO 11568 (all parts), *Banking — Key management (retail)*

ISO/IEC 11770 (All parts), *Information technology — Security techniques — Key management*

ISO 15782 (all parts), *Certificate management for financial services*

ISO 16609:2004, *Banking — Requirements for message authentication using symmetric techniques*

ISO/IEC 17799, *Information technology — Security techniques — Code of practice for Information security management*

ISO/IEC 18028 (All parts), *Information technology — Security techniques — IT network security*

ISO/IEC 18033 (All parts), *Information technology — Security techniques — Encryption algorithms*

ISO 21188, *Public key infrastructure for financial services — Practices and policy framework*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1

access control

functions that limit access to information or information processing facilities, to those persons or applications authorized such access, including physical access controls, which are based on placing physical barriers between unauthorized persons and the information resources being protected, and logical access controls, which employ other means

3.2

accountability

property that ensures that the actions of an entity may be traced uniquely to the entity

[ISO 7498-2; ISO/IEC 13335-1:2004, definition 2.1]

3.3

alarm

indication of a security violation, or unusual or dangerous condition, which may require immediate attention

3.4

asset

anything that has value to the organization

[ISO/IEC 13335-1:2004, definition 2.2]

3.5

audit

function that seeks to validate that controls are in place, adequate for their purposes, and that reports inadequacies to appropriate levels of management

3.6

audit journal

chronological record of system activities which is sufficient to enable the reconstruction, review and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results

[ISO 15782-1:2003, definition 3.3]

3.7

authentication

provision of assurance of the claimed identity of an entity

[ISO/IEC 10181-2; ISO/IEC TR 13335-4:2000, definition 3.1]

3.8

authenticity

property, as applied to entities such as users, processes, systems and information, that ensures that the identity of a subject or resource is the one claimed

3.9

availability

property of being accessible and usable upon demand by an authorized entity

[ISO 7498-2; ISO/IEC 13335-1:2004, definition 2.4]

3.10**back-up**

saving of business information to assure business continuity in case of loss of information resources

3.11**biometric**

measurable biological or behavioural characteristic that reliably distinguishes one person from another, used to recognize the identity, or verify the claimed identity, of an individual

[ANSI X9.84:2003]

3.12**biometrics**

automated methods used to recognize the identity, or verify the claimed identity, of an individual, based on physiological or behavioural characteristics

3.13**card authentication method****CAM**

concept that allows unique machine-readable identification of a financial transaction card, and that prevents copying of cards

3.14**classification**

scheme that separates information into categories, such as fraud potential, sensitivity or information criticality, so that appropriate controls may be applied

3.15**confidentiality**

property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[ISO 7498-2; ISO/IEC 13335-1:2004, definition 2.6; ISO 15782-1:2003, definition 3.19]

3.16**contingency plan**

procedure that, when followed, allows an organization to resume operations after natural or other disasters

3.17**control**

see safeguard

3.18**corporate information security policy****Policy**

general statement of the intentions and goals of establishing an information security programme

3.19**credit risk**

risk that a party within the system will be unable to fully meet its financial obligations within the system either when due or at any time in the future

[CPSS, Core Principles for Systemically Important Payment Systems]

3.20**criticality**

requirements that certain information or information processing facilities be available to conduct business

3.21

cryptography

mathematical process used for encryption or authentication of information

3.22

cryptographic authentication

authentication based on a digital signature, message authentication code as generated under ISO 16609 with a cryptographic key distributed under ISO 11568, or inferred through successful decryption of a message encrypted under ISO 18033 (coupled with ISO/TR 19038 or ANSI X9.52) with a key distributed under ISO/IEC 11770

3.23

cryptographic key

value that is used to control a cryptographic process, such as encryption or authentication

NOTE Knowledge of an appropriate key allows correct decryption or validation of the integrity of a message.

3.24

destruction of information

any condition which renders information unusable regardless of cause

3.25

digital signature

cryptographic transformation that, when associated with a data unit, provides the services of origin authentication, data integrity and signer non-repudiation

[ANSI X9.79]

3.26

disclosure of information

unauthorized viewing or potential viewing of information

3.27

dual control

process of utilizing two or more separate entities (usually persons), who are operating in concert, to protect sensitive functions or information

NOTE 1 Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is able to access or to utilize the materials (e.g. cryptographic key).

NOTE 2 For manual key and certificate generation, conveyance, loading, storage and retrieval, dual control requires split knowledge of key among the entities.

NOTE 3 Whenever dual control is required, care should be taken to assure that individuals are independent of each other. See also split knowledge.

[ISO 15782-1:2003, definition 3.31]

3.28

encryption

process of converting information to render it as a form unintelligible to all except holders of a specific cryptographic key

NOTE Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.

3.29**firewall**

collection of components placed between two networks that collectively have the properties that

- all network traffic from inside to outside, and vice-versa, must pass through the firewall;
- only authorized network traffic, as defined by local security policy, is allowed to pass;
- that it is itself immune to penetration

3.30**identification**

process of uniquely determining the unique identity of an entity

[ISO/IEC TR 13335-4:2000, definition 3.2]

3.31**image**

digital representation of a document for manipulation or storage within an information processing system

3.32**incident**

any unexpected or unwanted event that might cause a compromise of business activities or information security, such as

- loss of service, equipment or facilities;
- system malfunctions or overloads;
- human errors;
- non-compliances with policies or guidelines;
- breaches of physical security arrangements;
- uncontrolled system changes;
- malfunctions of software or hardware;
- access violations

[ISO/IEC 13335-1:2004, definition 2.10]

3.33**information processing facility**

any information processing system, service or infrastructure, or the physical locations housing them

[ISO/IEC 13335-1:2004, definition 2.13]

3.34**information**

any data, whether in an electronic form, written on paper, spoken at a meeting, or on any other medium which is used by a financial organization to make decisions, move funds, set rates, make loans, process transactions and the like, including software components of the processing system

3.35**information asset**

information or information processing resources of an organization

3.36

information security

all aspects related to defining, achieving and maintaining confidentiality, integrity, availability, non-repudiation, accountability, authenticity and reliability of information or information processing facilities

[ISO/IEC 13335-1:2004, definition 2.14]

3.37

information security officer

ISO

person responsible for implementing and maintaining the information security programme

3.38

information resource

equipment used to manipulate, communicate or store information, such as telephones, facsimiles, and computers, whether these are inside or outside the organization

3.39

integrity

the property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004, definition 2.15]

3.40

key

see cryptographic key

3.41

kiting

using a bad cheque to get credit or money

3.42

legal risk

risk of loss because of the unexpected application of a law or regulation or because a contract cannot be enforced

[CPSS, Core Principles for Systemically Important Payment Systems]

3.43

letter of assurance

document setting forth the information security controls which are in place for the protection of information held on behalf of the recipient of the letter

3.44

liquidity risk

risk that a party within the system will have insufficient funds to meet financial obligations within the system as and when expected, although it may be able to do so at some time in the future

[CPSS, Core Principles for Systemically Important Payment Systems]

3.45

message authentication code

MAC

code appended to a message by the originator, which is the result of processing the message through a cryptographic process

NOTE If the receiver can generate the same code, confidence is gained that the message was not modified and that it originated with the holder of the appropriate cryptographic key.

3.46**modification of information**

unauthorized or accidental change in information, whether detected or undetected

3.47**need to know**

security concept that limits access to information and information processing resources to that which is required to perform one's duties

3.48**network**

collection of communication and information processing systems that may be shared among several users

3.49**non-repudiation**

ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

[ISO/IEC 13888-1; ISO 7498-2; ISO/IEC 13335-1:2004, definition 2.16]

3.50**operational risk**

risk that operational factors such as technical malfunctions or operational mistakes will cause or exacerbate credit or liquidity risks

[CPSS, Core Principles for Systemically Important Payment Systems]

3.51**owner of information**

person or function responsible for the collection and maintenance of a given set of information

3.52**password**

string of characters which serves as an authenticator of the user

3.53**prudent business practice**

set of practices which have been generally accepted as necessary

3.54**reliability**

property of consistent intended behaviour and results

[ISO/IEC 13335-1:2004, definition 2.17]

3.55**residual risk**

risk that remains after risk treatment

[ISO/IEC 13335-1:2004, definition 2.18]

3.56**risk**

potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

NOTE It is measured in terms of a combination of the probability of an event and its consequence.

[ISO/IEC 13335-1:2004, definition 3.19]

3.57

risk acceptance

approved risk associated with an exception to the Policy

3.58

risk analysis

systematic process of estimating the magnitude of risks

[ISO/IEC 13335-1:2004, definition 2.20]

3.59

risk assessment

process of combining risk identification, risk analysis and risk evaluation

[ISO/IEC 13335-1:2004, definition 2.21]

3.60

risk evaluation

process of comparing analysed levels of risk against pre-established criteria and identifying areas needing risk treatment

3.61

risk identification

process of identifying risks considering business objectives, threats and vulnerabilities as the basis for further analysis

3.62

risk management

total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect information and communications technology system resources

[ISO/IEC 13335-1:2004, definition 3.22]

3.63

risk treatment

process of selection and implementation of measures to modify risks

3.64

safeguard

practice, procedure or mechanism that treats risk

NOTE The term "safeguard" may be considered synonymous with the term "control".

[ISO/IEC 13335-1:2004, definition 2.24]

3.65

security

quality or state of being protected from unauthorized access or uncontrolled losses or effects

NOTE 1 Absolute security is impossible to achieve in practice, and the quality of a given security system is relative.

NOTE 2 Within a state-model security system, security is a specific "state" to be preserved under various operations.

3.66

server

computer that acts as a provider of some service to other computers, such as processing communications, file storage interface or printing facility

3.67**sign-on**

completion of identification and authentication of a user

3.68**split knowledge**

division of critical information into multiple parts in such a way as to require a minimum number of parts to be present before an action can take place

NOTE Split knowledge is often used to enforce dual control.

3.69**stored value card**

token that is capable of storing and transferring electronic money

3.70**systemic risk**

risk that the inability of one of the participants to meet its obligations, or a disruption of the system itself, could result in the inability of other system participants or of other financial institutions in other parts of the financial system to meet their obligations as they become due

NOTE Such a failure could cause widespread liquidity or credit problems and, as a result, could threaten the stability of the system or of financial markets.

[CPSS, Core Principles for Systemically Important Payment Systems]

3.71**threat**

potential cause of an incident that may result in harm to a system or organization

[ISO/IEC 13335-1:2004, definition 2.25]

3.72**token**

user-controlled device (e.g., disk, smart card, computer file) that contains information that can be used in electronic commerce for authentication or for access control

3.73**user ID**

character string that is used to uniquely identify each user of a system

3.74**vulnerability**

weakness of an asset or group of assets that can be exploited by one or more threats

[ISO/IEC 13335-1:200, definition 2.26]

4 Symbols and abbreviated terms

ATM	Automated Teller Machine
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Corporate Information Security Officer
COO	Chief Operating Officer
CPSS	Committee on Payment and Settlement Systems
CTO	Chief Technology Officer
DMZ	De-Militarized Zone
EFT	Electronic Funds Transfer
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IP	Internet Protocol
IPSEC	IP Security Protocol
IT	Information Technology
LAN	Local Area Network
LEAP	Lightweight Extensible Agent Platform
MAC	Message Authentication Code
OS	Operating System
PC	Personal Computer
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PIN	Personal Identification Number
POTS	Plain Old Telephone System
RF	Radio Frequency
SMTP	Simple Mail Transport Protocol

SSH	Secure Shell
SSL	Secure Socket Layer
USB	Universal Serial Bus
VPN	Virtual Private Network
VTAM	Virtual Terminal Access Method
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WS	Web Services
XML	Extensible Markup Language

5 Corporate information security policy

5.1 Purpose

All financial services institutions today rely heavily on the use of Information Technology (IT) and Information and Communication Technology (ICT), and therefore, need to protect information and to manage the security of their information assets. In order for management to fulfil their responsibilities, information security must be provided, and the management of information security must become an important component of the organization's management plan.

Development of an information security programme is a prudent business practice that will help a financial services organization to identify and manage risk. This Technical Report recommends a general, policy-based approach to information security management, and provides guidance that can be tailored to meet the business objectives of the organization. Business objectives must be supported by policies and procedures for protecting IT assets. A policy-based approach is applicable to different size institutions, different management styles, and organizational environments.

This Technical Report is intended to provide guidance, not specific solutions, on the management aspects of information security, and to assist financial services management in developing and maintaining an information security programme. Other references, especially ISO/IEC 17799, provide important general purpose detailed information that will be invaluable for implementation and maintenance. However, this Technical Report addresses the specific legal and regulatory requirements that must be considered by financial institutions when establishing a policy-based information management programme.

5.2 Legal and regulatory compliance

5.2.1 General

Regulatory authorities concern themselves principally with issues of safety, soundness and compliance with laws and regulations. One element of safety and soundness is the organization's system of safeguards that protects information from unavailability, and unauthorized modification, disclosure and destruction. Recent national and international legislation, such as Basel II, the Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley (GLB)^[22] and European Directive 95/46/EC, has created an environment of legal and regulatory risk for global providers of financial services. The organization's security policy must address this risk.

Compliance officers should work with the CISO, CFO, business managers, risk managers and auditors to ensure that information security requirements derived from national and international laws and regulations are understood and addressed. Compliance officers should also remain current on new technologies or

methodologies that may become subject of regulation; e.g. compliance with predefined functionality classes for Information Technology products.

5.2.2 Requirements for financial institutions

5.2.2.1 Overview

For Institutions in the financial sector there are some legal and regulatory requirements, which have an impact on IT security and have to be followed. The inherent problem is that these requirements differ from country to country. Although the European Union has led the way towards a legal alignment, there are still national regulations which demand specific attention.

In the following, each subclause will describe the most important laws from a perspective of a financial services provider operating in a global environment. A description of the legislative environment will be divided into three sectors: corporate governance, data protection (privacy) and financial sector legislation specific to financial services providers (e.g., money laundering legislation). The description of the regulatory environment will concentrate on financial reporting requirements and the Basel II recommendations, which are freely available from the Bank for International Settlement^[19] in Basle, Switzerland at:

<http://www.bis.org/bcbs/publ.htm>.

5.2.2.2 Legal requirements

5.2.2.2.1 Corporate governance

In recent years, many national and regional legislative bodies have brought forth laws that address corporate governance. Notable among these are the Sarbanes-Oxley (SOX) Act in the United States (U.S.), the Kontrolle- und Transparenz Gesetz (KonTraG) in Germany, and the European Union Draft Directive on Corporate Governance. All three have altered the landscape of legal risks faced by providers of financial services.

The Sarbanes-Oxley Act requires all companies publicly traded on U.S. stock exchanges to provide evidence that they have adequate controls in place for financial reporting. In detail, SOX obliges the CEO and CFO of any such company to assess the effectiveness of their internal control framework and explicitly sign and accept responsibility for the annual financial reports of the organization. With regards to IT, this requires that the operation of critical business applications and their associated risks must be assessed and controlled. In summary, the entire life cycle of these applications must be assessed and controlled, ranging from initial development to business continuity to ensure that adequate measures are in place. Though national in origin, this legislation is applicable to any company whose stocks are publicly traded within the U.S.

The German Kontrolle- und Transparenz Gesetz (KonTraG) legislation requires corporations to implement an internal monitoring process identifying internal developments and decisions that may pose a high risk to this corporation. Implicitly, this means that management has to implement a corporate-wide internal risk management system. It also obliges management to report any identified major risk in their reporting system (bi-annual and annual). With regards to IT, this covers a similar aspect as the Sarbanes-Oxley Act. However, since German publicly traded companies have a two-tier management board, this enforces stronger reporting from the management board to the supervisory board. Non-compliance act may lead to a reduction in the banking rating of the corporation and may therefore influence interest rates for credits.

The European Union (EU) is drafting a directive which will influence EU national legislation: all publicly listed companies are required to publish a corporate governance report. This report will provide details on the Board of Directors, its decisions, its financial situation and its compliance with national law. This report will also include the results of independent audits. This directive has similar implications to the Sarbanes-Oxley Act and Kontrolle- und Transparenz Gesetz (KonTraG) legislation for IT. There are other national laws in place covering this topic but none is so stringent that it would have the influence of an EU Directive.

5.2.2.2.2 Data protection (privacy)

Data protection is gaining more and more attention caused by various laws on the regional, national and state level. This legislation is triggered by the fact that the Internet and its use pose additional risks on misuse in that area and those individuals using this medium need appropriate protection.

The Gramm-Leach-Bliley (GLB) Act is intended to protect consumer information held by financial institutions. It requires these institutions to provide their customers with privacy notices explaining the institutions' information sharing practice. In turn, consumers have the right to limit some – but not all – sharing of their information. The law requires also that financial institutions protect information collected about individuals; it does not apply to information collected in business or commercial activities. The Federal Trade Commission (FTC) has published a set of standards which should be applied to achieve compliance with GLB.

The European Directive 95/46/EC is a joint effort to achieve privacy for all member states at a high level. It protects information of individuals during the whole processing life cycle. Simply spoken, it requires an institution to ask for permission if information is used other than for the officially intended (and stated) use. It also limits the transfer of personal data to those countries where adequate data protection is provided. In general, individuals have to grant permission explicitly (opt-in) to allow further processing. This is contrary to the procedure in the U.S. where individuals are asked to opt out, to prohibit further processing. This directive is implemented into national law within all member states.

The Swiss data protection law is similar to the laws existent in other European countries. It is mentioned here for two reasons: Switzerland is not part of the European Union and therefore it should be mentioned. On the other hand, the Swiss law prohibits the transfer of personal data into other states, if there is no adequate protection and requires the transmitting entity to inform the legal authority on the transfer. Another important law relating to financial institutions is the Swiss Bank Customer Secret (Schweizer Bankkundsgeheimnis), which explicitly protects the customer information maintained by banks.

5.2.2.2.3 Money laundering

Almost all countries have some kind of money laundering legislation which usually means that money transfers exceeding a certain amount have to be examined to verify its sources and destination. As recently as the 1990s such legislation would have had no explicit security relevance for it could be implemented independently of any security issues.

The terrorist attacks of September 11th, 2001 in the United States vividly illuminated the importance of anti-money laundering laws and controls. The attacks fostered an even greater recognition of the importance of anti-money laundering cooperation around the world. This recognition galvanized international cooperation and led to significant modifications to anti-money laundering laws that have paid dividends in the world community's ability to trace the funds of those who finance international terrorism.

Since 2001, the United States has continued its vigorous inter-agency international anti-money laundering training programme to improve worldwide efforts to combat money laundering and financial crime. Other governments and international organizations have also strengthened anti-money laundering programmes. The European Union broadened its anti-money laundering directive and imposed anti-money laundering obligations on "gatekeepers", professionals such as lawyers and accountants who help place dirty money in the financial system. Regional anti-money laundering bodies in Europe, Asia and the Caribbean continued working effectively, and nascent anti-money laundering regional organizations in South America and Africa became operational.

A major money laundering focus of the year was the work of the Financial Action Task Force (FATF), the world's pre-eminent multilateral anti-money laundering body, which continued its non-cooperative countries and territories exercise. FATF moved quickly after 11/9/01 to convene an extraordinary plenary on the financing of terrorism, which decided to expand its mission beyond money laundering, and to focus its energy and expertise on the worldwide effort to combat terrorist financing. The FATF has since adopted eight special recommendations regarding terrorist financing.

The terrorist attacks gave strong impetus to many countries to amend and strengthen their money laundering laws. In the United States, the Uniting and Strengthening America by Providing Appropriate Tools Required to

Intercept and Obstruct Terrorism ("USA PATRIOT") Act of 2001 made major changes to the U.S. anti-money laundering regime. The broad new authorities provided in the USA PATRIOT Act will have significant influence on the relationships between U.S. financial institutions and their individual and institutional customers

An information security management programme can help financial institutions to thwart money laundering schemes. More importantly, these programmes can be used to demonstrate to law enforcement organizations that the institution is compliant with relevant legislation and provide documentation that it is systematically and actively taking measures to comply.

5.2.2.2.4 Financial market legislation

Most of the laws regulating the financial sector primarily define the responsibilities of a financial institution. This includes the obligation to provide qualified services. Some national authorities interpret this in such a way that it covers integrity of IT services used. The following national laws will point out specific IT security issues.

Under the Argentina central banking legislation, a financial institution has to incorporate an Information Security Officer (ISO) who provides an annual report to the Central Bank of Argentina. This report must reflect how the internal controls of the institution are established and maintained to ensure proper services.

European Union Directive 82/121/EEC regulates the reporting of financial institutions. It was recently updated to achieve more regular reporting throughout the European Union. European Union Directive 2000/31/EC (Electronic Commerce) requests a legal framework for electronic commerce, which must include customer privacy issues, spam handling, taxation, electronic contracts and their treatment, confidentiality of communications among others. It also defines a Code of Conduct as a medium to communicate the rights of involved entities.

The German Kreditwesengesetz (KWG) law regulates almost everything specific to financial institutions in Germany. It defines the way banks have to operate, who is allowed to lead a financial institution, what is to be reported, etc. Of special interest are three paragraphs. The first one deals with automated access to customer data by the financial authorities (§ 24c) which requires additional security measures in place. The second one (§ 25a) defines the specific obligations a financial institution has to fulfil which covers issues like internal risk management, security measures and internal audit and its cooperation with the overseeing authorities. Finally, there are regulations for if a financial institution or its management do not fulfil their obligations possibly leading to that management losing its right to conduct business in the financial sector.

5.2.2.3 Regulatory requirements

There are two financial institution regulatory requirement topics of high relevance. The first concerns the obligations of the institution for financial reporting (usually overseen by national financial authorities). The second is the financial soundness obligation which is described in the Bank for International Settlement (BIS - see <http://www.bis.org/bcbs/index.htm>) Basel II accords. These requirements include the need for the institution to consider operational risks.

The Basel Committee on Banking Supervision formulates broad supervisory standards, guidelines and best practice recommendations. The committee expects individual national financial authorities to take steps to implement these recommendations through detailed arrangements – statutory or otherwise – in a manner that best suits their own national systems. Regulatory requirements lead to the need to audit institutions. In order to limit the disruptions that audits cause to normal business operations, institutions should put systems in place (internal audit, information security management, etc.) that can easily provide regulators with what they need to examine to be assured that the institution is compliant.

Each financial institution must interpret "operational risk" in terms of its own business activities and identify the risks that it is exposed to. An analysis of operational risks should include fraud and criminal activities, systems failures, human errors, natural disasters and acts of terrorism. The tsunami that caused widespread death and destruction throughout Asia in December 2004 and the September eleventh terrorist attacks in 2001 that targeted the financial services industry in New York City are both examples of extremely low probability events. But such events do happen and must be planned for.

Basel II enforces the need for an institution to perform a systematic risk analysis. Both qualitative and quantitative techniques for managing contingencies should be utilized, and the selection of controls for an individual business unit should be based on a cost benefit analysis that considers the likelihood of a contingency, its probable frequency, and the projected loss and impact on business operations should an event occur.

Note that there is a distinction between banking supervision to ensure a bank's financial health and bank oversight, which considers the institutions systems in terms of operational risk. This oversight is based not on Basel II but on the BIS Core Principles (see <http://www.bis.org/publ/bcbs49b.pdf>), which are aimed at systemically important payment systems. Those payment systems which are classified as having "systemic importance" to the health and normal operations of financial markets must meet all ten of the Core Principles. "Prominent systems" have only to meet at least seven. For other payment systems, requirements to meet the core principles vary, but institutions may use their compliance as a selling point, as compliance is viewed as a measure of quality.

5.3 Development

After establishing the information security objectives of the organization, and assessing the impact of regulations and legislation, a plan of action should be developed that is consistent with the established business objectives. This plan should be used as the roadmap for the development of a corporate information security policy (Policy)¹⁾.

It is essential that a corporation develop a Policy and that it take into account the corporate objectives and particular aspects of the organization. The security policy must be consistent with the corporate business, culture, and the regulatory and legislative environment in which the business operates. The development of a Policy is essential to ensure that the results of the risk management process of the security programme are appropriate and effective. Management support across the organization is required for the development and effective implementation of the Policy. With the alignment of security policy to corporate business objectives, the Policy will help to achieve the most effective use of resources, and will ensure a consistent approach to security across a range of different information system environments.

5.4 Documentation hierarchy

5.4.1 Overview

5.4.1.1 General

Three levels of information security programme documentation are described in this guideline. These are the corporate information security policy (Policy) document, the security practice documents and the operational security procedures documents²⁾. The documentation hierarchy and the meaning of each level are illustrated in Figure 1.

1) Throughout this document, "Policy" is synonymous with "corporate information security policy".

2) This nomenclature and hierarchy are not definitive. Organizations may use more levels of hierarchy and different nomenclature.

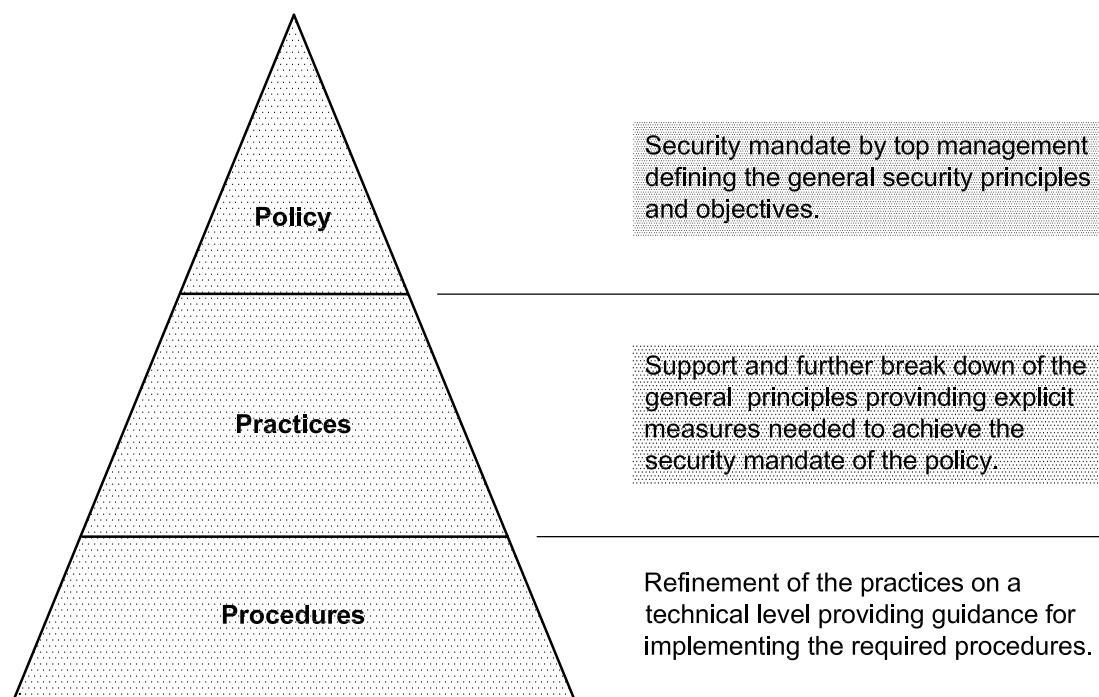


Figure 1 — Programme documentation

The information security documents should range from the high level organizational goals down to the specific security settings of devices that implement the security policy. This range of general and specific information is best covered in multiple layers of documentation. The number of levels should be kept to a minimum, and this guideline recommends three: a Policy document, security practice documents, and operational security procedures documents.

Additional documents will be required as new and emerging technology is introduced into the organization. While the Policy document will often be a single page, the procedures documentation may consist of many multi-page documents representing separate, specific environments, business units, and policy issues within the organization. In some cases, a single, well-bounded system may also have its own practices document. All practices and procedures should flow from the higher level to the detailed level, maintaining a consistency with corporate risk assessments and the overall Policy.

5.4.1.2 Corporate information security policy

The Policy document is the smallest of all of the documents in the information security programme document hierarchy. Typically, the Policy is documented in a few paragraphs explaining that management regards information in any form as a valuable corporate resource that must be protected. The Policy should be broad in scope and stated as simply and concisely as possible, but should provide specific information of the assets to be protected, e.g., customer data, employee records, partner agreements and processes. For example, a very simple Policy document might contain the single assertion, *“The confidentiality, availability, and integrity of all corporate information assets must be protected by appropriate security controls”*.

The Policy document is an abstract document, comprehensive in scope, and the most influential of the information security programme documents in its effects on the organization. Only a single instance of the Policy document should exist at any given time, and it should be promulgated throughout the organization. It should be signed by the board members involved in Information security, e.g. the Chief Executive Officer (CEO) and the Chief Information Officer (CIO).

The Policy document should be public in nature, widely distributed and made available to all of the organization's stakeholders. It should stress that protecting and providing information assets is the responsibility of management and all employees, and that management at the highest level is committed to security education and awareness.

It should be clear to all stakeholders that the Policy document derives its authority directly from the corporate officers and board-level personnel. The document should state the intention of the organization to operate in accordance with relevant local and international legal and regulatory strictures, and to base their information security programme on sound principals and practices recognized in national and international security standards.

The Policy document should be almost immutable. It should change only as required by shifts in strategic goals, changes in perceived business risk, or events affecting the regulatory and legal environment in which the organization operates. Corporate officers and board-level personnel should dictate the change control parameters and procedures.

5.4.1.3 Representation

When developing the Policy, representatives from a variety of functions should participate. The development group should include members of the board of directors, executive officers, legal representation, risk management committee and audit committee members. In formulation of the policy, the development group will obtain input from experts throughout the enterprise, e.g. information technology, physical security and finance functions.

5.4.1.4 Information classification

One aspect of implementing the Policy is the classification of information. Much like the military systems of "Top Secret", "Secret" and "Unclassified", financial organizations have information with differing values. The results of information asset classification will indicate when a good, better or best control should be implemented. There are many types of classification system. For the financial organization, the important point is to define classification levels and leverage the classification of the information in making risk acceptance decisions. For example, a risk that is acceptable for public information would likely be unacceptable for highly classified information. One benefit of classifying information is to communicate management's expectation of how employees should handle the information. If a document, file or database contains information at various classification levels, it must be treated according to the procedures established for the highest classification level of information it contains.

It is important to note that the classification level of information may change during its useful life. These changes should be controlled under the Policy of the organization.

5.4.2 Security practice documents

Security practice documents are derived from the content of the Policy document. These documents specify the general security standards that should be followed by the organization. They mirror the intentions and goals established by the highest levels of management in creating the information security programme, and document the intention to implement the Policy in a technology-independent way. Each security practice document is narrower in scope than the Policy document. Each practice document is a technology-neutral and content statement of the organization's security requirements. The size of a given practice document is variable and topic-dependant.

The number of practice documents should be kept to a minimum. The number of documents needed varies with the size of an organization and its business needs, and with the scope and complexity of the organization's activities. The legal and regulatory environment that affects the organization can also influence the number of practice documents needed.

A practice document is not public³⁾. It is general purpose in nature, and technology-neutral. It is less abstract than a Policy document, and may have less influence on the overall organization, since it may be applied only to some aspects of the organization. For example, a very simple practice document might contain the simple assertion:

3) There may be occasion to furnish a practice document to regulators.

“Access to Corporate information assets must be authenticated in a manner commensurate with the sensitivity of the asset. Two-factor authentication is the minimum acceptable level of authentication; assets classified ‘Confidential’ by the asset owner should be accessible only with three-factor⁴⁾ authentication. Two-factor (biometric and password-based) access control systems must enforce the following regulations...”

Though practice documents derive their authority from, and must strictly comply with, the Policy, they are more mutable than policy documents. This is because they are subject to changes that are more frequent, arising as new risks and controls are identified. Each practice document has a restricted audience, as it usually affects a specific part of an organization or business unit, does not affect the overall security management programme of the organization.

It is helpful to include a document scope section that indicates the audience and owner of each practice document. The owner of a practice might be a business manager, an IT manager or an operations manager. It is also helpful to include how information related to a given practice is classified, as the category of classification indicates the level of protection the information requires.

5.4.3 Operational security procedures documents

Operational security procedures documents are derived from one or more security practice documents. Their lengths vary with the topic and complexity of the procedures. These documents are the narrowest in scope of all of the documents in the document hierarchy. They are technology-specific expressions of how the Policy is implemented. These are applied to actual business systems, and vendor-specific product details are covered in platform-dependent documentation.

There should be as many procedures documents as necessary, but care should be taken when developing the documents that they are complete, accurate and appropriate and that none of them contradicts any other practice or Policy. An example of the type of guidance to be found in a very simple procedures document might be one that contains the instructions:

“Use the ‘*pwadmin*’ command to ensure that user passwords meet the criteria established in the Corporate Access Control and Authentication Practice document. Issue the following commands ...”

Procedures documents must comply with the overall Policy of the organization and the practices that the procedures are based on. No procedure document should contradict any policy-based practice. Regulatory restrictions, externally produced standards, and other procedural documents must be taken into account.

The procedures documents should include results of previous security risk analysis and management reviews including identification of any residual risks, results of follow-up actions such as security compliance checking of implemented controls, a list of actions to be taken to monitor and review information security in day to day use, and reports of security relevant incidents.

6 Management of information security — Security programme

6.1 General

Implementing the Policy requires an information security programme. At the highest level, the ethical values and control imperatives of corporate management must be communicated and periodically reinforced with management and staff. Information security is a team-based process as well as an individual responsibility. Developing, maintaining, improving and monitoring an information security programme requires participation by multiple disciplines in the organization. Close coordination is required between the business managers and

4) The term “three-factor” is often expressed by the phrase “what you have, what you know and what you are”. What you have may be a card or token. What you know may be a PIN or pass phrase. And a biometric is used to represent what you are.