TECHNICAL REPORT

ISO/TR 13569

Third edition
2005-11-15

Financial services — Information security guidelines

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

Reference number
ISO/TR 13569:2005(E)

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

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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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.

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]