Rahandusteenused. Infoturbe suunised

Financial services — Information security guidelines

EESTI STANDARDIKESKUS
ESTONIAN CENTRE FOR STANDARDISATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

Käesolev Eesti standard EVS-ISO/TR 13569:2006 sisaldab rahvusvahelise standardi ISO/TR 13569:2005 ingliskeelset teksti.	This Estonian standard EVS-ISO/TR 13569:2006 consists of the English text of the international standard ISO/TR 13569:2005.
Standard on kinnitatud Eesti Standardikeskuse 15.12.2006 käskkirjaga ja jõustub sellekohase teate avaldamisel EVS Teatajas.	This standard is ratified with the order of Estonian Centre for Standardisation dated 15.12.2006 and is endorsed with the notification published in the official bulletin of the Estonian national standardisation organisation.
Standard on kättesaadav Eesti standardiorganisatsioonist.	The standard is available from Estonian standardisation organisation.

ICS 03.060

Võtmesõnad: infoturve, rahandusteenused

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*