TECHNICAL REPORT

ISO/IEC TR 27015

First edition
2012-12-01

Information technology — Security techniques — Information security management guidelines for financial services

Technologies de l'information — Techniques de sécurité — Lignes directrices pour le management de la sécurité de l'information pour les services financiers

Reference number
ISO/IEC TR 27015:2012(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is entirely informative in nature and does not have to be reviewed until the data it provides are considered to be no longer valid or useful.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/IEC TR 27015 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee 27, *IT Security techniques*.

Introduction

Continuous developments in information technology have led to an increased reliance by organizations providing financial services on their assets processing information. Consequently, management, customers and regulators have heightened expectations regarding an effective information security protection of these assets and of processed information.

Whereas ISO/IEC 27001:2005 and ISO/IEC 27002:2005 address information security management and controls, they do so in a generalised form.

Organizations providing financial services have specific information security needs and constraints within their respective organization or while performing financial transactions with business partners, which require a high level of reliance between involved stakeholders.

This technical report is a supplement to ISO/IEC 27000 family of International Standards for use by organizations providing financial services. In particular, the guidance contained in this technical report complements and is in addition to information security controls defined in ISO/IEC 27002:2005.

The term “financial services” should be understood as services in the management, investment, transfer, or lending of money which could be provided by organizations offering their fiscal expertise rather than selling physical products (i.e. anyone in the “business of money”).

In addition to the implementation of both ISO/IEC 27001:2005 and ISO/IEC 27002:2005, by using this technical report, organizations providing financial services may establish a higher level of trust within their organization, with customers and with business partners, in particular, when it can be demonstrated that they have adopted sector-specific guidance for information security management.

This technical report reflects the state of art and is not intended for certification purposes.

Information technology — Security techniques — Information security management guidelines for financial services

1 Scope

This Technical Report provides information security guidance complementing and in addition to information security controls defined in ISO/IEC 27002:2005 for initiating, implementing, maintaining, and improving information security within organizations providing financial services.

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/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 27000:2009 and the following apply.

3.1.1
financial services
services in the management, investment, transfer, or lending of money

3.2 Abbreviated terms

ATM	Automatic Teller Machines
COBIT	Control Objectives for Information Technology
OTP	One-Time Password
PCI-DSS	Payment Card Industry - Data Security Standard
POS	Point Of Sale
SST	Self Service Terminal

4 Structure of this technical report

Information security guidance complementing and in addition to information security controls from ISO/IEC 27002:2005 is provided in clauses 5 to 15 below.

5 Security Policy

No additional guidance for organizations providing financial services.

6 Organization of information security

6.1 Internal organization

6.1.1 Management commitment to information security

No additional guidance for organizations providing financial services.

6.1.2 Information security co-ordination

No additional guidance for organizations providing financial services.

6.1.3 Allocation of information security responsibilities

Control 6.1.3 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

An organization providing financial services should consider the following in the definition of information security roles and responsibilities requirements and recommendations stated by laws and regulations, which applied to it, along with industry frameworks.

Care should also be taken by an organization providing financial services to ensure local implementation of relevant requirements and recommendations stated by international partners in regards to its definition of information security roles and responsibilities.

Examples of frameworks which are generally used by organizations providing financial services and which provide information about allocation of information security roles and responsibilities:

a) PCI-DSS [1] with the following sub-clause:

   1. PCI 12.5 Assigned information security management responsibilities.

b) COBIT [2] with following sub-clauses:

   2. 4.0 Define the IT organization and relationships.

   3. 4.4 Roles and Responsibilities.

   4. 4.6 Responsibility for Logical and Physical Security.

Assigned information security roles and responsibilities should be reviewed on a regular basis to ensure conformity with changes in requirements and recommendations stated by laws, regulations, industry frameworks and partners.

6.1.4 Authorization process for information processing facilities

No additional guidance for organizations providing financial services.

6.1.5 Confidentiality agreements

No additional guidance for organizations providing financial services.

6.1.6 Contact with authorities

No additional guidance for organizations providing financial services.

6.1.7 Contact with special interest groups

Control 6.1.7 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

In addition to the guidance provided in ISO/IEC 27002, membership in special interest groups or forums should be considered as a means to:

a) confidentially share and exchange information about recent fraudulent and criminal activities.

6.1.8 Independent review of information security

No additional guidance for organizations providing financial services.

6.2 External parties

6.2.1 Identification of risks related to external parties

Control 6.2.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

In addition to the guidance provided in ISO/IEC 27002, the following issue should also be considered by an organization providing financial services when identifying risks related to external party access:

a) Legal and regulatory requirements, along with contractual obligations which could be imposed to the external party located in foreign countries and which could result in customer and financial information disclosure to third parties (e.g. mother organization, affiliate, or public authority) without prior notification to the organization. This issue could then induce significant security breaches with the unauthorized disclosure of this information.

6.2.2 Addressing security when dealing with customers

Control 6.2.2 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

In addition to the guidance provided in ISO/IEC 27002, the following principles should be considered to address security when dealing with customers:

a) The organization should give information security advice to customers to raise awareness around threats (e.g. Trojans, phishing, fraudulent calls) which may introduce information security risks for them.

   This advice should be tailored towards the customer needs and the right level of technical communication needs to be chosen in order to ensure customer awareness is effective.

   The organization should regularly review information security advice provided to customers to ensure that it remains adequate and appropriate to the organization's risk profile and it addresses new information security threats.

   Examples of information security advice given would typically include: