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 ..... vi

Introduction ..... vii

1 Scope ..... 1

2 Normative references ..... 1

3 Terms, definitions and abbreviated terms ..... 1
3.1 Terms and definitions ..... 1
3.2 Abbreviated terms ..... 1

4 Structure of this technical report ..... 1

5 Security Policy ..... 2

6 Organization of information security ..... 2
6.1 Internal organization ..... 2
6.1.1 Management commitment to information security ..... 2
6.1.2 Information security co-ordination ..... 2
6.1.3 Allocation of information security responsibilities ..... 2
6.1.4 Authorization process for information processing facilities ..... 2
6.1.5 Confidentiality agreements ..... 2
6.1.6 Contact with authorities ..... 3
6.1.7 Contact with special interest groups ..... 3
6.1.8 Independent review of information security ..... 3
6.2 External parties ..... 3
6.2.1 Identification of risks related to external parties ..... 3
6.2.2 Addressing security when dealing with customers ..... 3
6.2.3 Addressing security in third party agreements ..... 5

7 Asset management ..... 6
7.1 Responsibility for assets ..... 6
7.1.1 Inventory of assets ..... 6
7.1.2 Ownership of assets ..... 6
7.1.3 Acceptable use of assets ..... 6
7.2 Information classification ..... 7

8 Human resources security ..... 7
8.1 Prior to employment ..... 7
8.1.1 Roles and responsibilities ..... 7
8.1.2 Screening ..... 7
8.1.3 erms and conditions of employment ..... 7
8.2 During employment ..... 8
8.2.1 Management responsibilities ..... 8
8.2.2 Information security awareness, education and training ..... 8
8.3 Termination or change of employment ..... 8

9 Physical and environmental security ..... 8
9.1 Secure areas ..... 8
9.1.1 Physical security perimeter ..... 8
9.1.2 Physical entry controls ..... 8
9.1.3 Securing offices, rooms, and facilities ..... 8
9.1.4 Protecting against external and environmental threats ..... 8
9.1.5 Working in secure areas ..... 8
9.1.6 Public access, delivery, and loading areas ..... 9
9.2 Equipment security ..... 9

9.2.1 Equipment siting and protection ..... 9
9.2.2 Supporting utilities ..... 9
9.2.3 Cabling security ..... 9
9.2.4 Equipment maintenance ..... 9
9.2.5 Security of equipment off-premises ..... 9
9.2.6 Secure disposal or re-use of equipment ..... 9

10 Communications and operations management ..... 10
10.1 Operational procedures and responsibilities ..... 10
10.1.1 Documented operating procedures ..... 10
10.1.2 Change management ..... 10
10.1.3 1Segregation of duties ..... 10
10.1.4 Separation of development, test, and operational facilities ..... 10
10.2 Third party service delivery management ..... 10
10.3 System planning and acceptance ..... 10
10.3.1 Capacity management ..... 10
10.3.2 System acceptance ..... 11
10.4 Protection against malicious and mobile code ..... 11
10.4.1 Controls against malicious code ..... 11
10.4.2 Controls against mobile code ..... 11
10.5 Back-up ..... 11
10.6 Network security management ..... 11
10.7 Media handling ..... 11
10.7.1 Management of removable media ..... 11
10.7.2 Disposal of media ..... 11
10.7.3 Information handling procedures ..... 11
10.7.4 Security of system documentation ..... 12
10.8 Exchange of information ..... 12
10.9 Electronic commerce services ..... 12
10.9.1 Electronic commerce ..... 12
10.9.2 On-Line Transactions ..... 12
10.9.3 Publicly available information ..... 12
10.9.4 Internet banking services ..... 12
10.10 Monitoring ..... 13
10.10.1 Audit logging ..... 13
10.10.2 Monitoring system use ..... 13
10.10.3 Protection of log information ..... 13
10.10.4 Administrator and operator logs ..... 13
10.10.5 Fault logging ..... 13
10.10.6 Clock synchronization ..... 13

11 Access control ..... 13

12 Information systems acquisition, development and maintenance ..... 14
12.1 Security requirements of information systems ..... 14
12.1.1 Security requirements analysis and specification ..... 14
12.2 Correct processing in applications ..... 14
12.3 Cryptographic controls ..... 15
12.3.1 Policy on the use of cryptographic controls ..... 15
12.3.2 Key management ..... 15
12.4 Security of system files ..... 15
12.4.1 Control of operational software ..... 15
12.4.2 Protection of system test data ..... 15
12.4.3 Access control to program source code ..... 15
12.5 Security in development and support processes ..... 16
12.6 Technical Vulnerability Management ..... 16

13 Information security incident management ..... 16

14 Business continuity management ..... 16
14.1 Information security aspects of business continuity management ..... 16
14.1.1 Including information security in the business continuity management process ..... 16



 

14.1.2 Business continuity and risk assessment ..... 16
14.1.3 Developing and implementing continuity plans including information security ..... 16
14.1.4 Business continuity planning framework ..... 16
14.1.5 Testing, maintaining and re-assessing business continuity plans ..... 17
15 Compliance ..... 17
15.1 Compliance with legal requirements ..... 17
15.2 Compliance with security policies and standards, and technical compliance ..... 17
15.2.1 Compliance with security policies and standards ..... 17
15.2.2 Technical compliance checking ..... 17
15.2.3 Compliance monitoring ..... 17
Bibliography ..... 18

## 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.