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.

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:

1. Applying appropriate controls (e.g. password protection, antivirus) for securing personal computers and other devices used to access internet banking services.

2. Not disclosing customer and financial information (e.g. payment card number) unnecessarily or where the integrity of the recipient is suspect.

3. Securely destroying expired or unusable payment cards.

   Examples of recommendations which could be provided to the customer:

   a. Correct cutting of the payment card.

   b. Using a shredder for destroying the payment card.

   c. Being sure to have destroyed the chip and the magnetic stripe of the payment card.

   d. Using several dustbins located in different places to throw away card pieces.

   e. Avoiding using recycling bins to throw away card pieces, because of potential human interventions at the recycling center.

4. When conducting banking activities, taking safeguards to ensure no one else is able to observe or access user credentials or other IT security information.

5. Using secure authentication mechanisms such as adopting strong passwords, PIN codes or two-factor authentication where available.

6. Avoiding using the same password for accessing internet banking services provided by different organizations.

7. Avoiding using the same PIN code for all payment cards.

8. Reminding customers that the organization will not make unsolicited requests for authentication information (e.g. password, PIN code).

9. Informing customers to monitor account transactions and balances on a regular basis.

10. Notifying the customer on the process to follow if he or she suspects to have been the victim of fraud or identity theft (including attempts thereof).

To help reduce the risk of being targeted for the perpetration of fraud, the organization may find it beneficial to compare customer advice with its peers and with the financial services industry community more broadly, on a regular basis.

b) The organization should inform customers of:

1. A dedicated security contact point where customers can address any information security issues or concerns they may have in regards to the use of financial services provided by the organization.

2. Actions that need to be taken if their user authentication information (e.g. password, PIN code) has been compromised, even if this happened through their fault.

3. The manner to report unexpected events while attempting to access financial services provided by the organization.

c) The organization should consider the followings when establishing an on-line transactions system (e.g. internet banking) to customers:

1. Terms and conditions for on-line transaction system usage. Care should be particularly taken to define legal recognition of performed transactions along with provisions.

2. A clear statement regarding roles and responsibilities as well as liabilities which apply to the organization and the customer.

3. A clear statement regarding privacy and usage monitoring, including fraud-monitoring, of the on-line transaction system, by means of protecting both the customer and the organization's interests.

4. The allocation of access rights based on following principles:

   a. Know your customer: this principle is used by regulators to express their attitude to financial institutions from the standpoint of the knowledge of the activities of their customers.

   b. Need to know: this principle limits the powers to access information and resources relating to the processing of information to the level barely necessary for the fulfilment of certain activities.

   c. Dual control: this is the principle of preserving process integrity and combating distortions of the functions of the system requiring the (algorithmic, time, resource and other) backing up of actions until the completion of certain transactions.

5. The establishment of the following:

   a. Strong user authentication methods (e.g. OTP token, user certificate).

   b. Verification systems for ensuring the validity of presented user credentials and devices.

   c. Verification of the recognition level of certificate authorities.

6. A user identifier uniquely assigned to each customer.

7. Notification mechanisms to inform customers (on a regular basis, continuously or on request) about all operations conducted on their behalf.

Other information

Whilst customers of many industries or service providers may be considered stakeholders to a business, in the context of financial services the organization has in general a duty of care to advise its customers of appropriate protection measures. If a breach or loss were to occur, the organization would risk being damaged, either financially or by reputation.

6.2.3 Addressing security in third party agreements

Control 6.2.3 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

In addition to the guidance provided in ISO/IEC 27002, the following should be considered in a supplier agreement if the scope relates to financial services provided by an organization:

a) A clear contact point authorized to handle enquiries from the organization.

b) Provision for the property of records which may be generated by the supplier during the supplier agreement execution.

c) Timely notification of security changes within supplier assets supporting the delivery of organization’s financial services.

d) The assurance that organization’s information available to the supplier will be processed solely within the terms and conditions specified in the agreement.

e) The assurance that changes of subcontractors or storage location of processed organization’s information (e.g. offshoring) will be notified to the organization and may be subject to prior approval by the organization, particularly when it involves processing organization’s information.

f) The assurance that incidents which arise during the supplier agreement execution will be reported to the organization in a timely manner and that appropriate investigations will be performed by the supplier.

g) The involvement of the supplier in case an incident or a suspicious event may go beyond the borders of the organization. Care should be taken to ensure supplier reactivity in this domain for being able for example to monitor or cancel a financial transaction distributed among several organizations in case there is a doubt in its legitimacy.

h) The right to:

   a. Audit subcontractors to the same level defined for the supplier.

   b. Access to the supplier information and operations and its subcontractors by the organization’s regulators.

7 Asset management

7.1 Responsibility for assets

7.1.1 Inventory of assets

Control 7.1.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Care should be taken by the organization to ensure that:

a) Specific assets used in the context of providing financial services, such as payment devices (ATM, SST, POS), payment cards (debit, credit, prepaid) and interbanking systems stored on and off-site are included in its assets inventory.

b) The payment cards inventory held by a supplier (such as a payment service provider approving payments performed with payment cards issued by the organization and on behalf of it) is accurate at any time and contains the correct status (validated, revoked) of issued payment cards to avoid the processing of payments performed with an unauthorized payment card.

7.1.2 Ownership of assets

No additional guidance for organizations providing financial services.

7.1.3 Acceptable use of assets

Control 7.1.3 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

An organization providing financial services should also ensure that rules addressing the handling and the disposal of uniforms and any other such branded items, including pre-printed forms, are established to avoid their unauthorized use to commit fraud or criminal activity.

7.2 Information classification

No additional guidance for organizations providing financial services.

8 Human resources security

8.1 Prior to employment

8.1.1 Roles and responsibilities

No additional guidance for organizations providing financial services.

8.1.2 Screening

Control 8.1.2 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

An organization providing financial services needs to be aware that organized crime may place personnel in key business processes.

In particular, care should be given to certain functions, such as the following, by ensuring that more detailed criminal and background checks have been performed, where permissible by law:

a) All personnel having access to customer and financial information (e.g. payment card information, customer passwords, PIN codes).

b) System administrators responsible for processing customer and financial information.

c) Security custodians responsible for the management of cryptographic keys used for following purposes:

   1. Customer and financial information transmission and storage.

   2. Financial transaction’s authenticity.

   3. Customer passwords, PIN codes or two-factor authentication management.

8.1.3 Terms and conditions of employment

Control 8.1.3 from ISO/IEC 27002:2005 is enhanced as follows:

Implementation guidance

The terms and conditions of employment should also incorporate a vacation policy applied to the organization and suppliers personnel who perform sensitive financial activities.

As anti-fraud measure the vacation policy should enforce a minimum period of leave (e.g. 10 consecutive working days each calendar year) in order to ensure that sensitive financial activities are not always performed solely by the same person.

8.2 During employment

8.2.1 Management responsibilities

No additional guidance for organizations providing financial services.

8.2.2 Information security awareness, education and training

Control 8.2.2 from ISO/IEC 27002:2005 is enhanced as follows:

Implementation guidance

The organization providing financial services should take into account that laws and regulations applicable to it, along with statements from regulators, require specific issues (such as telephone usage for disseminating customer and financial information, anti-money laundering program) to be addressed within the security awareness and training activities applied to the organization.

The information security awareness should also address specific topics such as social engineering, phishing, online vectors of attack, cards system skimming and software malware.

8.3 Termination or change of employment

No additional guidance for organizations providing financial services.

9 Physical and environmental security

9.1 Secure areas

9.1.1 Physical security perimeter

No additional guidance for organizations providing financial services.

9.1.2 Physical entry controls

No additional guidance for organizations providing financial services.

9.1.3 Securing offices, rooms, and facilities

No additional guidance for organizations providing financial services.

9.1.4 Protecting against external and environmental threats

No additional guidance for organizations providing financial services.

9.1.5 Working in secure areas

Control 9.1.5 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Care should be taken to ensure that the use of mobile devices is particularly restricted in key business processing areas, where payment card number or other customer information is available or processed, to prevent unauthorized records or transfer of this information.

9.1.6 Public access, delivery, and loading areas

No additional guidance for organizations providing financial services.

9.2 Equipment security

9.2.1 Equipment siting and protection

Control 9.2.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Care should be taken to protect payment devices (e.g. ATM, SST, POS) located outside the organization premises and processing customer and financial information or material assets against unauthorized modification, opening and theft. Implemented security measures should include, as examples, constructed chassis and fixation, auto-destruction mechanism as well as protection of any cabling.

9.2.2 Supporting utilities

No additional guidance for organizations providing financial services.

9.2.3 Cabling security

No additional guidance for organizations providing financial services.

9.2.4 Equipment maintenance

Control 9.2.4 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

In addition to the guidance provided in ISO/IEC 27002, the organization should also consider establishing dual control for maintenance of payment devices (e.g. ATM, SST, POS).

9.2.5 Security of equipment off-premises

No additional guidance for organizations providing financial services.

9.2.6 Secure disposal or re-use of equipment

Control 9.2.6 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Care should be taken to ensure that customer and financial information stored in memory components (e.g. ATM, SST, hard disks, POS internal memories) of payment devices is securely destroyed, deleted or overwritten prior to disposal.

9.2.7 Removal of property

No additional guidance for organizations providing financial services.

10 Communications and operations management

10.1 Operational procedures and responsibilities

10.1.1 Documented operating procedures

No additional guidance for organizations providing financial services.

10.1.2 Change management

No additional guidance for organizations providing financial services.

10.1.3 1Segregation of duties

Control 10.1.3 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Segregation of duties should be applied within the scope of financial transactions systems to ensure that not only the initiation of an event, such as a financial transaction, is separated from its processing or its authorization but that this initiation is also separated from its verification.

The organization should at a minimum ensure a dual control in financial transactions management, i.e. that the processing of financial information or transaction and the verification of the outcome are performed by different personnel or automated processes.

10.1.4 Separation of development, test, and operational facilities

No additional guidance for organizations providing financial services.

10.2 Third party service delivery management

No additional guidance for organizations providing financial services.

10.3 System planning and acceptance

10.3.1 Capacity management

Control 10.3.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Care should be taken to ensure that capacity requirements are defined for following assets which have been implemented or which are planned to be deployed:

a) Internet banking services, based on the consideration of following business requirements:

1. Current and expected number of transactions.
2. Current and expected peak periods and spikes in transactions.
3. Current number of customers.
4. Expected growth in the number of customers.

5. Assurance of the availability of internet banking services even in times with high access rates of customers.

b) Payment devices (e.g. ATM, SST, POS) processing customer and financial information

10.3.2 System acceptance

No additional guidance for organizations providing financial services.

10.4 Protection against malicious and mobile code

10.4.1 Controls against malicious code

Control 10.4.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Checks carried out by malicious code detection and repair software should include payment devices (e.g. ATM, SST, POS) processing customer and financial information that are often considered less impacted by malicious codes.

10.4.2 Controls against mobile code

No additional guidance for organizations providing financial services.

10.5 Back-up

No additional guidance for organizations providing financial services.

10.6 Network security management

No additional guidance for organizations providing financial services.

10.7 Media handling

10.7.1 Management of removable media

No additional guidance for organizations providing financial services.

10.7.2 Disposal of media

Control 10.7.2 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Care should be taken to ensure that secure disposal procedures are in place for all types of assets processing customer and financial information (e.g. payment card information, customer passwords, PIN codes), along with specific assets used for the payment cards production, such as ribbons.

10.7.3 Information handling procedures

Control 10.7.3 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

The organization should also ensure that information handling procedures address the handling and the disposal of cheque and deposit books, cheques and payment cards (debit, credit, prepaid) and other printed stationary.

10.7.4 Security of system documentation

No additional guidance for organizations providing financial services.

10.8 Exchange of information

No additional guidance for organizations providing financial services.

10.9 Electronic commerce services

10.9.1 Electronic commerce

No additional guidance for organizations providing financial services.

10.9.2 On-Line Transactions

No additional guidance for organizations providing financial services.

10.9.3 Publicly available information

No additional guidance for organizations providing financial services.

10.9.4 Internet banking services

<u>Control</u>

Internet banking services should be protected from unauthorized access and modification to prevent unauthorized customer and financial information disclosure and financial transactions.

<u>Implementation guidance</u>

The organization should include following security considerations for protecting internet banking services:

a) Notification to the customer of the internet banking services activation using a previously established communication channel and media, such as bank statements printed on paper.

b) Preventive financial limitations, e.g. interbank limit, discretionary limit.

c) Separated user credentials for joint account holders with associated privileges reflecting preliminary defined power of signatures.

d) Limited disclosure of customer and financial information, such as user identifier, name and account numbers except for valid business purposes and actions carried out by the customer.

e) Approval of customer actions only if they have been submitted during the same user session with no disruption or disconnection. In case of user session disruption or disconnection, user authentication requirements should be again applied to the customer accessing to internet banking services.

<u>Other information</u>

Information systems hosting customers web interface for internet banking services should not store or process customers and financial information to reduce the risk of information breaches if they are compromised.

10.10 Monitoring

10.10.1 Audit logging

No additional guidance for organizations providing financial services.

10.10.2 Monitoring system use

Control 10.10.2 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

In addition to the areas provided in ISO/IEC 27002 for individual facilities monitoring activities, the following areas should also be considered:

a) Unusual events related to customer and financial information, along with transactions performed by customers, such as:

   1. Unusual transactions (e.g. money transfer to an unknown bank account in a foreign jurisdiction).

   2. User actions outside of standard usage hours.

   3. User actions executed with an abnormal speed for detecting non-human interventions.

   4. User actions skipping standard activities within the on-line transactions process.

   5. Duplicated user sessions.

10.10.3 Protection of log information

No additional guidance for organizations providing financial services.

10.10.4 Administrator and operator logs

No additional guidance for organizations providing financial services.

10.10.5 Fault logging

No additional guidance for organizations providing financial services.

10.10.6 Clock synchronization

No additional guidance for organizations providing financial services.

11 Access control

No additional guidance for organizations providing financial services.

12 Information systems acquisition, development and maintenance

12.1 Security requirements of information systems

12.1.1 Security requirements analysis and specification

Control 12.1.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

The organization should consider following security requirements when designing a new financial transactions system or when performing changes to an existing one:

a) The protection of financial transactions information from unauthorized distortion, falsification, readdressing and destruction.

b) The recovery of financial transactions information in case of unauthorized distortion, falsification, readdressing or destruction.

c) Automated compliance checks when initiating, processing, transmitting and storing financial transactions.

d) Possibility of tracking possible fraudulent financial transactions back to the originator.

e) Authentication of the following:

   1. Automated clients (workstations and servers) and participants involved in the exchange of financial transactions.

   2. Incoming and outgoing electronic payment messages.

f) Delivery of electronic payment messages to participants involved in the exchange of financial transactions.

g) Reconciliation of outgoing electronic payment messages with the corresponding incoming and processed electronic payment messages in interbank settlements.

h) User authentication for accessing to sensitive parameters or performing sensitive actions, such as double entry, reconciliation, setting limits of the value of financial operations.

i) Segregation of duties over transactions flows and disbursement approvals.

12.2 Correct processing in applications

No additional guidance for organizations providing financial services.

12.3 Cryptographic controls

12.3.1 Policy on the use of cryptographic controls

Control 12.3.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

In addition to the guidance provided in ISO/IEC 27002, the following should be considered when developing a cryptographic policy:

a) The organization should adopt as a general principle to systematically consider and apply cryptographic controls whenever customer and financial information is stored or processed to ensure its confidentiality and integrity.

b) Access to this information in clear format should only be possible for valid business purposes and should comply with the requirements laid down in laws and regulations applying to the organization.

c) The approach and methods for regularly evaluating the quality and strength of encryption algorithms used within cryptographic controls to detect at early stage related weaknesses and to prevent inappropriate or incorrect use of encryption algorithms, by changing in accordance cryptographic keys management (e.g. increasing the frequency of changing or updating cryptographic keys).

Care should be taken when defining and assigning roles and responsibility for cryptographic keys management to ensure that involved security custodians have not privileges in the use of generated cryptographic keys.

Cryptographic keys involved in financial transaction systems processing or storing customer and financial information may be maintained by multiple security custodians, respectively owning a specific part of the cryptographic keys.

12.3.2 Key management

No additional guidance for organizations providing financial services.

12.4 Security of system files

12.4.1 Control of operational software

Control 12.4.1 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

In addition to the guidelines provided in ISO/IEC 27002, the following recommendation should be considered to minimize the risk of corruption to operational systems:

a) The authenticity of changes provided by vendors supplying applications and operating system software of payment devices (e.g. ATM, SST, POS) should be checked (e.g. through the use of digital signature, hashing algorithms) before being extensively and successfully tested.

12.4.2 Protection of system test data

No additional guidance for organizations providing financial services.

12.4.3 Access control to program source code

No additional guidance for organizations providing financial services.

12.5 Security in development and support processes

No additional guidance for organizations providing financial services.

12.6 Technical Vulnerability Management

No additional guidance for organizations providing financial services.

13 Information security incident management

No additional guidance for organizations providing financial services.

14 Business continuity management

14.1 Information security aspects of business continuity management

14.1.1 Including information security in the business continuity management process

No additional guidance for organizations providing financial services.

14.1.2 Business continuity and risk assessment

Control 14.1.2 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Care should be given when carrying out business continuity risk assessments to consider external dependencies of business processes, such as the supply of:

a) Financial information transmitted by business partners, contractors or supplier.

b) Procured financial services (e.g. internet banking, cards processing, cash management).

14.1.3 Developing and implementing continuity plans including information security

Control 14.1.3 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Business continuity plans developed by the organization should address the following external dependencies as part of the recovery and restoration process of business operations:

a) Financial information transmitted by business partners, contractors or supplier.

b) Procured financial services (e.g. internet banking, cards processing, cash management) by considering worst-case scenarios to ensure the continuity of these services in the event of a disruption affecting supplier operations

14.1.4 Business continuity planning framework

No additional guidance for organizations providing financial services.

14.1.5 Testing, maintaining and re-assessing business continuity plans

No additional guidance for organizations providing financial services.

15 Compliance

15.1 Compliance with legal requirements

No additional guidance for organizations providing financial services.

15.2 Compliance with security policies and standards, and technical compliance

15.2.1 Compliance with security policies and standards

No additional guidance for organizations providing financial services.

15.2.2 Technical compliance checking

Control 15.2.2 from ISO/IEC 27002:2005 is augmented as follows:

Implementation guidance

Care should be given to carrying out technical compliance checks on a regular basis of on-line financial transaction systems (e.g. internet banking), in particular if these systems are available to customers or contain customer and financial information to ensure their correct implementation and conformity in regards to applicable laws and regulations.

15.2.3 Compliance monitoring

Control

The organization should ensure that relevant legal, regulatory and contractual requirements are periodically checked against information security management framework for ensuring compliance monitoring.

Implementation guidance

A compliance monitoring process should be defined for regularly carrying out a mapping between the following:

a) Legal, regulatory and contractual requirements applicable for information security, and

b) The organization's information security management framework, including security control objectives, controls, policies, standards and any other security requirements implemented by the organization.

The mapping should be regularly performed to address changes in the applicable legislation and in the information security management framework, e.g. in the risk evaluation, mitigation and when significant changes occur.

Non-compliance instances with applicable legislation should be identified and handled by the organization.

Bibliography

[1] Payment Card Industry (PCI) Data Security Standard, *Requirements and Security Assessment Procedures* (version 1.2).

[2] COBIT – Control Objectives for Information Technology – Version 4.1 – IT Governance Institute and Information Systems Audit and Control Association (ISACA).

[3] ISO/IEC 27003:2010, *Information technology — Security techniques — Information security management system implementation guidance*

[4] ISO/IEC 27004:2009, *Information technology — Security techniques — Information security management — Measurement*

[5] ISO/IEC 27005:2011, *Information technology — Security techniques — Information security risk management*

[6] ISO/TR 13569:2005, *Financial services -- Information security guidelines*

[7] ISO/IEC 24762:2008, *Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services*

[8] ISO/IEC 27031:2011, *Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*

[9] ISO/IEC 27033-1:2009, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*

[10] ISO/IEC 27033-2:2012, *Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*

[11] ISO/IEC 27033-3:2010, *Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*

[12] ISO/IEC 27035:2011, *Information technology — Security techniques — Information security incident management*

[13] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

[14] ISO/IEC 27002:2005, *Information technology — Security techniques — Code of practice for information security management*

ICS 03.060; 35.040

Price based on 18 pages