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