Obsah

Medzinárodné normy a pozadie ich príprav 6

Jazykové vysvetlivky a usmernenia 9

Ako používať príručku 11

Schematické znázornenie súvislostí v normách

Zoznam noriem podľa číselného poradia 13

ISO/IEC 7064 Check character systems / Systémy kontrolných znakov 13

ISO/IEC 9796 Digital signature schemes giving message recovery / Metóda digitálneho podpisu s obnovou správy 13

ISO/IEC 9797 Message authentication codes (MACs) 15

ISO/IEC 9798 Entity authentication 17

ISO/IEC 10116 Modes of operation for an n-bit block cipher 21

ISO/IEC 10118 Hash-functions 22

ISO/IEC 11770 Key management 24

ISO/IEC 11889 Trusted platform modul. 28

ISO/IEC 13888 Non-repudiation 30

ITU-T X.842 I ISO/IEC TR 14516 Guidelines on the use and management of Trusted Third Party services 32

ISO/IEC 14888 Digital signature with appendix 33

ISO/IEC 15408 Evaluation criteria for IT security 35

ISO/IEC 15443 A framework for IT Security assurance 37

ISO/IEC TR 15446:2009 Guide on the production of Protection Profiles and Security Targets 39

ITU-T X.841 I ISO/IEC 15816 Security information objects for access control 40

ITU-T X.843 I ISO/IEC 15945 Specification of TTP services to support the application of digital signatures. 41

ISO/IEC 15946 Cryptographic techniques based on elliptic curves. 42

ISO/IEC 18014 Time stamping services 43

ISO/IEC 18031 Random bit generation 45

ISO/IEC 18032 Prime number generation 46

ISO/IEC 18033 Encryption algorithms 47

ISO/IEC 18045 Methodology for IT security evaluation 49

ISO/IEC 19772 Authenticated encryption 50

ISO/IEC 19790 Security requirements for cryptographic modules 51

ISO/IEC TR 19791 Security assessment of operational systems 51

ISO/IEC 19792 Security evaluation of biometrics 52

ISO/IEC 20000 IT Service Management. 53

ISO/IEC 20004 Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045 62

ISO/IEC 20008 Anonymous digital signature 62

ISO/IEC 20009 Anonymous entity authentication 64

ISO/IEC 21827 Systems Security Engineering – Capability Maturity Model (SSE-CMM). 65

ISO/IEC 24745 Biometric information protection. 65

ISO/IEC 24759 Test requirements for cryptographic modules 66

ISO/IEC 24760 A framework for identity management 67

ISO/IEC 24761 Authentication context of biometrics 69

ISO/IEC 24762 Guidelines for information and communications technology disaster recovery services 70

ISO/IEC 27000 Information security management systems – Overview and vocabulary 70

ISO/IEC 27001 Information security management system – Requirements 71

ISO/IEC 27002 Code of practice for information security controls 72

ISO/IEC 27003 Information security management systems implementation guidance 73

ISO/IEC 27004 Information security management measurements 74

ISO/IEC 27005 Information security risk management/Riadenie rizík informačnej bezpečnosti 74

ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management system 75

ISO/IEC 27007 Guidelines for information security management systems auditing 76

ISO/IEC TR 27008 Guidelines for auditors on information security management systems controls 77

ISO/IEC 27010 Information security management for inter-sector and inter-organizational communications 78

ISO/IEC 27011 Information security management guidelines for telecommunications 79

ISO/IEC 27013 Guidelines on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 79

ISO/IEC 27014 Governance of information security 80

ISO/IEC TR 27015 Information security management guidelines for financial services 81

ISO/IEC TR 27016 Information security management – Organizational economics 82

ISO/IEC TS 27017 Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002 82

ISO/IEC 27018 Code of practice for data protection controls for public cloud computing services. . . 83

ISO/IEC 27031 Guidelines for ICT readiness for business continuity 84

ISO/IEC 27032 Guidelines for cybersecurity 85

ISO/IEC 27033 Network security 86

ISO/IEC 27034 Application security 89

ISO/IEC 27035 Information security incident management 92

ISO/IEC 27036 Information security for supplier relationships 93

ISO/IEC 27037 Guidelines for identification, Collection, acquisition and preservation of digital evidence 95

ISO/IEC 27038 Specification for digital redaction. 96

ISO/IEC 27039 Selection, deployment and operation of intrusion detection and prevention systems (IDPS) 96

ISO/IEC 27040 Storage security 97

ISO/IEC 27041 Guidance on assuring suitability and adequacy of investigation methods 98

ISO/IEC 27042 Guidelines for the analysis & interpretation of digital evidence 98

ISO/IEC 27043 Investigation principles and processes. 99

ISO/IEC 27799 Health informatics – Information security management in health using ISO/IEC 27002 100

ISO/IEC 29100 Privacy framework. 101

ISO/IEC 29101 Privacy reference architecture 101

ISO/IEC 29115 Entity authentication assurance 102

ISO/IEC 29128 Verification of cryptographic protocols 103

ISO/IEC 29146 A framework for access management 104

ISO/IEC 29147 Vulnerability disclosure 104

ISO/IEC TR 29149 Best practice on the provision of timestamping services 105

ISO/IEC 29150 Signcryption 106

ISO/IEC 29190 Privacy capability maturity model 107

ISO/IEC 29191 Requirements for partially anonymous, partially unlinkable authentication 107

ISO/IEC 29192 Lightweight cryptography 108

ISO/IEC TR 29193 Secure system engineering principles and techniques 110

ISO/IEC TS 30104 Physical security attacks, mitigation techniques and security requirements 111

ISO/IEC 30111 Vulnerability handling processes 112