Information Security Management References

Corporate Information Security Working Group - Adam H. Putnam, Chairman
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census
Government Reform Committee, United States House of Representatives

Mapping of Existing Work on Infosec "Best Practices" Subgroup
Clint Kreitner and Michael Rasmussen, Coordinators
(3/18/04 11:00 AM EST)

	Document	URL	# Pages
	Comprehensive IS Mgmt – Principles Based		
1.	OECD Guidelines for the Security of Information Systems and Networks (9 pervasive principles for information security upon which several other guides are based.)	www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html	30, English & French
2.	GAPP – "Generally Accepted Principles and Practices" NIST SP 800-18, "Guide for Developing Security Plans for Information Technology Systems" December 1998 (Marianne Swanson & Barbara Guttman), ". Eight generally accepted principles (see OECD) and "Common IT Security Practices."	http://csrc.nist.gov/publications/nistpubs/index.html	55
3.	GAISP – Generally Accepted Information Security Principles Currently available: Generally Accepted Systems Security Principles (GASSP) consisting of Pervasive Principles (PP), & Broad Functional Principle (BFP), June, 1999. Detailed Principles are under development (ISSA)	www.issa.org/gaisp.html http://web.mit.edu/security/www/gassp1.html	PP 10 BFP 57
4.	NIST 800-14 Generally Accepted Principles and Practices for Securing IT Systems, 1996	http://csrc.nist.gov/publications/nistpubs/index.html	60
5.	NIST 800-26 Self Assessment Guide for IT Systems	http://csrc.nist.gov/publications/nistpubs/index.html	95
6.	NIST 800-27 Engineering Principles for IT Security	http://csrc.nist.gov/publications/nistpubs/index.html	31
7.	IFAC International Guidelines on Information Technology Management—Managing Information Technology Planning for Business Impact: International Federation of Accountants, New York, 1999.	www.ifac.org	20
	Comprehensive IS Mgmt - Controls Based		
8.	BS 7799 – Parts 1 & 2, Code of Practice for Information Security Management (British Standards Institute)	www.bsi.org.uk	Part 1, 77 Part 2, 11
9.	ISO 17799 – Information Technology – Code of Practice for Information Security Management	www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3	71
10.	Trust Services Criteria; including SysTrust/WebTrust (AICPA)	www.aicpa.org/trustservices	68
11.	Standard of Good Practice for Information Security (Information Security Forum)	www.isfsecuritystandard.com/index_ie.htm	224
12.	ITCG: Information Technology: Control Guidelines 1998 (CICA)	www.cica.ca	414
13.	ISO TR 13335 "Guidelines for the Management of Information Security", Parts 1-5	www.iso.org/iso/en/StandardsQueryFormHandler.StandardsQueryFormHandler	18, 14, 47, 61, 31
14.	IT Baseline Protection Manual - P BSI 7152 E 1, BSI - Bundesamt für Sicherheit in der Informationstechnik	http://www.bsi.bund.de/gshb/english/menue.htm	1600 in 3 binders
15.	NIST 800-12 The Computer Security Handbook, 1995	http://csrc.nist.gov/publications/nistpubs/index.html	290
16.	NIST 800-37 Guide for The Security Certification and Accreditation of Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/index.html	55

IS Management References (cont'd.)

17.	NIST 800-53 - Recommended Security Controls for Federal Info Systems (draft)	http://csrc.nist.gov/publications/nistpubs/index.html	229
18.	Personal Information Protection and Electronic Documents Act (PIPEDA), Canadian	www.pipeda.org	31
19.	EU Data Protection Directive - Part 1 & Part 2 available in separate PDFs	http://aspe.os.dhhs.gov/datacncl/eudirect.htm http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf http://europa.eu.int/comm/internal_market/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf	Pt1: 9 Pt 2: 11
20.	FDA 21 CFR Part 11 – U.S. Food & Drug Administration; Title 21 Code of Federal Regulations Electronic Records; Electronic Signatures	www.fda.gov/ora/compliance_ref/part11	2
21.	DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. London, 1993, 1995. (Became BS 17799)	www.dti.gov.uk www.dti.gov.uk/industries/information_security/	
	Audit Guides		
22.	FISCAM - Federal Information Systems Controls Audit Manual (GAO)	www.gao.gov	284
23.	Systems Auditability and Control (SAC) – IIA RF	www.theiia.org/eSAC	1600+
24.	Electronic Systems Assurance and Control (eSAC) – IIA RF Series of reports on IT management and security topics.	www.theiia.org/eSAC	various
	Security Metrics		
25.	NIST 800-55 Security Metrics Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/index.html	91
26.	Consensus Benchmark Scoring Tools	www.cisecurity.org	various
	Capability Maturity Models		
27.	ISO 21827 System Security Engineering Capability Maturity Model	http://www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=34731&ICS1=35&ICS2=40&ICS3	123
28.	SSE-CCM: Model Description Document, V 2.0 April 1, 1999	http://www.sse-cmm.org/	322
	Product Security Models		
29.	ISO 15408 Common Criteria	http://csrc.nist.gov/cc/ccv20/ccv2list.htm	618
	Governance Guides		
30.	Information Security Governance: Guidance for Boards of Directors and Executive Management", 2001 – IT Governance Institute	www.itgi.org http://www.itgi.org/template_ITGI.cfm?Section=Recent_Publications&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=43&ContentID=6579	28
31.	Information Security Management and Assurance – Three report series from IIA, NACD, CIAO, et al	http://www.theiia.org/esac/index.cfm?fuseaction=or&page=rciap	Rpt 1 – 20 Rpt 2 – 28 Rpt 3 - 66

IS Management References (cont'd.)

32.	Information Security Governance: Toward a Framework for Action (Business Software Alliance)	http://www.bsa.org/resources/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=5841	16
33.	Information Security Oversight: Essential Board Practices (Nat'l Assoc of Corporate Directors)	http://www.nacdonline.org/publications/pubDetails.asp?pubID=138&user=6158BBEB9D7C4EE0B9E4B98B601E3716	14
34.	IT Governance Implementation Guide	http://www.isaca.org/Template.cfm?Section=Browse_By_Topic&Template=/Ecommerce/ProductDisplay.cfm&ProductID=503	58
35.	Turnbull Report - Internal Control - Guidance for Directors on the Combined Code – Institute of Chartered Accountants in England & Wales (ICAEW)	http://www.icaew.co.uk/index.cfm?AUB=TB2I_6242,MNXI_47896	18
	Management Guides		
36.	Common Sense Guide for Senior Managers (Internet Security Alliance)	http://www.isalliance.org	21
37.	Building Security in the Digital Resource: An Executive Resource – Business Roundtable, Nov. 2002	www.businessroundtable.org	17
38.	Information Security for Executives – Business and Industry Advisory Committee to the OECD, and International Chamber of Commerce, Paris, November 2003	http://www.iccwbo.org/home/e_business/word_documents/SECURITY-final.pdf	40
39.	VISA Cardholder Information Security Program (CISP) Digital Dozen	http://usa.visa.com/business/merchants/cisp_index.html?ep=v_sym_cisp	1
40.	ICC Handbook on Information Security Policy for Small to Medium Enterprises - International Chamber of Commerce, April 11, 2003	www.iccwbo.org	
41.	Corporate Information Security Evaluation for CEO's (TechNet)	www.technet.org/cybersecurity	16
42.	The 60 Minute Network Security Guide (NSA SNAC)	www.nsa.gov/snac/support/download.htm	35
43.	Security Checklists for: Mid/Large Businesses Small Businesses Government Agencies Consumers (Business Software Alliance)	http://global.bsa.org/usa/policy/security/checklists.phtml	1 each
44.	NIST 800-26 Security Self-Assessment Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/index.html	87
45.	NIST 800-50 Building an Information Technology Security Awareness and Training Program	http://csrc.nist.gov/publications/nistpubs/index.html	70
46.	NIST 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories, Volumes 1 & 2	http://csrc.nist.gov/publications/nistpubs/index.html	V1 – 38 V2 - 266
	Sector Specific Guides		
47.	Electronic Security: Risk Mitigation in Financial IT Transactions - The World Bank, (Thomas Glaessner, Tom Kellermann, and Valerie McNevin), June 2002	http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/(attachmentweb)/E-security-RiskMitigationInFinancialTransactionsv4/$FILE/E-security-Risk+Mitigation+In+Financial+Transactions+v+4.0.pdf	164

IS Management References (cont'd.)

48.	Interim Security Guidelines: Standard 1200 – Cyber Security – North American Electric Reliability Council (NERC)	ftp://ftp.nerc.com/pub/sys/all_updl/standards/Urgent-Req-CyberStnd-3-3121.pdf	24
49.	Basel II – The New BASEL Capital Accord – Bank for International Settlements	http://www.bis.org/publ/bcbsca.htm	126
50.	ISO TR 13569 "Banking and Related Financial Services – Information Security Guidelines, 9/9/2003	http://www.iso.org/iso/en/stdsdevelopment/techprog/workprog/TechnicalProgrammeProjectDetailPage.TechnicalProgrammeProjectDetail?csnumber=37245	100
51.	BITS Framework: Managing Technology Risk for Information Technology (IT) Service Provider Relationships – Financial Services Roundtable (FSR)	www.bitsinfo.org www.bitsinfo.org/bits2003framework.pdf	63
52.	Federal Financial Institutions Examination Council (FFIEC) - FFIEC "Audit IT Examination Handbook," and "FFIEC Audit Examination Procedures"	www.ffiec.gov www.ffiec.gov/ffiecinfobase/index.html	HB 49 Proc. 27
	Legal/Regulatory /Enforcement		
53.	Sarbanes-Oxley Act (SOX)	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ204.107.pdf	60
54.	Gramm, Leach, Bliley Act (GLBA) - The Financial Modernization Act of 1999	www.ftc.gov/privacy/glbact/	385
55.	Health Information Portability and Accountability Act - HIPAA	www.hhs.gov/ocr/hipaa/	18?
56.	Federal Information Security Management Act of 2002 (FISMA) – U.S. Congress, 2002	www.fedcirc.gov/library/legislation/FISMA.html	17
57.	CA SB 1386 (the "You've Been Hacked" Act)	http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html	4
58.	Federal Trade Commission enforcement guidelines/actions	http://www.ftc.gov/ogc/brfovrvw.htm http://www.ftc.gov/opa/2003/11/cybersecurity.htm	9
	Risk Management Models		
59.	NIST 800-30 Risk Management Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/index.html	55
60.	SEI's OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)		128
61.	Sound Practices for Mgmt & Supervision of Operational Risk	http://www.bis.org/publ/bcbs96.pdf	14
	Guides for Small Business		
62.	Consensus Benchmark Technical Controls	http://www.cisecurity.org	various
63.	e-Security Guide for Small Business **(**Association of Small Business Development Centers, and Microsoft)	http://www.asbdc-us.org	50
64.	Small Business Best Practices (draft) (Internet Security Alliance and Small Business Working Group)	http://www.us-cert.gov	
65.	Seven Simple Computer Security Tips for Small Business and Home Computer Users (InfraGard)	http://www.infragard.net/library/seven_pc_tips.htm	1

IS Management References (cont'd.)

	Guides for Home and Individual Users		
66.	Common Sense Guide for Home and Individual Users (Internet Security Alliance)	http://www.isalliance.org	26
67.	StaySafeOnline (FTC/NCSA) – Top 10 Security Tips, Security Test, educational materials, more.	www.staysafeonline.info	various
68.	FTC Consumer and Business Education	http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html	various
69.	Cybersecurity and Consumer Data: What's at Risk for the Consumer? – Prepared statement of the Federal Trade Commission (FTC) before the Commerce, Trade, & Consumer Protection Subcommittee, Committee on Energy & Commerce, U.S. House of Representatives, Nov. 19, 2003	http://www.ftc.gov/os/2003/11/031119swindletest.htm	6
70.	Cyber-Safety for Everyone: From Kids to Elders	http://www2.norwich.edu/mkabay/cyberwatch/cybersafety.pdf	82
71.	Internet & Computer Ethics for Kids: (and Parents & Teachers Who Haven't Got a Clue.) – Winn Schwartau & D.L. Busch	www.amazon.com	200
72.	Top Ten Security Steps for Kids	http://www.iisw.cerias.purdue.edu/k-12/top10_kids.php	1
73.	Security Procedures for Educators	http://www.iisw.cerias.purdue.edu/k-12/top10_educators.php	1
	Technical Controls Guides		
74.	Consensus Benchmarks	www.cisecurity.org	various
75.	DISA Security Technical Implementation Guides	http://csrc.nist.gov/pcig/cig.html	various
76.	NIST Configuration Guides	http://csrc.nist.gov/pcig/cig.html	various
77.	NSA Configuration Guides	www.nsa.gov/snac	various
78.	SANS Step-by Step Guides	https://store.sans.org	various
79.	Vendor Configuration Guides		
	Comprehensive IT Governance and Management		
80.	Board Briefing on IT Governance (IT Governance Institute)	www.itgi.org http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm	63
81.	COBIT – Control Objectives for Information and Related Technologies (ISACA)	www.isaca.org	148

Organizations:

AICPA – The American Institute of Certified Public Accountants, www.aicpa.org
ANSI – American National Standards Institute, www.ansi.org
ASBDC-US – The Association of Small Business Development Centers, www.asbdc-us.org
BITS - The Technology Group for The Financial Services Roundtable, www.bitsinfo.org
BR – Business Roundtable, www.businessroundtable.org
BSA – Business Software Alliance, www.bsa.org/usa
BSI – British Standards Institute, www.bsi.org.uk
BSI - Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de
CERT – Computer Emergency Response Team, www.cert.org
CIAO – Critical Infrastructure Assurance Office (formerly U.S. Dept. of Commerce, now IAIP of DHS)
CICA – Canadian Institute of Chartered Accountants www.cica.ca
CIS – The Center for Internet Security, www.cisecurity.org

IS Management References (cont'd.)

CMU – Carnegie Mellon University, www.cmu.edu
COSO – Committee of Sponsoring Organizations for the Commission on Fraudulent Financial Reporting (Treadway Commission), www.coso.org
DHS – Department of Homeland Security, www.dhs.gov
DISA - Defense Information Systems Agency www.disa.mil
FFIEC – Federal Financial Institutions Examination Council, www.ffiec.gov
FSR – Financial Services Roundtable, www.fsround.org
FTC - Federal Trade Commission, www.ftc.gov
GAISPC – Generally Accepted Information Security Principles Committee, www.issa.org/gaisp.html
IAIP – Information Assurance and Infrastructure Protection Directorate of the DHS, (See www.dhs.gov.)
ICAEW – Institute of Chartered Accountants in England & Wales, www.icaew.co.uk
ICC – International Chamber of Commerce, www.iccwbo.org
IFAC – International Federation of Accountants, www.ifac.org
IIA – The Institute of Internal Auditors, Inc. (and IIA Research Foundation), www.TheIIA.org
ISA – Internet Security Alliance, www.isalliance.org
ISACA – The Information Systems Audit and Control Association, www.isaca.org
ISF – Information Security Forum, www.securityforum.org
ISO – International Organization for Standardization, www.iso.org
ISSA – Information Systems Security Association, www.issa.org
NACD – National Association of Corporate Directors, www.nacdonline.org
NCSA – National Cyber Security Alliance, www.staysafeonline.info
NERC – North American Electric Reliability Council www.nerc.com
NIST – National Institute for Standards and Technology, www.nist.gov
NSA – National Security Agency, www.nsa.gov
OECD – Organization for Economic Cooperation and Development, www.oecd.org
PCAOB – Public Company Accounting Oversight Board, www.pcaobus.org
SANS – Systems Administration, Audit, and Network Security Institute, www.sans.org
SEC – Securities & Exchange Commission, www.sec.gov
SEI – Carnegie Mellon University Software Engineering Institute, www.sei.cmu.edu
SNAC – Systems and Network Attack Center (NSA), www.nsa.gov/snac
US-CERT – U.S. Computer Emergency Readiness Team, www.us-cert.gov
WB – World Bank, www.worldbank.org

Subgroup Members

Clint Kreitner- Center for Internet Security, ClintKreitner@aol.com, 540-459-1861 Coordinator
Michael Rasmussen- Information Systems Security Association (for Dave Cullinane) Coordinator
mrasmussen@forrester.com, 262-534-9188
Gretchen Beyer- TechNet (for Rick White) gbeyer@technet.org
Roger Cressey-Business Roundtable (for Marian Hopkins) roger@goodharbor.net
Brett Kilbourne- United Telecom Council (for Bill Moroney, bill.moroney@utc.org) brett.kilbourne@utc.org
Jim Kohlenberger- Business Software Alliance (for Robert Holleyman) jimk@bsa.org
Charles Le Grand- Institute of Internal Auditors (for William Bishop, bbishop@theiia.org), clegrand@theiia.org, 407-937-1380
Mark Silver- Business Roundtable (for Marian Hopkins) mark.silver@siemens.com 732-512-7044
Karyn Waller- AICPA (for James O'Malley) kwaller@aicpa.org

Adjunct Members:

Phil Campbell, Sandia Laboratories, plcampb@sandia.gov, 505-845-8518
Mike Dickson, mike@mikedickson.com,
Don Holden, Concordant, donholden@rcn.com, 603-673-8454
Mike Hines, Purdue University, mshines@purdue.edu, 765-494-5875
Prudence Parks, United Telecom Council, prudence.parks@utc.org,
Adam Stone, Fortis, Adam.Stone@us.fortis.com, 651-361-4215
Dan Swanson, The Institute of Internal Auditors, Inc. dswanson@theiia.org, 407-937-1363