Appendix eE

List of Security Standards

BITS Financial Services Roundtable (www.bits.org/FISAP/index.php): Security assessment questionnaire and review process based on ISO/IEC 27002 (access requires free registration). Also information on the overlaps between ISO/IEC 27002, PCI-DSS 1.1 and COBIT.

Common Criteria (www.commoncriteriaportal.org/thecc.html): Provides the Common Criteria for Information Technology Security Evaluation, also published as ISO/IEC 15408.

ISO 27001 Certificates (iso27001certificates.com/): List of organizations certified against ISO/IEC 27001 or equivalent national standards, maintained by the ISMS International User Group based on inputs from all the certification bodies.

ISO 27000 Directory (www.27000.org/): Information covering the ISO/IEC 27000 series of standards, including updates and consultants directory.

ISO 27001 Security (www.iso27001security.com/): Information about the ISO/IEC 27000-series information security standards and other related standards, with discussion forum and FAQ.

ISO 27000 Toolkit (www.17799-toolkit.com/): Package containing the ISO/IEC 27001 and 27002 standards plus supporting materials such as policies and a glossary.

ISO/IEC 27002 Explained (www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice/legislationpolicystandards/securitystandards/isoiec27002/page33370.html): Information on ISO/IEC 27001 and 27002 from BERR, the UK government department for Business Enterprise and Regulatory Reform (formerly the DTI, the Department of Trade and Industry).

ISO/IEC 27001 Frequently Asked Questions (www.atsec.com/01/index.php?id=06-0101-01): FAQ covers the basics of ISO/IEC 27001, the ISO/IEC standard Specification for an Information Security Management System.

NIST Special Publication 800-53 (csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf): Recommended Security Controls for Federal Information Systems has a similar scope to ISO/IEC 27002 and cross-references the standard. [PDF]

Overview of Information Security Standards (www.infosec.gov.hk/english/technical/files/overview.pdf): Report by the Government of the Hong Kong Special Administrative Region outlines the ISO/IEC 27000-series

Federal Information Processing Standards (FIPS)

Number	Date	Title
FIPS 201–2	Jul 9, 2012	DRAFT Personal Identity Verification (PIV) of Federal Employees and Contractors (REVISED DRAFT) draft_nist-fips-201-2_revised.pdf
		comment-template_draft-nist-fips201-2_revised.xls
		draft-nist-fips-201-2-revised_track-changes.pdf
		draft-fips-201-2_comments_disposition-for-2011-draft.pdf
FIPS 201–1	Mar 2006	Personal Identity Verification (PIV) of Federal Employees and Contractors (*including Change Notice 1 of June 23, 2006*) FIPS-201-1-chng1.pdf
FIPS 200	Mar 2006	Minimum Security Requirements for Federal Information and Information Systems FIPS-200-final-march.pdf
FIPS 199	Feb 2004	Standards for Security Categorization of Federal Information and Information Systems FIPS-PUB-199-final.pdf
FIPS 198–1	Jul 2008	The Keyed-Hash Message Authentication Code (HMAC) FIPS-198-1_final.pdf
FIPS 186–3 Proposed Change	April 10, 2012	DRAFT Proposed Change Notice for Digital Signature Standard (DSS) change-notice_fips-186-3.pdf
		fips_186-3.pdf
FIPS 186–3	Jun. 2009	Digital Signature Standard (DSS) fips_186-3.pdf
FIPS 180–4	March 2012	Secure Hash Standard (SHS) fips-180-4.pdf
FIPS 140–3	Dec. 11, 2009	DRAFT Security Requirements for Cryptographic Modules (Revised Draft) revised-draft-fips140-3_PDF-zip_document-annexA-to-annexG.zip
		revised-fips140-3_comments-template.dot

standards plus related standards, regulations etc. including PCI-DSS, COBIT, ITIL/ISO 20000, FISMA, SOX and HIPAA. [PDF]

Praxiom Research Group Ltd. (praxiom.com/#ISO%20IEC%2027001%20LIBRARY): Plain English descriptions of ISO/IEC 27001, 27002 and other standards, including a list of the controls.

The Security Practitioner (security.practitioner.com/intro-duction/): The ISO 27001 Perspective: An Introduction to Information Security is a guide to ISO/IEC 27001 and 27002 in the form of an HTML help file.

Veridion (www.veridion.net/): ISO/IEC 27001 and 27002 training courses including Lead Auditor and Lead Implementer, plus other information security, risk management and business continuity courses on BS 25999, CISSP, CISA, CISM, MEHARI and OCTAVE.