





audit standards are reasonable and customary standards in the industry.” This safe harbor offers organizations the opportunity to reduce compliance risk by adopting the CobiT audit standards. However, there could be many reasons why the CobiT standards are inappropriate for the particular organization – cost, complexity, etc., may simply not warrant the use of that standard. Is the organization bound to use CobiT anyway? (If you’ve read this far, you probably already know the answer.) The answer, of course, is **no** – the organization is free to use whatever auditing standard it chooses *provided* it meets the two-prong test of “reasonable” and “customary in the industry.” However, if the organization chooses to use a standard other than CobiT and the regulator doesn’t like it, the organization may have an uphill battle to convince the regulator (and, perhaps ultimately, the court) that the chosen standard is, in fact, reasonable and customary in the industry.

Safe harbors tend to be very conservative and avoid gray areas. If a safe harbor is available, it’s always good to know – even if you choose not to follow it, it can provide valuable guidance and insight into the regulator’s mindset. However, the needs of the organization may dictate that it leave the safe harbor and enter riskier waters.

The authority documents tracked by the UCF

To give you a scope of the authority documents that we’ve used to form this material, and all of the other material within the Unified Compliance Framework, here is a listing of all of the authority documents that we are currently tracking and referencing. Please know that this is an ever growing list and is subject to change as the documents themselves change. For the most up-to-date listing, along with URL links to each of the documents we track, see the Unified Compliance Framework website at www.unifiedcompliance.com.

Sarbanes Oxley

-  Sarbanes-Oxley Act (SOX)
-  PCAOB Auditing Standard No. 2
-  AICPA SAS 94
-  AICPA/CICA Privacy Framework

- Av AICPA Suitable Trust Services Criteria
- Av Retention of Audit and Review Records, SEC 17 CFR 210.2-06
- Av Controls and Procedures, SEC 17 CFR 240.15d-15
- Av Reporting Transactions and Holdings, SEC 17 CFR 240.16a-3
- Av COSO Enterprise Risk Management (ERM) Framework

Banking and Finance

- Av Basel II: International Convergence of Capital Measurement and Capital Standards - A Revised Framework
- Av BIS Sound Practices for the Management and Supervision of Operational Risk
- Av Gramm-Leach-Bliley Act (GLB)
- Av Standards for Safeguarding Customer Information, FTC 16 CFR 314
- Av Privacy of Consumer Financial Information, FTC 16 CFR 313
- Av Safety and Soundness Standards, Appendix of OCC 12 CFR 30
- Av FFIEC Information Security
- Av FFIEC Development and Acquisition
- Av FFIEC Business Continuity Planning
- Av FFIEC Audit
- Av FFIEC Management
- Av FFIEC Operations

NASD NYSE

- Av NASD Manual
- Av NYSE Rules
- Av Recordkeeping rule for securities exchanges, SEC 17 CFR 240.17a-1
- Av Records to be made by certain exchange members SEC 17 CFR 240.17a-3
- Av Records to be preserved by certain exchange members SEC 17 CFR 240.17a-4
- Av Recordkeeping SEC 17 CFR 240.17Ad-6
- Av Record retention SEC 17 CFR 240.17Ad-7

Healthcare and Life Science

- Av HIPAA (Health Insurance Portability and Accountability Act)
- Av HIPAA HCFA Internet Security Policy
- Av Introductory Resource Guide for HIPAA NIST (800-66)
- Av CMS Core Security Requirements (CSR)
- Av CMS Information Security Acceptable Risk Safeguards (ARS)
- Av CMS Information Security Certification and Accreditation (C&A) Methodology
- Av CMS Info Security Business Risk Assessment
- Av CMS Business Partners Systems Security Manual
- Av FDA Electronic Records; Electronic Signatures FDA 21 CFR Part 11+D1

Energy

- Av FERC Security Program for Hydropower Projects
- Av North American Electric Reliability Corporation Critical Infrastructure Protection Cyber Security Standards

Payment Card

- Av PCI DSS (Payment Card Industry Data Security Standard)
- Av PCI DSS Security Scanning Procedures
- Av VISA CISP: What to Do If Compromised
- Av American Express Data Security Standard (DSS)
- Av MasterCard Wireless LANs - Security Risks and Guidelines

U.S. Federal Security

- Av FTC Electronic Signatures in Global and National Commerce Act (ESIGN)
- Av Uniform Electronic Transactions Act (UETA)
- Av FISMA (Federal Information Security Management Act)
- Av FISCAM (Federal Information System Controls Audit Manual)
- Av FIPS 140-2, Security Requirements for Cryptographic Modules
- Av FIPS 199, Standards for Security Categorization of Federal Information and Information Systems

- Av FIPS 191, Guideline for the Analysis of LAN Security
- Av Clinger-Cohen Act (Information Technology Management Reform Act)
- Av The National Strategy to Secure Cyberspace
- Av GAO Financial Audit Manual
- Av Standard for Electronic Records Management Software, DOD 5015.2
- Av CISWG Report on the Best Practices Subgroup
- Av CISWG Information Security Program Elements
- Av Appendix III to OMB Circular No. A-130: Security of Federal Automated Information Resources
- Av NCUA Guidelines for Safeguarding Member Information, 12 CFR 748

U.S. Internal Revenue

- Av IRS Revenue Procedure: Retention of books and records, 97-22
- Av IRS Revenue Procedure: Record retention: automatic data processing, 98-25
- Av IRS Internal Revenue Code Section 501(c)(3)

Records Management

- Av Federal Rules of Civil Procedure
- Av Uniform Rules of Evidence
- Av ISO 15489-1, Information and Documentation: Records management: General
- Av ISO 15489-2, Information and Documentation: Records management: Guidelines
- Av The DIRKS Manual: A Strategic Approach to Managing Business Information
- Av The Sedona Principles Addressing Electronic Document Production

NIST Publications

- Av Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST SP 800-14
- Av Developing Security Plans for Federal Information Systems, NIST SP 800-18
- Av Security Self-Assessment Guide, NIST SP 800-26
- Av Risk Management Guide, NIST SP 800-30

- Av Underlying Technical Models for Information Technology Security
- Av Contingency Planning Guide for Information Technology Systems, NIST SP 800-34
- Av Creating a Patch and Vulnerability Management Program, NIST SP 800-40
- Av Guidelines on Firewalls and Firewall Policy, NIST SP 800-41
- Av Recommended Security Controls for Federal Information Systems, NIST SP 800-53
- Av Guide for Mapping Types of Information and Information Systems to Security Categories, NIST SP 800-60
- Av Computer Security Incident Handling Guide, NIST SP 800-61
- Av Security Considerations in the Information System Development Life Cycle, NIST SP 800-64

International Standards Organization

- Av ISO 73:2002, Risk Management - Vocabulary
- Av ISO 13335, Information Technology - Guidelines for Management of IT Security
- Av ISO 17799:2000, Code of Practice for Information Security Management
- Av ISO 17799:2005, Code of Practice for Information Security Management
- Av ISO 27001:2005, Information Security Management Systems - Requirements
- Av ISO/IEC 20000-12:2005 Information technology — Service Management Part 1
- Av ISO/IEC 20000-2:2005 Information technology — Service Management Part 2
- Av ISO/IEC 15408-1:2005 Common Criteria for Information Technology Security Evaluation Part 1
- Av ISO/IEC 15408-2:2005 Common Criteria for Information Technology Security Evaluation Part 2
- Av ISO/IEC 15408-3:2005 Common Criteria for Information Technology Security Evaluation Part 3
- Av ISO/IEC 18045:2005 Common Methodology for Information Technology Security Evaluation Part 3

IT Information Library

- Av OGC ITIL: Planning to Implement Service Management
- Av OGC ITIL: ICT Infrastructure Management
- Av OGC ITIL: Service Delivery
- Av OGC ITIL: Service Support
- Av OGC ITIL: Application Management
- Av OGC ITIL: Security Management

General Guidance

- Av CobiT 3rd Edition
- Av CobiT 4.0
- Av ISACA IS Standards, Guidelines, and Procedures for Auditing and Control Professionals
- Av Disaster / Emergency Management and Business Continuity, NFPA 1600
- Av ISF Standard of Good Practice for Information Security
- Av ISF Security Audit of Networks
- Av A Risk Management Standard, jointly issued by AIRMIC, ALARM, and IRM
- Av Business Continuity Institute (BCI) Good Practice Guidelines
- Av ISSA Generally Accepted Information Security Principles (GAISP)
- Av CERT Operationally Critical Threat, Asset & Vulnerability Evaluation (OCTAVE)
- Av The GAIT Methodology
- Av IIA Global Technology Audit Guide (GTAG)

U.S. Federal Privacy

- Av Cable Communications Privacy Act Title 47 § 551
- Av Telemarketing Sales Rule (TSR), 16 CFR 310
- Av CAN SPAM Act
- Av Children's Online Privacy Protection Act (COPPA), 16 CFR 312
- Av Driver's Privacy Protection Act (DPPA), 18 USC 2721
- Av Family Education Rights Privacy Act (FERPA), 20 USC 1232

- Av Privacy Act of 1974, 5 USC 552a
- Av Video Privacy Protection Act (VPPA), 18 USC 2710
- Av Specter-Leahy Personal Data Privacy and Security Act
- Av Amendments to the FTC Telemarketing Sales Rule
- Av Children's Online Privacy Protection Act
- Av U.S. State Privacy
- Av Arkansas Personal Information Protection Act AR SB 1167
- Av Arizona Amendment to Arizona Revised Statutes 13-2001, AZ HB 2116
- Av California Information Practice Act, CA SB 1386
- Av California General Security Standard for Businesses CA AB 1950
- Av California Public Records Military Veteran Discharge Documents, CA AB 1798
- Av California OPP Recommended Practices on Notification of Security Breach
- Av Colorado Prohibition against Using Identity Information for Unlawful Purpose, CO HB 1134
- Av Colorado Consumer Credit Solicitation Protection, CO HB 1274
- Av Colorado Prohibiting Inclusion of Social Security Number, CO HB 1311
- Av Connecticut law Requiring Consumer Credit Bureaus to Offer Security Freezes, CT SB 650
- Av Connecticut law Concerning Nondisclosure of Private Tenant Information, CT HB 5184
- Av Delaware Computer Security Breaches DE HB 116
- Av Florida Personal Identification Information/Unlawful Use, FL HB 481
- Av Georgia Consumer Reporting Agencies, GA SB 230
- Av Georgia Public employees; Fraud, Waste, and Abuse, GA HB 656
- Av Hawaii Exempting disclosure of Social Security numbers HI HB 2674
- Av Illinois Personal Information Protection Act IL HB 1633
- Av Indiana Release of Social Security Number, Notice of Security Breach IN SB 503
- Av Louisiana Database Security Breach Notification Law, LA SB 205 Act 499
- Av Maine law To Protect Maine Citizens from Identity Theft, ME LD 1671

- Av Minnesota Data Warehouses; Notice Required for Certain Disclosures, MN HF 2121
- Av Missouri War on Terror Veteran Survivor Grants, MO HB 957
- Av Montana bill to Implement Individual Privacy and to Prevent Identity Theft, MT HB 732
- Av New Jersey Identity Theft Prevention Act, NJ A4001/S1914
- Av New York Information Security Breach and Notification Act
- Av Nevada Security Breach Notification Law, NV SB 347
- Av North Carolina Security Breach Notification Law (Identity Theft Protection Act) , NC SB 1048
- Av North Dakota Personal Information Protection Act, ND SB 2251
- Av Ohio Personal information - contact if unauthorized access, OH HB 104
- Av Rhode Island Security Breach Notification Law, RI HB 6191
- Av Tennessee Security Breach Notification, TN SB 2220
- Av Texas Identity Theft Enforcement and Protection Act, TX SB 122
- Av Vermont Relating to Identity Theft , VT HB 327
- Av Virginia Identity theft; penalty; restitution; victim assistance, VA HB 872
- Av Washington Notice of a breach of the security, WA SB 6043

EU Guidance

- Av EU Directive on Privacy and Electronic Communications, 2002/58/EC
- Av EU Directive on Data Protection, 95/46/EC
- Av US Department of Commerce EU Safe Harbor Privacy Principles
- Av Consumer Interests in the Telecommunications Market, Act No. 661
- Av OECD / World Bank Technology Risk Checklist
- Av OECD Guidelines on Privacy and Transborder Flows of Personal Data
- Av UN Guidelines for the Regulation of Computerized Personal Data Files (1990)
- Av ISACA Cross-Border Privacy Impact Assessment
- Av Information Technology Security Evaluation Manual (ITSEM)
- Av Information Technology Security Evaluation Criteria (ITSEC)

Av Directive 2003/4/EC Of The European Parliament

UK and Canadian Guidance

- Av FSA Combined Code on Corporate Governance
- Av Turnbull Guidance on Internal Control, UK FRC
- Av Smith Guidance on Audit Committees, UK FRC
- Av UK Data Protection Act of 1998
- Av IT Service Management Standard , BS 15000-1
- Av IT Service Management Standard - Code of Practice, BS 15000-2
- Av British Standards Institute PAS 56, Guide to Business Continuity Management
- Av Canada Keeping the Promise for a Strong Economy Act, Bill 198
- Av Canada Personal Information Protection Electronic Documents Act (PIPEDA)
- Av Canada Privacy Policy and Principles

Latin American Guidance

- Av Argentina Personal Data Protection Act
- Av Mexico Federal Personal Data Protection Law

Other European and African Guidance

- Av Austria Data Protection Act
- Av Austria Telecommunications Act
- Av Bosnia Law on Protection of Personal Data
- Av Czech Republic Personal Data Protection Act
- Av Denmark Act on Competitive Conditions and Consumer Interests
- Av Finland Personal Data Protection Act
- Av Finland act on the amendment of the Personal Data Act (986/2000)
- Av France Data Protection Act
- Av German Federal Data Protection Act
- Av IT Baseline Protection Manual Germany
- Av Greece Law on the Protection of Individuals with Regard to the Processing of Personal Data

- Av Hungary Protection of Personal Data and Disclosure of Data of Public Interest
- Av Iceland Protection of Privacy as regards the Processing of Personal Data
- Av Ireland Data Protection Act of 1988
- Av Ireland Data Protection Amendment 2003
- Av Italy Personal Data Protection Code
- Av Italy Protection of Individuals Other Subject with regard to the Processing of Personal Data
- Av Lithuania Law on Legal Protection of Personal Data
- Av Luxembourg Data Protection Law
- Av Netherlands Personal Data Protection Act
- Av Poland Protection of Personal Data Act
- Av Slovak Republic Protection of Personal Data in Information Systems
- Av Personal Data Protection Act of the Republic of Slovenia of 2004
- Av South Africa Promotion of Access to Information Act
- Av ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data
- Av Sweden Personal Data Act
- Av Switzerland Federal Act on Data Protection

Asia and Pacific Rim Guidance

- Av Australia Better Practice Guide - Business Continuity Management
- Av Australia Spam Act
- Av Australia Spam Act 2003: A practical guide for business
- Av Australia Privacy Act
- Av Australia Telecommunications Act
- Av Hong Kong Personal Data (Privacy) Ordinance
- Av India Information Technology Act (ITA-2000)
- Av Japan ECOM Guidelines Concerning the Protection of Personal Data in Electronic Commerce in the Private Sector (version 1.0)
- Av Japan Handbook Concerning Protection Of Personal Data
- Av Japan Personal Information Protection Act (Law No. 57 of 2003)

- Av Korea Act on Promotion of Information & Communication Network Utilization and Information Protection, etc
- Av Korea Act on the Protection of Personal Information Maintained by Public Agencies 1994
- Av Korea Act Relating to Use and Protection of Credit Information
- Av New Zealand Privacy Act 1993
- Av Taiwan Computer-Processed Personal Data Protection Law 1995
- Av India's Information Technology Act, 2000