Compliance Regulations

Security

Federal Information Processing Standard 140-2 (FIPS 140-2)

A standard that describes US federal government requirements, which IT products should meet for Sensitive but Unclassified (SBU) use. The standard was published by the National Institute of Standards and Technology (NIST), has been adopted by the Canadian government's Communications Security Establishment (CSE), and is likely to be adopted by the financial community through the American National Standards Institute (ANSI). FIPS 140-2

ITAR/Export Control (Worldwide)

The US Department of State's International Traffic in Arms Regulations (ITAR) that prohibit the disclosure or transfer of regulated technical data to a non-US citizen, whether in the United States or abroad. ITAR

OMB Memorandum M-06-16

The US Office of Management and Budget (OMB) issued memorandum M-06-16 on June 23, 2006, outlining recommended actions for all federal departments and agencies to properly safeguard information assets. In OMB Memorandum M-06-16, the Deputy Director for Management directed all federal agencies and departments to "encrypt all sensitive data on their mobile computers/devices." The deadline set for compliance with this Memorandum was Aug. 7, 2006. This recommendation is in addition to the National Institute of Standards and Technology (NIST) checklist for protection of remote information. OMB Memorandum M-06-16

Privacy

Gramm-Leach-Bliley (US)

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act (GLBA), controls the manner in which financial institutions handle customer information. The act contains several provisions relating to the privacy of consumer financial data, including a definition of privacy and information disclosure policies. GLBA

HIPAA (US)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets requirements for healthcare and related organizations concerning the electronic communication of patient information. For example, hospitals cannot send private patient data via open email channels. The information must be transmitted securely, typically using encryption. HIPAA defines the types of data used to uniquely identify a patient. This includes names, birth dates, admission dates, telephone/fax numbers, Social Security numbers, medical record numbers, health plan beneficiary numbers, and biometric identifiers like fingerprints. HIPAA

PIPEDA (Canada)

The Personal Information Protection and Electronic Documents Act (PIPEDA) protects personal

information from improper disclosure during commercial transactions, activities involving federal work, and business dealings within Canada as well as internationally. The act also provides guidelines for the gathering, use, and storage of data. PIPEDA

Basel II Accord (EU)

Basel II is a global standard for risk management in financial institutions. The accord seeks to ensure the privacy of financial information when transferred across international borders. It also presents guidelines on the disclosure of private information. Basel II Accord

Retention

Sarbanes-Oxley (US)

The Public Company Accounting Reform and Investor Protection Act of 2002, also known as the Sarbanes-Oxley Act (SOX), was drafted principally in response to the corporate corruption and financial scandals rampant at the turn of the millennium. Also known as the "Enron Law," Sarbanes-Oxley provides severe criminal penalties, including prison sentences, for corporate executives who destroy documents and business information. The act also specifies a records retention period of seven years and defines record types, such as physical and electronic documents and correspondence. SOX

SEC Rule 17a-4 (US)

The US Securities and Exchange Commission (SEC), which regulates financial organizations, has implemented a comprehensive and specific set of rules for the management of electronic communication. These mandates include SEC Rule 17a-4, which requires storage of duplicate copies and maintenance of indices. The rule also mandates the ability to present stored messages for inspection and review within a reasonable time frame, typically 24 hours. The SEC regulations and SOX overlap in that both address auditability and accountability of financial organizations, as well as record keeping and the protection of investors' private information. SEC Rule 17a-4

Title 21 Code of Federal Regulations (US)

Part 11 of Title 21 of the Code of Federal Regulations (CFR) for the Food and Drug Administration focuses on electronic records and signatures relevant to the pharmaceutical industry. The code specifies criteria for acceptance of electronic records, signatures, and handwritten signatures affixed electronically to documents. Title 21 CFR

Data Protection Act 1998 (UK)

The United Kingdom's Data Protection Act 1998 specifies that personal information held electronically must be secured and retained for defined periods, after which it must be destroyed. It also includes rules on the transfer of personal data. DPA 1998

ISO 15489 (Worldwide)

The International Organization for Standardization (ISO) has released ISO 15489—Information and Documentation, Records Management. This standard offers guidelines on the classification, conversion, destruction, disposition, migration, preservation, tracking, and transfer of records. ISO 15489

FSA (UK)

The Financial Services Authority (FSA) sets policies and standards for records management concerning the review, retention, and destruction of documents, computer files, email, and Web pages. The FSA defines retention schedules for various financial records, ranging from three years to indefinitely. FSA also draws a distinction between emails that contain information about business transactions (records) and those that contain no business information (ephemeral), and establishes storage and retention guidelines for both. FSA

Monitoring

NASD Rule 3010 (US)

The National Association of Securities Dealers (NASD) Rule 3010, as applied to email, requires that management be able to perform routine sampling and inspect customer communications to ensure that they are in accordance with regulations. NASD Rule 3010

NASD 2711(US)

The National Association of Securities Dealers (NASD) Rule 2711 ensures trust in the public markets by governing that investment banking must be run separately from research and trading, which includes all email and digital communications. NASD 2711

RIPA (UK)

The Regulation of Investigatory Powers Act (RIPA) 2000 addresses the interception of electronic communications as part of an investigative action and under what circumstances this information would be disclosed. RIPA

PCI DSS (US)

The Payment Card Industry (PCI) Data Security Standard (DSS) provides guidelines for the protection of credit card holder information, including the use of encryption, the storage of secure data, and access control methods. PCI DSS

E-Discovery

FRCP Rules 26 and 30(b) (US)

In December 2006, the Federal Rules of Civil Procedure (FRCP) were amended to include regulations concerning the processes for electronic discovery (e-discovery) and the implementation of a legal hold on email. According to Rule 26, organizations now must confer with the opposing party much earlier in the litigation process, and they must plan the way that electronic evidence will be collected, preserved, produced, and transferred. As part of this rule, IT staff must determine the accessibility of the data and develop a map of all data sources. FRCP Rule 30(b) calls for an expert IT witness to be designated. FRCP Rules 26 and 30(b)

Notification

SB 1386 (US)

The California Information Practices Act, SB1386, mandates that companies must notify consumers when they suspect or know that unencrypted personal information has been improperly disclosed, stolen, or lost. The company must notify those California customers directly affected as well as organizations doing businesses with customers in the state. Proper notifications of any suspected or actual improper disclosure include emails, Web postings, and media alerts. If all the information disclosed was encrypted, then notifications are not required. SB 1386 As of April 2007, 35 states have implemented similar legislation to protect their citizens. View a list of the other states that have passed comparable bills at current state list.