Compliance Management

Janco Associates, Inc.

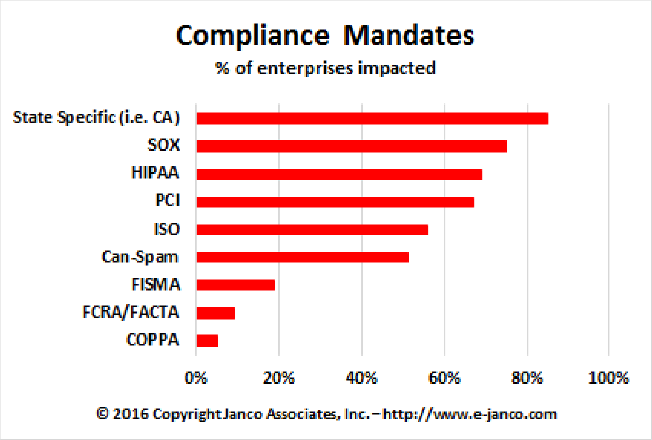
Table of Contents

License Conditions 1
Table of Contents 2
Compliance Management 3
Compliance Requirements 3
Record Management, Retention, and Destruction 3
ISO Security Domains 5
ISO 27000 6
HIPAA 12
Gramm-Leach-Bliley (Financial Services Modernization) 17
FISMA 18
FCRA 18
FCTA 18
COPPA 18
FTC Information Safeguards 19
Sarbanes-Oxley Act 19
State Security Breach Notification Laws 20
California SB 1386 Personal Information Privacy 22
Massachusetts 201 CMR 17.00 Data Protection Requirements 22
Implementation 23
Understand the enterprise's requirements 23
Understand the enterprise and its associated system of internal controls 23
Define the compliance processes, metrics, and success criteria 24
Identify all in-scope IT components 24
Collect fine-grain user and system activities 24
Begin a structured implementation process 24
Validate compliance status to auditors 25
Substantiate reports and alerts 25
Version History 26

Compliance Management

Compliance is not an isolated IT project; it's an enterprise wide endeavor that requires cooperation between business units and a deep understanding of the requirements, regulations, mandates and IT controls necessary for your industry and business. Compliance is as a business requirement that requires a cross functional approach, involving people, processes and technology across the enterprise. Taking the steps necessary to understand, define and implement the appropriate IT controls and frameworks for your business will simplify compliance and reduce the costs and resources involved in completing compliance related tasks.

More small and mid-sized business are impacted by state mandated (i.e. California, Massachusetts, New York, and others) than federal and SEC mandates.



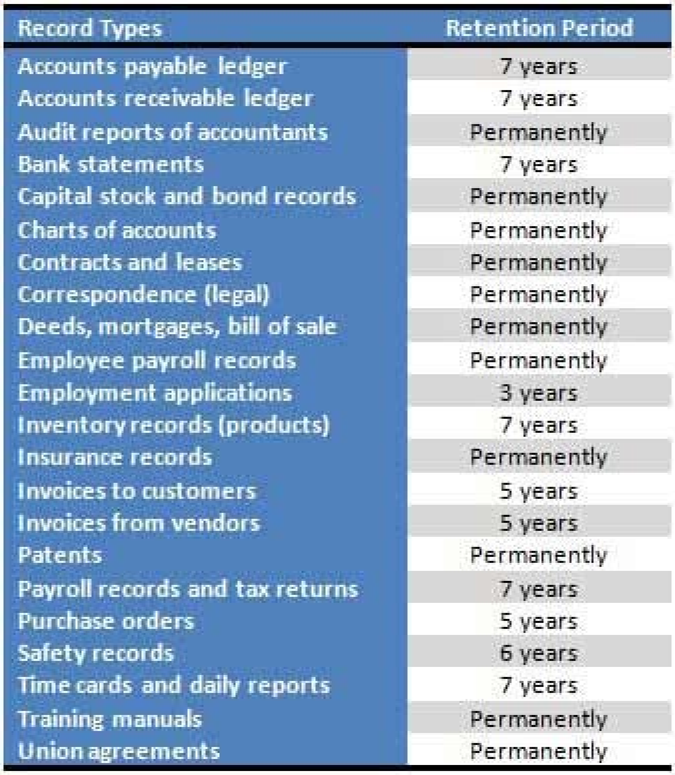
© 2016 Copyright Janco Associates, Inc. – http://www.e-janco.com

Compliance Requirements

Record Management, Retention, and Destruction

The reality is that while regulatory compliance data, including Sarbanes-Oxley, ISO, financial or HIPAA medical, require long-term retention, many other common application data for almost every business, including those that do not fall under regulatory requirements, can benefit from - if not require - long–term data retention. The notion is to think beyond regulatory compliance. In other words, organizations of all sizes need and rely on information, both current and past.

A record is essentially any material that contains information about your company's plans, results, policies or performance. In other words, anything about your company that can be represented with words or numbers can be considered a business record – and you are now expected to retain and manage every one of those records, for several years or even permanently depending on the nature of the information. The need to manage potentially millions of records each year creates many new challenges for your business, and especially for your IT managers who must come up with rock-solid solutions to securely store and manage all this data.



Record Types	Retention Period
Accounts payable ledger	7 years
Accounts receivable ledger	7 years
Audit reports of accountants	Permanently
Bank statements	7 years
Capital stock and bond records	Permanently
Charts of accounts	Permanently
Contracts and leases	Permanently
Correspondence (legal)	Permanently
Deeds, mortgages, bill of sale	Permanently
Employee payroll records	Permanently
Employment applications	3 years
Inventory records (products)	7 years
Insurance records	Permanently
Invoices to customers	5 years
Invoices from vendors	5 years
Patents	Permanently
Payroll records and tax returns	7 years
Purchase orders	5 years
Safety records	6 years
Time cards and daily reports	7 years
Training manuals	Permanently
Union agreements	Permanently

Record Retention Periods

Janco (http://e-janco.com/recordmanagementpolicy.html) has a Record Management, Retention, and Destruction policy. It is a detail template which can be utilized on day one to create a records management process. Included with the policy are forms for establishing the record management retention and destruction schedule and a full job description with responsibilities for the Manager Records Administration.

ISO Security Domains

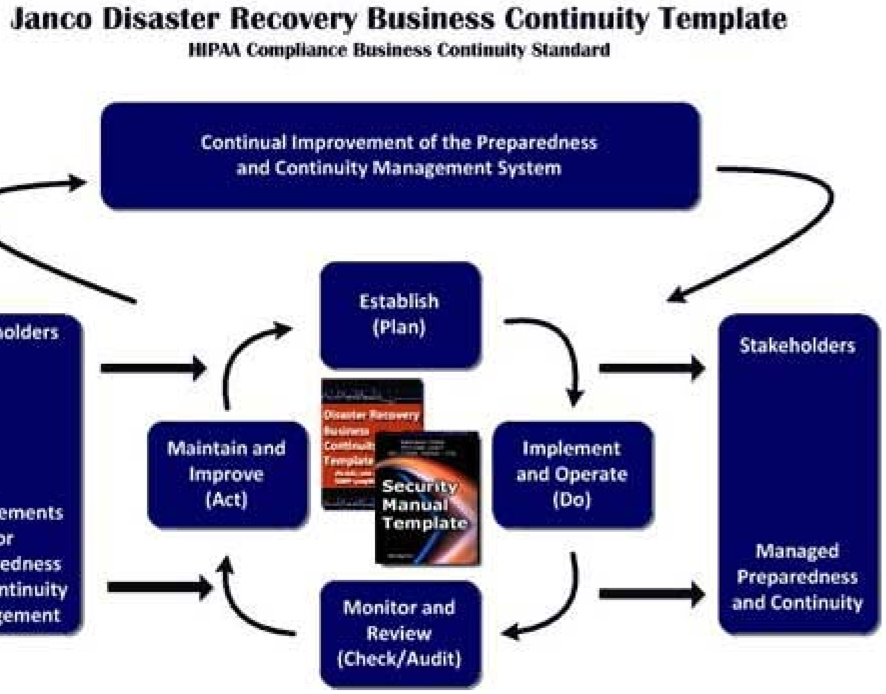
The International Standards Organization (ISO) has developed two specifications on the governance of information security, ISO 17799 and ISO 27001. Both have originated from British Standards, BS7799 parts 1 and 2, which have been used to certify over 2,500 organizations around the world. ISO 17799 is an international code of practice, or implementation framework, for information security best practices. ISO 27001 serves as the auditing and certification standard for the ISO 17799 framework with 133 information security controls covering eleven domains and also specifies how to design an ISO-certified Information Security Management System (ISMS). Further, ISO 27001 also specifies the Plan-Do- Check-Act (PDCA) model for continual quality improvement, which is the same PDCA model used in ISO 9001 Total Quality Management (TQM) initiatives. According to the Institute of Internal Auditors (IIA), the PDCA cycle helps “the organization to know how far and how well it has progressed” and “influences the time and cost estimates to achieve compliance.” BSI Management Systems, the world’s largest ISO certification body and the author of BS7799 standards, defined the ISMS as “a systematic approach to managing sensitive company information so that it remains secure. ISMS encompasses people, processes, and IT systems.”

The ISO Domain standard is comprised of 11 distinct domains of information security. The Security Manual Template addresses each throughout the template with particular emphasis in the sections outlined below:

ISO Security Domain	Security Manual Template Sections
Security Policy	• Security General Policy Chapter
Organization of Information Security	• Responsibility Chapter
Asset Management	• Insurance Chapter
Human Resources Security	• Physical Control Chapter • Facility design, construction, and operational considerations Chapter
Physical and Environmental Security	• Physical Control Chapter • Data and Software Security Chapter
Communications and Operations Management	• Responsibilities Chapter
Access Control	• Physical Control Chapter • Access Control Chapter
Information Systems Acquisition, Development and Maintenance	• Processes, Forms, and Checklist - Appendix
Information Security Incident Management	• Incident Reporting Procedure - Appendix
Business Continuity Management	• Internet and IT Contingency Planning Chapter
Compliance	• Minimum and Mandated Security Standards and Best Practices to Manage Compliance Chapters

HIPAA

The U.S. Department of Health and Human Services (HHS) has published a final rule amending Health Insurance Portability and Accountability (HIPAA) regulations by adding provisions that require notice to patients and others of a "breach," or disclosure of unsecured protected health information (PHI), by HIPAA-covered entities and business associates (the "HIPAA Rule"). The Federal Trade Commission published the Health Breach Notification Rule to address breach notification by personal health-records vendors (the "FTC Rule").

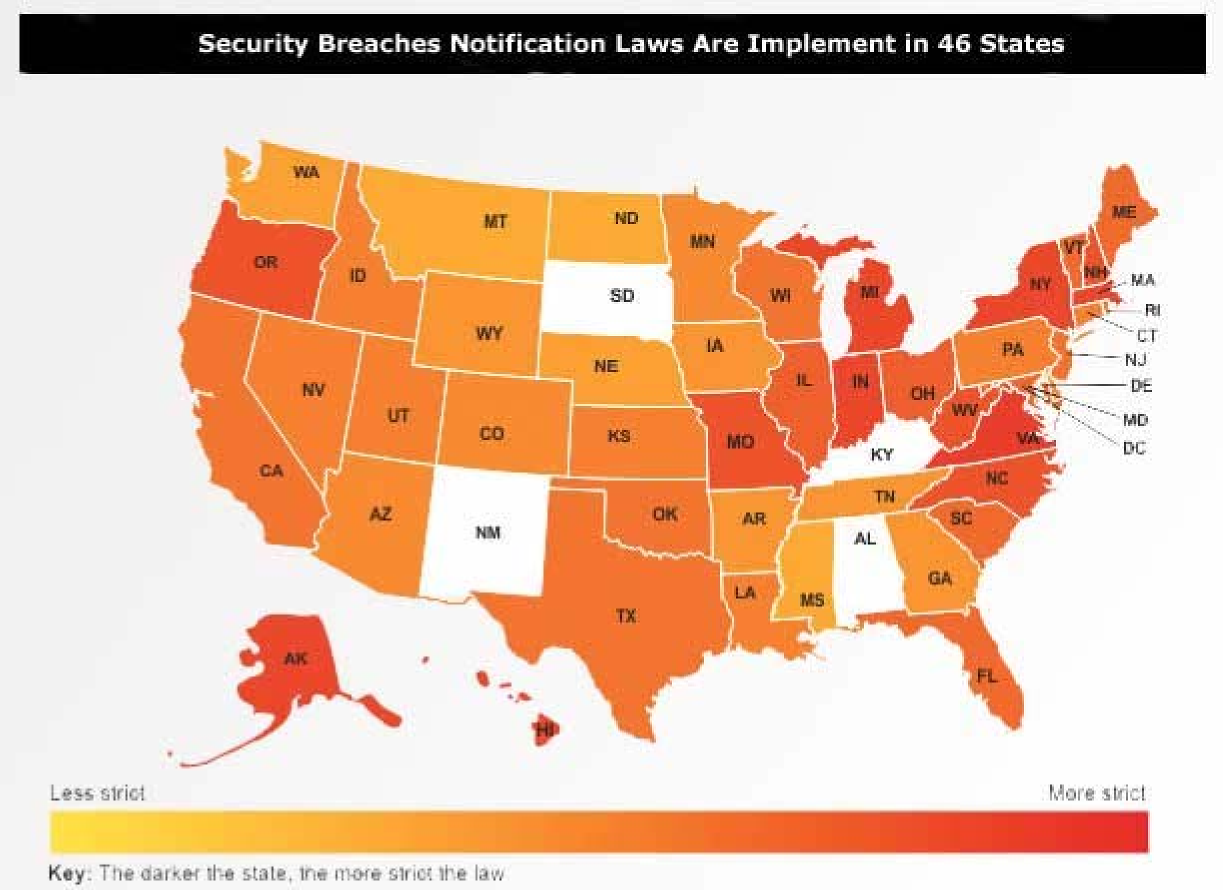

Janco Disaster Recovery Business Continuity Template
HIPAA Compliance Business Continuity Standard
Continual Improvement of the Preparedness and Continuity Management System
Stakeholders
Requirements for Preparedness And Continuity Management
Establish (Plan)
Maintain and Improve (Act)
Implement and Operate (Do)
Monitor and Review (Check/Audit)
Disaster Recovery Business Continuity Template
Security Manual Template
Stakeholders
Managed Preparedness and Continuity

See http://www.e-janco.com/DRP_and_Security.htm

In general, the HIPAA Rule requires that a HIPAA-covered entity (a healthcare provider, payer or clearinghouse) notify an individual when unsecured PHI has been improperly disclosed. The entity must also notify HHS regarding confirmed breaches, either through an annual report or sooner, depending on the number of individuals affected. In some instances, media must also be notified. The HIPAA Rule specifies the content of the notice. Integral components of the HIPAA Rule are definitions of "unsecured PHI" and "breach," which exclude unauthorized uses and disclosures that do not violate the HIPAA Rule and do not significantly harm an individual. The HIPAA Rule and its preamble reveal a new twist in HHS's perspective on when, for notice purposes, a business associate is acting as an agent, as opposed to an independent contractor—a potentially confusing aspect of the HIPAA Rule.

State Security Breach Notification Laws

The landscape for CIOs and protection of personal information continues to become more complex as more states add breach notification laws. Currently forty-six states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information.



Version History

Version 3.0

- Updated meet the latest ISO requirements
- Updated to reflect US, EU, and state mandated requirements
- Added sections on FISMA, FCRA, FACTA and COPPA compliance requirement

Version 2.2

- Updated with a table of State Notification mandated requirements

Version 2.1

- Updated text to reflect compliance requirements as of January 2012
- Added HIPAA section

Version 2.0

- Updated text to reflect compliance requirements as of January 2011