Compliance Management

2025

Table of Contents

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 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 businesses are impacted by state-mandated (i.e. California, Massachusetts, New York, and others) than federal and SEC mandates.

Compliance Requirements

Record Classificati

The reality is that whi ...financial, or HIPAA medical, requir ...or almost every business, includ ...benefit from - if not require - long- ...compliance. In other words, organ ...and past.

A record is essentially any material that contains information about your company's plans, results, policies, or performance. Anything about your company that can be represented withwords 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.

Janco's (https://e-janco.com/recordmanagementpolicy.html) Record Classification, Management, Retention, and Destruction policy. It is a detailed template that 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.

Record Classification Types	Retention Periods
Accounts Payable Ledger	7 Years
Accounts Payable Transaction	7 Years
Accounts Receivable Ledger	7 Years
Accounts Receivable Transaction	7 Years
Accountant Audit Reports	Permanently
Bank Statement	7 Years
Capital Stock and Bond Records	Permanently
Chart of Accounts	Permanently
Contracts and Leases	Permanently
Correspondence (legal)	Permanently
Deeds, Mortgages, Bill of Sale	Permanently
Employee Payroll Records	Permanently
Contractor Payment Records	Permanently
Employment Applications	3 Years
Inventory Records (products)	7 Years
Insurance Records	Permanently
Training Manuals	Permanently
Union Agreements	Permanently

Record Classification and Retention Periods

ISO Security Domains

The International Standards Organization (ISO) has developed two specifications for 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 continuous 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	
Information Systems Acqu and Maintenance	
Information Security Incid	
Business Continuity Mana	
Compliance	nd s

ISO 27000

The ISO 27000 series[1] of standards have been specifically reserved by ISO for information security matters. This, of course, aligns with several other topics, including ISO 9000 (quality management) and ISO 14000 (environmental management).

The 27000 series is a set of individual standards and documents defined as follows:

ISO 27001 - The specification for an Information Security Management System (ISMS) replaced the BS7799-2 standard.

An Information Security Management System provides a wide variety of benefits, including:

- A vehicle for the identification, classification, and protection of information in any form
- Forming the system by which multiple legal, regulatory, and business requirements can be identified, analyzed, addressed, managed, and monitored
- Bridging the gap between information security and the business
- Enabling business-friendly, risk-based management and information security

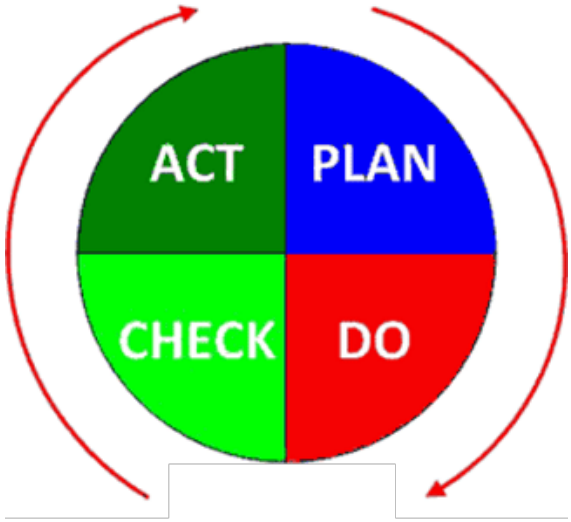
[1] *http://www.27000.org - The ISO 27000 series of standards have been specifically reserved by ISO for information security matters.*

- Showing proof of activities, due care, and due diligence
- Accelerating information security program maturity, proactive management, and the ability to change rapidly
- Assists in the definition of strategies, activities, management, standards, guidance, roles, and responsibilities
- Providing competitive advantage, while denying it to your competitors
- Forming the foundation and mechanism for informed decision-making
- Enhancing corporate governance and compliance-related activities
- Increasing efficiencies and consistency – bringing order to centralized or distributed environments

ISO 27002 – The ISO 27002 standard is a renaming of the ISO 17799 standard, which is a code of practice for information security. It outlines controls and control mechanisms, which may be implemented subject to the guidance provided within ISO 27001.

The standard "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization". The actual controls listed in the standard are intended to address the specific requirements identified via a forma uide for the development of "orga nt practices and to help build cont

ISO 27003 – This is a This will be the official number of ation of an ISMS (Information Security Management System). The purpose of this proposed development is to provide help and guidance in implementing ISMS. This will be a quality control standard when it is released. ISO 27003 will focus on utilizing the Plan-Do-Act-Check (PDCA) method when establishing, implementing, reviewing, and improving the ISMS.



Defining Compliance Management Audit Scope

Annual Audit Scope

- **Active Directory Terms vs. Systems Terms** - Conduct an annual audit/comparison of terminations in Active Directory vs. terminations in all systems
- **Verify Accounts with Administrative Privileges Audits** - Core Systems Run audits listing all users who have administrative privileges to core systems. Administrative privileges will be validated via an enterprise's role-based access matrix.

Semi-Annual Audit Scope

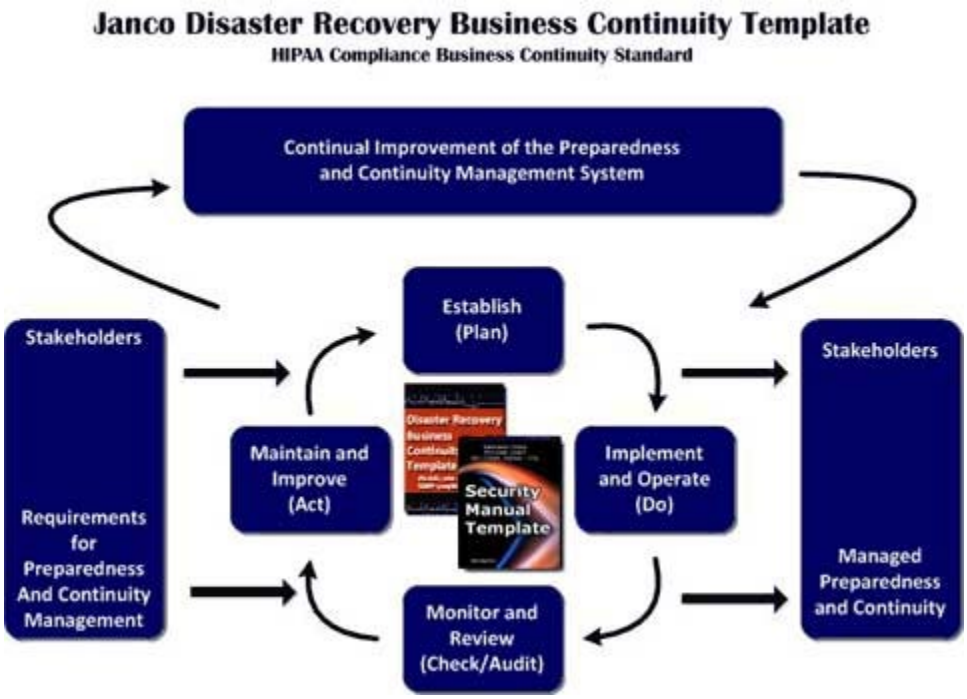
- **Disaster Recovery Plan Test / Audit – Local the enterprise's data center** - Conduct a tabletop test of the local enterprise's disaster recovery/business continuity plan and update as required for change management.

Quarterly Audit Scope

- **Change** … members to confirm … cessary based on … ermination with the …
- **Cyberse** … al simulatio… … e enterprise's policies and plans and make updates accordingly.
- **Day of Week / Time of Day Audit** - Create a detailed report of random user access to core based on the user's normal work hours. For example, if a user normally works on the weekend, the audit should check to see if the user id and password were used during the week, and visa versa. If a user normally works during the day, the audit should check to see if the user id and password were used during the night, and visa versa. Exceptions could indicate that a user-id is being shared or used in an unauthorized manner.
- **Departmental Downtime Procedures – Mock Test Audits** - Conduct periodic mock tests of departmental downtime procedures. The enterprises should randomly pick departments to meet with to review their downtime procedures in a tabletop test and document the meetings and audit findings.
- **Disabled AD Accounts Deletion Audits** - Conduct audits of all disabled Active Directory accounts and delete all accounts that have been disabled for over 30 days.
- **Random Audits** - Randomly pick a procedural requirement from a mandated requirement, policy, and audit operational compliance.
- **Intrusion Vulnerability Audit** - Create a quarterly report that contains exceptions when comparing current server OS security patches vs. the patch list. The report should be reviewed by operational staff and mitigation action items will be assigned accordingly.

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").

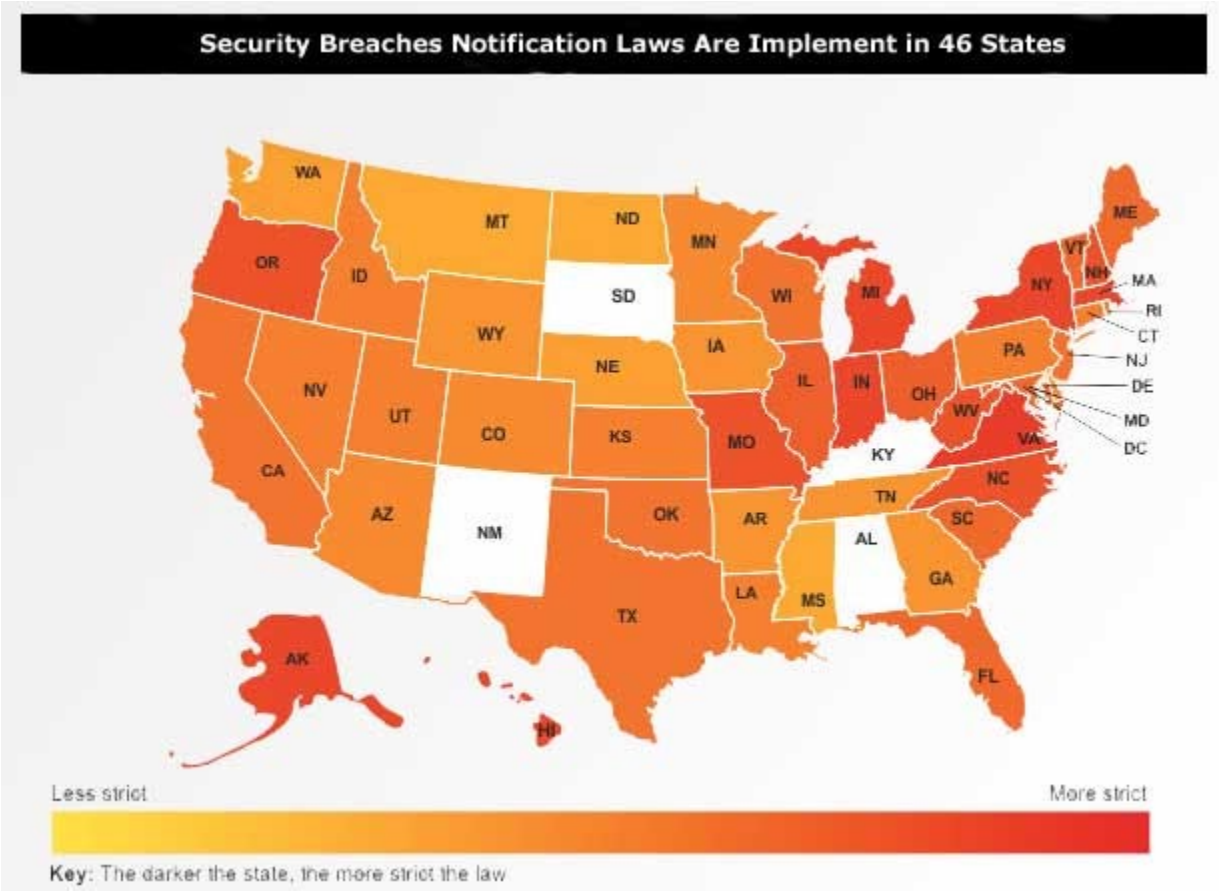


See https://e-janco.com/drp_and_security.htm

In general, the HIPAA Rule requires that a HIPAA-covered entity (a healthcare provider, payer, or clearinghous ly disclosed. The entity must a n annual report or sooner, depe s, the media must also be notif l components of the HIPAA Rule a unauthorized uses and disclosu 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 the 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.



State Notification Requirements Table

Alaska	Alaska Stat. § 45.48.010 et seq.
Arizona	
Arkansas	
California	
Colorado	
Connecticut	
Delaware	
Florida	
Georgia	Ga. Code §§ 10-1-910, -911
Hawaii	Haw. Rev. Stat. § 487N-2
Idaho	Idaho Stat. §§ 28-51-104 to 28-51-107
Illinois	815 ILCS 530/1 et seq.
Indiana	Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.
Iowa	Iowa Code § 715C.1

Compliance Tools Purchase Options

Compliance Infrastructure Governance Options	COBIT	Compliance				SOX			
		Std	S	G	P	Std	S	G	P
Compliance Management White Paper	X	X	X	X	X				
PCI Audit Program	X		X	X	X				
Compliance Management Job Descriptions	X		X	X	X				
Security Audit Program	X		X	X	X	X	X	X	X
Supply Chain Security Audit Program - ISO 28000	X		X	X	X				
HIPAA Audit Program	X		X	X	X	X	X	X	X
Record Management and Destruction Policy Template	X			X	X	X	X	X	X
Sensitive Information Policy	X			X	X	X	X	X	X
Security Policies and Procedures Template	X				X	X	X	X	X
Disaster Recovery Business Continuity Template	X					X	X	X	X
Practical Guide for IT Outsourcing	X					X	X	X	X
Business and IT Impact Questionnaire	X					X	X	X	X
Safety Manual Template						X	X	X	X
Threat & Vulnerability Assessment Tool	X					X	X	X	X
Job Description Chief Security Officer	X		X	X	X	X	X	X	X
Internet and IT Position Descriptions HandiGuide	X						X	X	X
331 Internet and IT Position Descriptions								X	X
IT Service Management (ITSM) Service Oriented Architecture	X								X
IT Infrastructure, Strategy, and Charter Template	X								
SLA Policy Template with Sample Metrics	X								
KPI Metrics for the Internet, IT, and Service Management	X								
IT Salary Survey	X								

Legend: S-Silver G-Gold P-Platinum; Compliance-Compliance Management Kit, SOX-Sarbanes Oxley Compliance

Compliance Management Kit Versions

The Compliance Management Kit comes in 3 separate versions: Silver, Gold, and Platinum. In addition, each version can be acquired as a standalone item or with 12 or 24 months of update service.

Silver Edition

- Compliance Management White Paper
- ISO 28000 - Supply Chain Compliance Audit
- Security Audit Program - fully editable -- Comes in MS EXCEL and PDF formats -- Meets ISO 27001, 27002, Sarbanes-Oxley, PCI-DSS, and HIPAA requirements -- Over 400 unique tasks divided into 11 areas of audit focus which are divided into 39 separate task groupings including BYOD.
- PCI Audit Program - Word and PDF
- HIPAA Audit Program – Word and PDF
- Compliance Management Job Description Bundle (25 key positions) - Word Format - fully editable and PDF - Chief Compliance Officer (CCO), Chief Data Officer, Chief Mobility Officer, Chief Security Officer, Data Protection Officer, Director Electronic Commerce, Director IT Management and Controls, Director Sarbanes-Oxley Compliance, Manager Blockchain Architecture, Manager BYOD Support, Manager Compliance, Manager E-Commerce, Manager Enterprise Architecture, Manager Internet Systems, Manager Record Administration, Manager Transaction Processing, Manager Video, and Website Content, Manager Web Content, Manager Wireless Systems, PCI-DSS Administrator, System Administrators - Linux, System Administrators - Windows, System Administrators - UNIX, Webmaster, and Wi-Fi Network Administrator

Order at https://e-janco.com/session/add_product.aspx?detail=1&catalog=36kit

Gold Edition

- Compliance Management White Paper
- ISO 28000 - Supply Chain Compliance Audit
- Security Audit Program
- HIPAA Audit Program
- PCI Audit Program
- Compliance Management Job Description Bundle (25 key positions)
- Record Classification and Management Policy - Word - Policy that complies with mandated US, EU, and ISO requirements
- Privacy Compliance Policy that addresses the EU's GDPR and the latest California Consumer Privacy Act

Order at https://e-janco.com/session/add_product.aspx?detail=1&catalog=36kit

Platinum Edition

- Compliance Management White Paper
- ISO 28000 - Supply Chain Compliance Audit
- Security Audit Program
- HIPAA Audit Program
- PCI Audit Program
- Compliance Management Job Description Bundle (25 key positions)
- Record Classification and Management
- Privacy Compliance Policy that addresses the EU's GDPR and the latest California Consumer Privacy Act
- Security Manual Template - Word - 240 plus packed pages which are usable as-is. Over 3,000 companies worldwide have chosen this as the basis for their best practices to meet mandated US, EU, and ISO requirements

Order at https://e-janco.com/session/add_product.aspx?detail=1&catalog=36kit

COBIT Edition

A much more robust version of the Compliance Kit contains

- Compliance Management White Paper
- Record Classification Management Retention and Destruction Policy
- IT Infrastructure, Strategy, and Charter Template
- Disaster Recovery Business Continuity Template
- Practical Guide for IT Outsourcing
- Service Level Agreement Policy Template with Sample Metrics
- Metrics for the Internet, Information Technology, and Service Management
- IT Service Management (ITSM) Service Oriented Architecture (SOA)
- Internet and Information Technology Position Descriptions HandiGuide
- Security Policies and Procedures
- ISO 28000 - Supply Chain Compliance Audit
- Security Audit Program
- HIPAA Audit Program
- Business and IT Impact Questionnaire
- IT Salary Survey

Order at https://e-janco.com/session/catalog_items.aspx?catalog=209&detail=1

Appendix

Included as separate files:

Chief Compliance Officer Job Description

HIPAA Audit Program

PCI Audit Program

ISO 28000 - Supply Chain Compliance Audit Program

Security Audit Program

Compliance Management Job Description Bundle

Privacy Compliance Policy

Record Classification, Management, Retention, Destruction Policy

Version History

2025

- Added section defining compliance mandates audit scope
- Updated all included job description
- Updated all included forms
- Updated all included policies

2024

- Added job description for the Chief Compliance Officer
- Updated all of the included items to the latest versions

2023

- Added section on ISO 28000 Supply Chain to the main body
- Added ISO 28000 - Supply Chain Compliance Audit
- Updated all included job description
- Updated all included forms
- Updated all included policies

2022

- Added a standalone version of the HIPAA Audit Program

2022

- Updated meet the latest mandated requirements
- Added Compliance Management Governance Purchase options table

2021

- Updated meet the latest mandated requirements