Compliance Management

White Paper

Jancd Associates, Inc.

License Conditions

Published by:
Janco Associates Inc.

e-mail - support@e-janco.com

Printed in the United States of America

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 Classification, 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. 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
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/Sheets & Daily Reports	7 Years
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	• 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

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

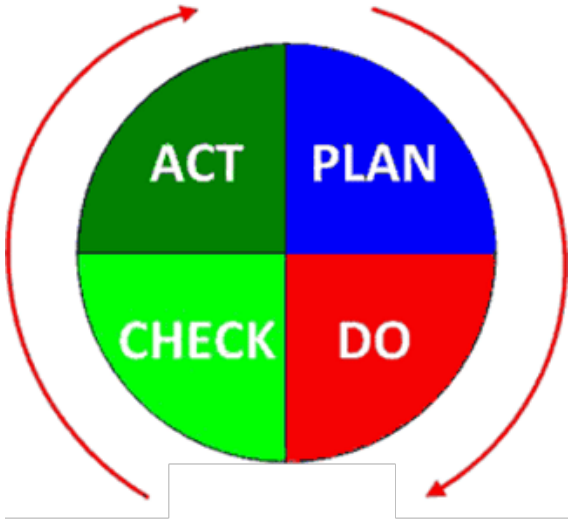
[1] *http://www.27000.org - The ISO 27000 series of standards have been specifically reserved by ISO for information security matters.*

- 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 formal risk assessment. The standard is also intended to provide a guide for the development of "organizational security standards and effective security management practices and to help build confidence in inter-organizational activities".

ISO 27003 – This is a PROPOSED Standard, which has yet to be completely defined. This will be the official number of a new standard intended to offer guidance for the implementation 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.



ISO 27004 - This is the designated number for a PROPOSED standard covering information security, system management, measurement, and metrics.

ISO 27005 – This is the name of a PROPOSED standard emerging standard covering information security risk management. As with the other standards within the ISO 27000 series, no firm dates have been established for its release. However, it will define the ISMS risk management process, including the identification of assets, threats, and vulnerabilities. This is the ISO number assigned for an emerging standard for information security risk management.

ISO 27006 - This standard offers guidelines for the accreditation of organizations that offer certification and registration concerning ISMS.

Information is an asset that, like other important business assets, is essential to an enterprise's business and consequently needs to be suitably protected. This is especially important in the increasingly interconnected business environment. Because of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities (see OECD Guidelines for the Security of Information Systems and Networks).

Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or how it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities.

Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software, and hardware functions. These controls need to be established, implemented, monitored, reviewed, and improved, where necessary, to ensure
that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

ISO 27000[2] establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO 27000 (27001 and 27002) contains best practices of control objectives and controls in the following areas of information security management:

- Security policy;
- Organization of information security;
- Asset management;
- Human resources security;
- Physical and environmental security;
- Communications and operations management;
- Access control;
- Information systems acquisition, development, and maintenance;
- Information security incident management;
- Business continuity management; and
- Compliance

The control objectives and controls in ISO 27000 (27001 and 27002) are to be implemented to meet the requirements identified by a risk assessment. ISO 27001 and ISO 27002 are intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.[3]

Thus ISO 27000 is an information security code of practice. The formal document includes several sections, covering a wide range of security issues. This security manual meets these objectives. The focus areas defined by 17799 and the objectives are as follows:

Risk Assessment and Treatment

Fundamentals of security risk analysis.

System Policy

Objective: To provide management direction and support for information security

Organizing Information Security

Objectives:

- To manage information security within the organization
- Maintain the security of information and processing facilities for external parties.

[2] *Formerly was ISO 17799*

[3] *International Standards Organization*

Asset Management

Objectives:

- Achieve and maintain appropriate protection of organizational assets.
- Ensure that information receives an appropriate level of protection.

Human Resources Security

Objectives:

- Ensure that employees, contractors, and third parties are suitable for the jobs they are considered for, understand their responsibilities, and reduce the risk of abuse (theft, misuse, etc.).
- Ensure that the above are aware of IS threats and their responsibilities, and able to support the organization's security policies
- Ensure that the above exits the organization in an orderly and controlled manner.

Physical and Environmental Security

Objectives:

- Prevent unauthorized physical access, interference, and damage to the organization's information and premises.
- Prevent loss, theft, and damage of assets
- Prevent interruption from the organization's activities.

Communications and Operations Management

Objectives:

- Ensure the secure operation of information processing facilities
- Maintain the appropriate level of information security and service delivery, aligned with 3rd party agreements
- Minimize the risk of systems failures
- Protect the integrity of information and software
- Maintain the availability and integrity of information and processing facilities
- Ensure the protection of information in networks and the supporting infrastructure
- Prevent unauthorized disclosure, modification, removal, or destruction of assets.
- Prevent unauthorized disruption of business activities.
- Maintain the security of information and/or software exchanged internally and externally.
- Ensure the security of e-commerce services
- Detect unauthorized information processing activities

Access Control

Objectives:

- Control access to information
- Ensure authorized user access
- Prevent unauthorized access to information systems
- Prevent unauthorized user access and compromise of information and processing facilities
- Prevent unauthorized access to networked services
- Prevent unauthorized access to operating systems
- Prevent unauthorized access to the information within application systems
- Ensure information security for mobile computing and telecommuting facilities

Information Systems Acquisition, Development, and Maintenance

Objectives:

- Ensure that security is an integral part of information systems
- Prevent loss, errors, or unauthorized modification/use of information within applications
- Protect the confidentiality, integrity, or authenticity of information via cryptography
- Ensure the security of system files
- Maintain the security of application system information and software
- Reduce/manage risks resulting from the exploitation of documented vulnerabilities

Information Security Incident Management

Objectives:

- Ensure that security information is communicated in a manner that allows corrective action to be taken in a timely fashion
- Ensure a consistent and effective approach is applied to the management of IS issues

Business Continuity Management

Objectives:

- Counteract interruptions to business activities and protect critical processes from the effects of major failures/disasters
- Ensure timely resumption of the above

Compliance

Objectives:

- Avoid the breach of any law, regulatory or contractual obligation, and of any security requirement.
- Ensure systems comply with internal security policies/standards
- Maximize the effectiveness of and minimize associated interference from and to the systems audit process

ISO 28000

This International Standard specifies the requirements for a security management system, including those aspects critical to security assurance of the supply chain. Security management is linked to many other aspects of business management. Aspects include all activities controlled or influenced by organizations that impact supply chain security. These other aspects should be considered directly, where and when they have an impact on security management, including transporting these goods along the supply chain.

This International Standard applies to all sizes of organizations, from small to multinational, in manufacturing, service, storage, or transportation at any stage of the production or supply chain that wishes to:

- establish, implement, maintain, and improve a security management system
- assure conformance with the stated security management policy
- demonstrate such conformance to others
- seek certification/registration of its security management system by an Accredited third-party Certification Body or
- make a self-determination and self-declaration of conformance with this International Standard.

There are legislative and regulatory codes that address some of the requirements in this International Standard.

It is not the intention of this International Standard to require duplicative demonstration of conformance.

Organizations that choose third-party certification can further demonstrate that they are contributing significantly to supply chain security.

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 of Status Workforce Audits –** Create reports of workforce members to confirm the user's access based on job code. Make changes when necessary based on the feedback from the workforce, and coordinate any access termination with the covered entity facilities department.
- **Cybersecurity Tactical Simulations** - Conduct Cybersecurity tactical simulations (tabletop) to cover the latest known cyber threats against the 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.

- **PCI Data in Transit Audit** - Conduct an audit of the enterprise's PCI data in transit on to confirm that it is encrypted and conforms with all the enterprise's standards.
- **Random Facility Walk Through Audits** - Randomly audit work areas throughout the organization. The intent of the audit is to protect the enterprise's information and improve staff awareness. Immediate feedback of exceptions should be provided to staff on-site, documented, and reported to the Compliance / Privacy Officer. The Compliance / Privacy Officer can take part in any random audits upon request. Audits can be conducted during or after normal business hours.
- **Terminated Workforce Audits** - Create reports of workforce members to confirm that users are still active. Make deletions when necessary based on the feedback from the workforce, and coordinate any facility access termination with the covered entity facilities department.
- **Verify Accounts with Administrative Privileges Audits** - Active Directory Run audits listing all users who have administrative privileges to the active directory. Administrative privileges will be validated via the enterprise's role-based access matrix.
- **Virus Detection Alerts** - Conduct a random review of the email alerts along with a random check of PC workstations and remote access devices to confirm the integrity of the virus protection software.

Monthly Audit Scope

- **Audit physical access logs to the enterprise's secure locations** - including the enterprise's data center and network closets.
- **Change of the enterprise's workforce job status audits – core systems** – Create daily reports for workforce members (also including temporary and voluntary employees) that have changed their job status and will distribute the reports to the system administrator. The the enterprise's will conduct a random audit of 10% and confirm with the system administrators and facility managers that all system (on-site and remote) and facility access is still appropriate.
- **Change of status workforce Audits for covered users** - Create reports of users with active sign-on user ids to core systems and provide the report to the covered entity staff for confirmation. Make changes when necessary based on the feedback from the office, and coordinate any facility access termination with the covered entity facilities department.
- **Employee as a client (Peer access audit)** - Create reports for audits of up to three clients who are employees. The report should include user access to core clinical information. Randomly select users for further review and send the report to the user's manager. The user's manager should conduct a detailed review and identify exceptions and / or sign off.
- **Same last name** - Filter the audit log to check for records where the client and the employee both have the same last name.
- **Same street** - Filter the audit log to check for records where the client and the employee live on the same street.

- **Terminated Workforce Audits – Core systems** - Create reports of terminated workforce members (also including temporary and voluntary employees) to confirm that all system (on site and remote) and facility access has been terminated.
- **Terminated the enterprise's Workforce Audits – Active Directory** - Create reports of terminated workforce members (also including temporary and voluntary employees) to confirm that all system (on site and remote) and facility access has been terminated. Unauthorized or inappropriate access audits Create a report of 5 random users from various departments over a reasonable time-frame (e.g. two (2) week period). The report will include what data and functions the users accessed, and will be sent to the user's manager for review and sign off.
- **Unauthorized or inappropriate record access** - Create a report for random users and locations that includes user remote access to core over a reasonable time frame (e.g. two (2) week period). The report should include what data and functions the users accessed, and should be sent to the office Privacy Officer who should conduct a detailed review and identify exceptions and / or sign off.
- **Failed Login Attempts to Network Audits** - Conduct Audit based on Enterprises' Guidance for Security.
- **Post Department Moves Audits** - Conduct audits of user attempts to access inappropriate Internet sites, including 100% of user attempts to blocked sites.

Real-Time Compliance Monitoring and Reporting

- **Login Fails Audits** - Conduct audits of user log-in attempts from the covered entity domain to include 100% of failed user login attempts that are greater than fifteen (15).

Addition to Each Compliance Management Audits' Scope

- **Audit of all wireless devices** - Conduct audits of covered entity department moves to confirm Send controls, both physical and technical.
- **Enterprises' Guidance for Security** - Audit access to sensational user visits. A sensational user visit is defined as a visit directly connected to high-security data, users, media events, matters of public record, or a high-profile user figure (i.e., CEO), and other VIPs. The audit may be triggered by notification by Public Relations, Senior Administration, or the media. The audit will include 100% of user attempts to confidential data, personal identifying information and/or demographic data.
- **Internet Audits** - Review the inventory of laptops / BOYDs / tablets

Governmental Mandates

California Consumer Privacy Act (CaCPA)

CaCPA places new burdens on companies that do business with California residents. This includes both domestic and international organizations. Who must comply with CaCPA?

- Companies that serve California residents and have at least $25 million in annual revenue
- Companies of any size that have personal data on at least 50,000 people
- Companies that collect more than half of their revenues from the sale of personal data

Once California regulators notify a company that they violate CaCPA, companies have 30 days to comply. If the issue isn't resolved, there's a fine of up to $7,500 per record. In addition, the law allows for penalties of $100 to $750 per consumer per incident, or actual damages, whichever is greater.

What must companies do to comply

One of the first things they must do is add a visible footer on websites offering consumers the option to opt out of data sharing. If that footer is missing, consumers can sue. One shortcut that companies can follow if they do not share data is to put a comment in a common footnote that data is not shared.

CaCPA Mandates

The law originally covered employee data in addition to consumer data. That was amended to exclude employee data. Companies must allow consumers to choose not to have their data shared with third parties. That means that companies must be able to separate the data they collect according to the users' privacy choices. A California consumer has the right to find out what information a company collects about them.

After the access request, a company has 45 days to provide them a comprehensive report about what type of information they have, whether was it sold, and to whom, and if it was sold to third parties over the past 12 months, it must give the names and addresses of the third parties the data is sold to.

The CaCPA Mandates include:

- The bill grants a consumer a right to request a business to disclose the categories and specific pieces of personal information that it collects about the consumer, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of 3rd parties with which the information is shared.
- The bill requires a business to make disclosures about the information and the purposes for which it is used.

- The bill grants a consumer the right to request the deletion of personal information and would require the business to delete it upon receipt of a verified request, as specified.
- The bill grants a consumer a right to request that a business that sells the consumer's personal information or discloses it for a business purpose, disclose the categories of information that it collects and categories of information and the identity of 3rd parties to which the information was sold or disclosed.
- The bill requires a business to provide this information in response to a verifiable consumer request.
- The bill authorizes a consumer to opt out of the sale of personal information by a business and prohibits the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to the value provided by the consumer's data.
- The bill authorizes businesses to offer financial incentives for the collection of personal information.
- The bill prohibits a business from selling the personal information of a consumer under 16 years of age unless affirmatively authorized, as specified, to be referred to as the right to opt-in.
- The bill prescribes requirements for receiving, processing, and satisfying these requests from consumers.
- The bill prescribes various definitions for its purposes and would define "personal information" as a broad list of characteristics and behaviors, personal and commercial, as well as inferences drawn from this information. T
- The bill prohibits the provisions described above from restricting the ability of the business to comply with federal, state, or local laws, among other things.

California SB 1386 Personal Information Privacy

This regulation affects companies that do business with individuals living in California even if the ENTERPRISE is located outside of the state.

If unencrypted personal data is compromised, then ENTERPRISE must immediately disclose to the customer that a security breach has occurred.

COPPA

The Children's Online Privacy Protection Act of 1998 ["COPPA"] is a federal law set up to provide the parameters under which online operators can and cannot collect information from children under 13 years of age in the United States. COPPA compliance can be challenging and frustrating but is a must if you target this audience or know kids are using your offerings.

FCRA

The Fair Credit Reporting Act (FCRA) is a federal law (15 U.S.C. § 1681 et seq.) that regulates the collection, dissemination, and use of consumer information, including consumer credit information. Almost any type of background check that an employer requests to be used in the hiring process is considered a consumer report. In addition, Hire Level is considered a Consumer Reporting Agency. Employers must follow all FCRA requirements to remain in compliance.

FCTA

The Foreign Account Tax Compliance Act (FATCA) is a United States federal law whose intent is to enforce the requirement for United States persons (including those living outside the U.S.) to file yearly reports on their non-U.S. financial accounts to the Financial Crimes Enforcement Network (FINCEN). The law requires all non-U.S. (foreign) financial institutions (FFI's) to search their records for indicia indicating U.S. person status and to report the assets and identities of such persons to the U.S. Department of the Treasury. The FATCA is the revenue-raising portion of the 2010 domestic jobs stimulus bill, the Hiring Incentives to Restore Employment (HIRE) Act.

FISMA

FISMA requires federal agencies to implement a mandatory set of processes and system controls designed to ensure the confidentiality, integrity, and availability of system-related information. The processes and systems controlled in each federal agency must follow established Federal Information Processing Standards, National Institute of Standards and Technology standards, and other legislative requirements about federal information systems, such as the Privacy Act of 1974.

To facilitate FISMA compliance, GSA maintains a formal program for information security management focused on FISMA requirements, protecting GSA IT resources, and supporting the GSA mission. This program consists of policies, procedures, and processes to mitigate new threats and anticipate risks posed by new technologies. Designated GSA information system security managers and information system security officers implement information security requirements under FISMA requirements and GSA policies.

FTC Information Safeguards

The FTC Information Safeguards establishes rules to require standards for administrative, technical, and physical information security. It was one of the first to require that companies utilize a risk identification and assessment process to identify internal and external risks.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) sets specific compliance requirements on how your business does business with enterprises and individuals in the EU.

The EU requires that enterprises need to have consent or legitimate interests to use personal data. Whether you rely on consent or legitimate interests for your marketing, you need to do similar things to make sure you are GDPR compliant:

- Be clear with individuals about why you need their data at the point of collection
- Always use clear and concise language appropriate for your target audience
- Provide information at the point the data is collected. It cannot be hidden in small print.
- Give individuals control over their data. They should be able to decide whether to share their data with you or not.
- Under the GDPR principle of accountability, you should be able to demonstrate that you are compliant. This means recording the legal grounds for processing an individual's data.

Why Data is Captured

To capture personal data, the enterprise needs to demonstrate that they have a valid business or marketing reason to capture and retain data on an individual

- Validated that legitimate interests are the most appropriate lawful basis for processing
- Communicate how or why there is a need for an individual's data when it is collected
- Utilize a layered privacy notice/policy - A layered privacy notice puts the most important information upfront and then there is a more detailed privacy policy underneath it
- Inform Individuals on what the plan is for their data when it is collected
- Allow individuals to "opt out" of marketing
- Collect the minimum data necessary and delete records after use
    - Data needed for a suppression file can be kept.
    - Have a valid reason to process an individual's data using your legal legitimate interests. For example, an individual may have acquired a product, therefore, the business can market similar products to the customer

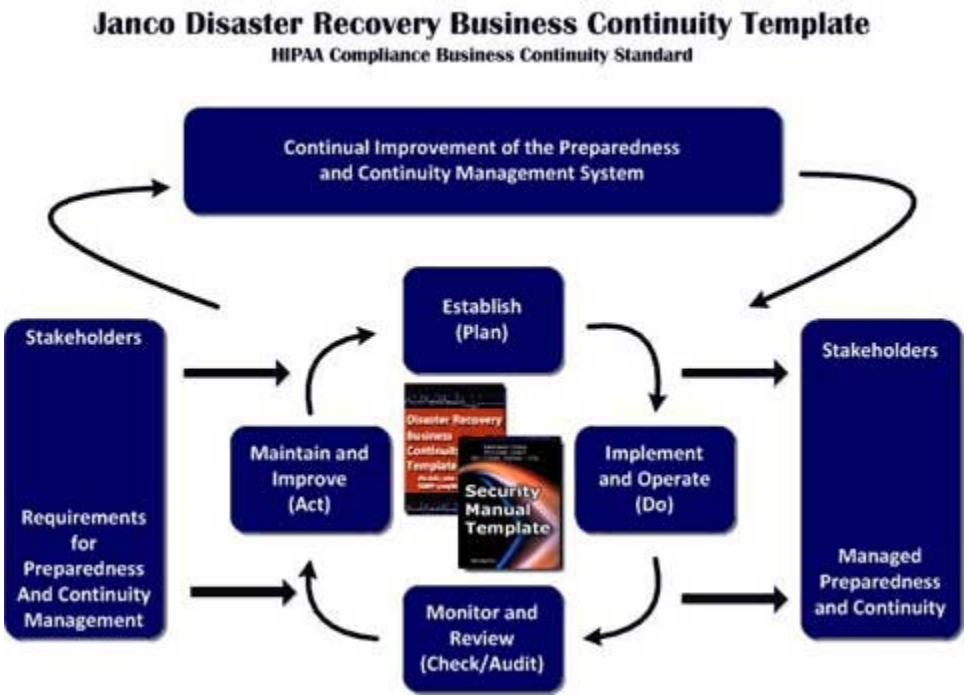
Gramm-Leach-Bliley (Financial Services Modernization)

Gramm-Leach-Bliley (GLBA) addresses both information security and privacy and holds ENTERPRISE management accountable for evaluating risks and implementing controls to keep all information secure. Features of the act include:

- Financial groups are required by GLBA to notify customers of policies related to disclosing nonpublic customer information to affiliates and third parties.
  - Protected information includes:
  - Name
  - Address (Physical and email)
  - Phone number
  - Credit Card numbers
  - Social Security Number
  - Loan application information
  - Credit history
  - Customers need to be given the option to opt out of having their private information disclosed.
- Notification should be:
  - At the beginning of the relationship and
  - At least annually to all customers

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 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, the 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.

Definitions

Unsecured PHI

Unsecured PHI is PHI that is not rendered "unusable, unreadable, or indecipherable" through the use of a "technology or methodology," specified by HHS in its guidance. The guidance listed the two acceptable technologies and methodologies for rendering PHI secure - encryption and destruction - and included specific definitions for each. For instance, paper, film, or other hard-copy media are considered "destroyed" only if they are shredded or altered so that they cannot be read or otherwise reconstructed, and redaction is specifically excluded as a mode of destruction. Thus, PHI that has not been encrypted or destroyed - and is subsequently disclosed = would be subject to the HIPAA Rule's notice provisions. Information technology staff and consultants may want to carefully review the HHS guidance, which is available in the Federal Register and on the HHS website, for additional requirements concerning encryption and destruction.

It is important to note that the data-protection standards recognized under the HIPAA Rule (encryption and destruction) are different from the data-protection standards articulated under the HIPAA Security Rule and the HIPAA Privacy Rule. The Security Rule requires that covered entities protect electronic PHI by satisfying several general standards. The Privacy Rule requires that covered entities apply reasonable safeguards to all PHI. Thus, even PHI that was protected per the Privacy and Security Rules, such as by use of firewalls, but was breached under the terms of the new HIPAA Rule, would have to be reported.

Breach

The definition of "breach" somewhat limits the situations when notice must be provided. When PHI is improperly disclosed, a covered entity or business associate should perform a specific analysis to determine whether a breach requiring notification has occurred:

- A breach occurs only if the following elements are present in the situation: (a) there has been "unauthorized" access, use, or disclosure of PHI, which violates the HIPAA Privacy Rule; and (b) the disclosure "compromises the security or privacy" of the PHI," which means that it "poses a significant risk of financial, reputational, or other harm to the individual.
- A breach does not occur if the PHI is part of a "limited data set," and does not include ZIP codes or dates of birth. A limited data set is a collection of PHI that excludes some but not all identifying PHI (e.g., names, addresses), and is used for research, public health, or operational purposes.
- A breach does not include (a) any "unintentional" acquisition, access, or use of PHI by a workforce member or individual acting under the authority of the covered entity or business associate that is made in good faith, within the course or scope of employment or other professional relationship, and is not further used or disclosed unlawfully under the HIPAA Privacy Rule; (b) an "inadvertent" disclosure to another authorized person at the same covered entity, business associate or organized healthcare arrangement, and the PHI is not further used or disclosed unlawfully

under the HIPAA Privacy Rule; and (c) a disclosure where the covered entity or business associate had a good-faith belief that the unauthorized person to whom the information was disclosed would not reasonably be able to "retain" such information.

- Determining Whether a Breach of Unsecured PHI Has Occurred
  In practical terms, how can a covered entity or business associate determine whether a breach has occurred?
- It should determine whether there has been a violation of the HIPAA Privacy Rule. An incidental disclosure of PHI, as permitted under the Privacy Rule, would not constitute a breach.
- If a HIPAA Privacy Rule violation has occurred, the entity should perform a risk assessment to determine whether the event poses a significant risk of financial, reputational, or other harm to the individual. If a laptop were lost and later recovered, and it was determined that the PHI on the laptop posed the minimal risk of harm to the individual or the laptop had not been used during the time it was lost, then no breach would have occurred. The risk assessment should also consider whether the PHI at issue was part of a limited data set and included ZIP codes or dates of birth; if not, there likely is no significant risk of harm to the individual posed by any disclosure.
- The entity should determine whether an exception applies. Here are some examples, as provided in the explanatory preamble to the HIPAA Rule:

    - A billing employee mistakenly receives an email from a clinician that contains PHI. The employee deletes the email and alerts the clinician. The first exception ("unintentional" access") applies.
    - A physician inadvertently sends an email containing PHI to a nurse at the same hospital regarding the wrong patient. The physician and the nurse are both authorized to access the PHI. The second exception ("inadvertent access") applies.
    - A hospital sends an explanation of benefits to the wrong individuals. Some are returned as undeliverable. The third exception (no ability to "retain" unsecured PHI) applies.

It is important to note that the burden is on the covered entity or business associate, through documentation or otherwise, to show that no breach has occurred or that an exception applies.

Notification Timing

If it is determined that a breach has occurred, the covered entity should notify the individual who is the subject of the breach of unsecured PHI without unreasonable delay, but in no case later than 60 days after discovery. The 60-day period begins on the day that the covered entity (including its workforce and other agents) first knew or, with reasonable diligence, should have known about the breach. The 60-day rule is designed to allow for a reasonable amount of time to perform an investigation, but the entity should not wait to perform its investigation or notify the individual until the end of the 60 days.

In determining whether a covered entity acted without unreasonable delay, HHS will consider whether the breach was known to an agent of the covered entity—which could include a business associate. The agent's knowledge of the breach is attributed to the covered entity, and the 60-day period begins with the timing of the agent's knowledge.

A potentially thorny aspect of the HIPAA Rule is whether a business associate is acting as an agent or as an independent contractor. In general terms, an agent steps into the principal's shoes to perform an act under the principal's scope of authority (e.g., billing); an independent contractor performs an independent activity on behalf of the principal (e.g., data analysis). One way to navigate this issue may be to impose strict notice time frames in business associate agreements.

Notice

The notice must be made by First-Class mail unless the individual (or next of kin) has agreed to electronic notice; however, if the contact information is insufficient or out-of-date and the individual is still living, the entity must provide for "substitute notice." Substitute notice is based on the circumstances and the number of individuals affected (e.g., if under 10 individuals, notice may be made by phone; if over 10 individuals, more "conspicuous" notice is required, such as on the provider's website with a toll-free number, active for three months to provide more information).

The notice must include a brief description of the breach, the type of information disclosed, any steps the individual should take (e.g., notifying the police), the steps taken to investigate and mitigate the breach, and contact procedures. The notice should not contain sensitive information, such as the type of medical treatment that happened to be disclosed.

When the breach involves more than 500 persons, the covered entity must notify HHS, per instructions to be posted on the HHS website. When the breach involves more than 500 residents of a particular state or "jurisdiction" (an area within a city), the covered entity must notify prominent media outlets without unreasonable delay, but no later than 60 days following the discovery of the breach. The notice must describe the breach according to the same content requirements for individual notices. The covered entity must keep a log of all breaches involving less than 500 individuals, and notify HHS annually.

Business Associates

For the business associate, like the covered entity, the beginning of the HIPAA Rule's timing requirements is tied to the day that the breach was known or should have been known with reasonable diligence. If the business associate is acting as an agent of the covered entity, the discovery of the breach by the business associate is imputed to the covered entity, so that the covered entity's time frame for notifying the individual begins on the day that the breach was discovered by the business associate. If the business associate is acting as an independent contractor, it must notify the covered entity without unreasonable delay, but in no case later than 60 days, after the discovery of the breach, at which time the covered entity's duties are triggered.

The business associate must also provide specified information, including the names of the individuals whose information was breached, to the covered entity. The covered entity and the business associate may determine which entity is in the best position to issue the notice to the individual. HHS discourages multiple notices to consumers.

Administrative Obligations

The HIPAA administrative obligations applicable to covered entities—including training, workforce sanctions, a complaint procedure, refraining from retaliatory acts, no waiver of rights, amendment of policies and procedures, and documentation—should be amended to take into account the HIPAA Rule. In addition, the covered entity, or the business associate as applicable, must demonstrate that, for any event, no breach occurred or that proper notice was made.

The FTC Rule

Under the FTC Rule, "breach of security" is defined as the acquisition of unsecured PHI of an individual in a PHR without the authorization of the individual. A breach of security is presumed "when there is unauthorized access to data . . . unless the entity that experienced the breach 'has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.'" Similar to entities covered by the HIPAA Rule, entities covered by the FTC Rule may rely on encryption and destruction to demonstrate that PHI is secure. In the event of a breach, vendors must contact the FTC and the consumer directly, or if the breach is experienced by the vendor's service provider, it must notify the vendor, which then must notify the consumer and the FTC. As with the HIPAA Rule, if the breach affects 500 or more people, the FTC Rule requires that the media, in addition to the consumer, should be notified. Breach notices must be given "without unreasonable delay" and in no case later than 60 calendar days after discovering the breach. However, unlike the HIPAA Rule, the entity is required to notify the FTC within 10 business days of the breach. Entities that do not properly notify consumers of the breach may be subject to civil penalties.

When a vendor provides PHRs under a business associate arrangement as well as independently to consumers, and a breach occurs that affects both sets of PHRs, the vendor is permitted to

issue the same notice to all affected individuals, according to the HIPAA Rule notice requirements, assuming that the covered entity has given the vendor/business associate the authority to issue the notice to its affected individuals.

Massachusetts 201 CMR 17.00 Data Protection Requirements

Standards for the Protection of Personal Information of Residents of the Commonwealth - Organizations that do business with Massachusetts residents must:

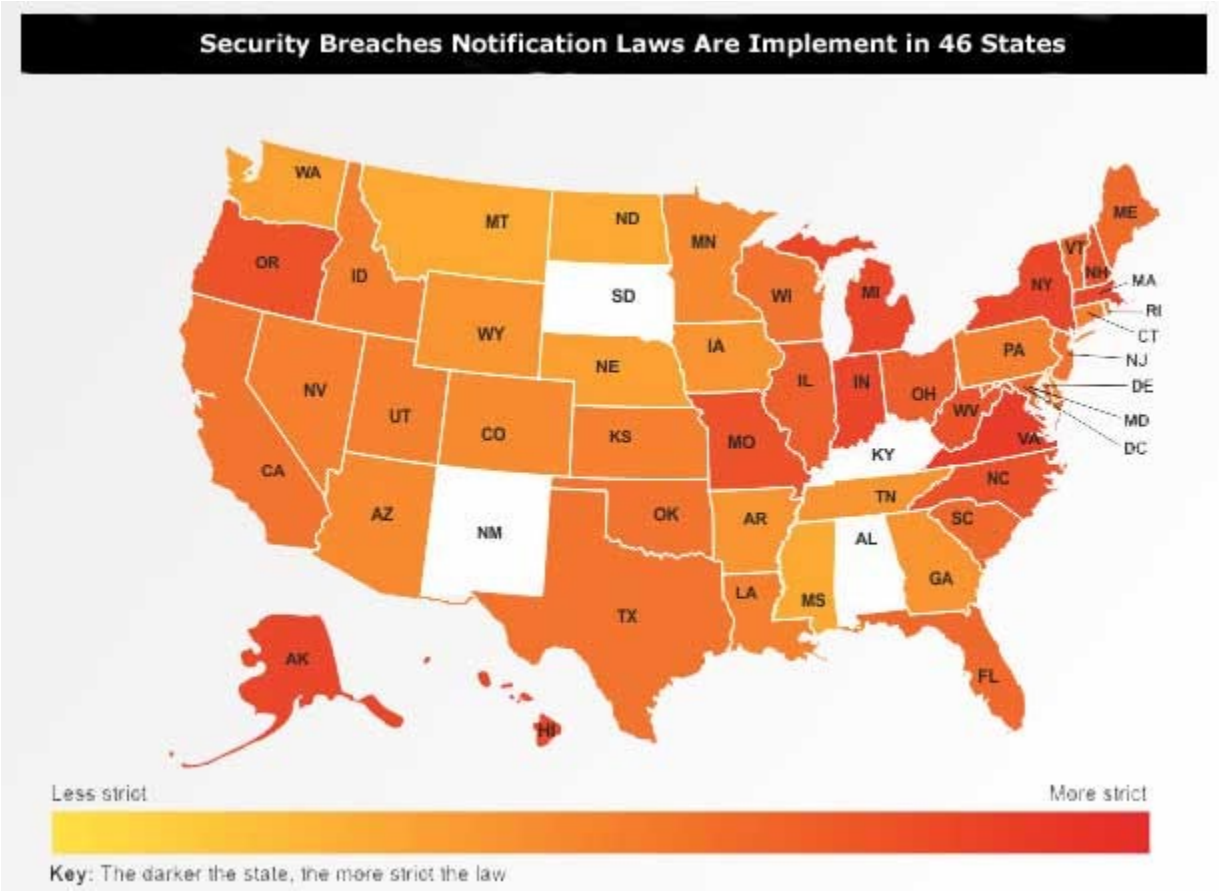
- Control passwords to ensure they are kept in a location and/or format that will not compromise the security of the data they protect
- Encrypt all personal information stored on laptops or other portable devices
- Ensure reasonably up-to-date firewall protection and operating system security patches, designed to maintain the integrity of the personal information
- Ensure up-to-date versions of system security agent software, which must include malware
  protection and up-to-date patches and virus definitions
- Have a Written Information Security Program (WISP) and take "reasonable steps" to ensure that any third-party/independent contractors comply with these data protection provisions. *Note: A copy of the WISP checklist is in the appendix of this template*.

Sarbanes-Oxley Act

Sarbanes-Oxley Act (SOX) requires the certification of the accuracy of the periodic reports and financial statements of ENTERPRISE by the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) of ENTERPRISE. In addition, it adds the requirement that the CEO and CFO on a "rapid and current basis" disclose information that can or does materially change the financial condition of a publicly-traded ENTERPRISE

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	Ariz. Rev. Stat. § 44-7501
Arkansas	Ark. Code § 4-110-101 et seq.
California	Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82
Colorado	Colo. Rev. Stat. § 6-1-716
Connecticut	Conn. Gen Stat. 36a-701b
Delaware	Del. Code tit. 6, § 12B-101 et seq.
Florida	Fla. Stat. § 817.5681
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

Kansas	Kan. Stat. 50-7a01, 50-7a02
Kentucky	KRS § 365.732, KRS §§ 61.931 to 61.934
Louisiana	La. Rev. Stat. § 51:3071 et seq.
Maine	Me. Rev. Stat. tit. 10 §§ 1347 et seq.
Maryland	Md. Code, Com. Law § 14-3501 et seq.
Massachusetts	Mass. Gen. Laws § 93H-1 et seq.
Michigan	Mich. Comp. Laws § 445.72
Minnesota	Minn. Stat. §§ 325E.61, 325E.64
Mississippi	2010 H.B. 583 (effective July 1, 2011)
Missouri	Mo. Rev. Stat. § 407.1500
Montana	Mont. Code §§ 30-14-1704, 2-6-504
Nebraska	Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807
Nevada	Nev. Rev. Stat. §§ 603A.010 et seq., 242.183
New Hampshire	N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21
New Jersey	N.J. Stat. 56:8-163
New York	N.Y. Gen. Bus. Law § 899-aa
North Carolina	N.C. Gen. Stat § 75-65
North Dakota	N.D. Cent. Code § 51-30-01 et seq.
Ohio	Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192
Oklahoma	Okla. Stat. § 74-3113.1 and § 24-161 to -166
Oregon	Oregon Rev. Stat. § 646A.600 et seq.
Pennsylvania	73 Pa. Stat. § 2303
Rhode Island	R.I. Gen. Laws § 11-49.2-1 et seq.
South Carolina	S.C. Code § 39-1-90
Tennessee	Tenn. Code § 47-18-2107, 2010 S.B. 2793
Texas	Tex. Bus. & Com. Code § 521.03, Tex. Ed. Code 37.007(b)(5) (2011 H.B. 1224)
Utah	Utah Code §§ 13-44-101, -102, -201, -202, -310
Vermont	Vt. Stat. tit. 9 § 2430 et seq.
Virginia	Va. Code § 18.2-186.6, § 32.1-127.1:05
Washington	Wash. Rev. Code § 19.255.010, 42.56.590
West Virginia	W.V. Code §§ 46A-2A-101 et seq.
Wisconsin	Wis. Stat. § 134.98 et seq.
Wyoming	Wyo. Stat. § 40-12-501 to -502
District of Columbia	D.C. Code § 28- 3851 et seq.
Guam	9 GCA § 48-10 et seq.
Puerto Rico	10 Laws of Puerto Rico § 4051 et. seq.
Virgin Islands	V.I. Code § 2208

- States with no security breach law: Alabama, New Mexico, and South Dakota
- The current version of this can be found at http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

Implementation

Implementing an enterprise-wide strategy for compliance requires an understanding of the requirements of your industry and business. Then, policies and procedures must be put in place for collecting, alerting, reporting on, storing, searching, and sharing data from all systems, applications, and network elements. This creates a closed-loop process that governs the lifecycle of enterprise data and ensures your compliance program is successful.

The steps for implementing a successful enterprise-wide compliance program include:

- Understand the enterprise's requirements
- Understand the enterprise and its associated system of internal controls
- Define the compliance processes, metrics, and success criteria
- Identify all in-scope IT components
- Collect fine-grain user and system activities
- Store all logs centrally for the required time
- Implement regular tasks
- Implement and verify continuous monitoring
- Validate compliance status to auditors
- Substantiate reports and alerts

Understand the enterprise's requirements

The first step is to understand the requirements of the regulations you must meet in your industry. No matter what industry your company plays in, numerous mandates and regulations apply, as well as frameworks and controls that help various business units within an organization maintain security and risk management policies. Failing to follow certain controls can result in lost customers or lost jobs, whereas failure to meet industry regulations and legal mandates could result in more serious ramifications, such as fines or even imprisonment. A thorough understanding of the requirements applicable to your industry can prevent unnecessary problems.

Understand the enterprise and the associated system of internal controls

Putting in place the IT controls and frameworks for meeting compliance helps to govern compliance tasks and keep companies on track for complying with legal mandates and industry regulations. However, this requires an understanding of the specific language within those frameworks regarding log data management. The most common frameworks - COBIT 4, ISO17799, NIST 800-53/FISMA, and PCI - all have specific language about log data collection and retention. For example, requirement 10 within the PCI standard states that companies must log and track user activities, automate and secure audit trails, review logs daily, and retain the audit trail for at least a year. Other frameworks have similar requirements for log data collection and retention. It's important that companies not only implement the frameworks but understand what they're asking for.

Define the compliance processes, metrics, and success criteria

Once you understand the requirements of a given regulation or mandate, determine the scope, configuration, and mechanism for collecting, alerting on, reporting on, and retaining the data necessary to satisfy auditors. This step-by-step process allows you to define goals and key tasks for successful compliance. For example, when you determine the scope, your goal should be to identify all system components that are subject to a given regulation. Then you can define key tasks related to that goal. Once those tasks are complete, you can move to configure network elements, systems, and applications to generate the required log messages. After configuration, you can move to define key tasks for important compliance activities, including the collection and retention of data and setting up automated alerts and reporting on that data.

Identify all in-scope IT components

It's a misconception that only hardware should be monitored for compliance. In addition to network elements, servers, applications, and homegrown systems should also be monitored. The specific components that need monitoring will depend on the mandates and regulations that apply to your industry. For example, if PCI applies to your business, all components that transmit, process, or store financial information are in scope.

Collect fine-grain user and system activities

Log data from IT components across the enterprise provide a fingerprint of user activity. This information includes failed login attempts, security breaches, file uploads and downloads, credit card data access, information leaks, user and system activity, privileges assigned and changed, runaway applications, customer transactions, and email data. This is the information that auditors will expect you to monitor daily. Log data contains a wealth of information that provides insight into the health and security of the network; hence, it's critical to collect, store, and have access to all of it.

Begin a structured implementation process

Janco recommends that the following steps be taken:

- I**mplement a Security Officer Position** - That individual does not do all of the work, rather they have responsibility for coordinating all compliance-based issues.
- **Conduct a compliance risk assessment** - The first step is to understand which compliance mandates the enterprise falls under and then conduct an audit to see how well the enterprise complies as it currently is structured.
- **Document** - All compliance mandates require that documentation is in place for policies and procedures. The three things that compliance bodies look for are:
    - Is a policy or procedure in place?
    - Is the policy or procedure followed?
    - Is the policy or procedure the right one?
- **Know the operating environment** - Once a user is authorized to access information how will they gain access and where are the potential failure points?

- **Prepare for Incidents** - Even if you have every policy or procedure in place there will be compliance violations that will occur. Have processes in place that focus:
  - Prevention
  - Detection
  - Correction
- **Expect the worst to happen** - Do not accept the answer "That never could occur". It will and you will have to respond to it quickly and effectively.
- **Control media and electronic files** - a violation cannot occur without data. That data can be in any form - paper or electronic.
- **Train users** - With all the best policies and procedures in place without proper training, a compliance program cannot work.
- **Log and audit** - This not only includes data but also individuals and processes used.
- Clean up old data and system - Often enterprises will only worry about new applications. That is not enough concern over legacy systems and data that needs to be considered.

Validate compliance status to auditors

Using alerts and scheduled reports, you can also demonstrate compliance status to auditors. Alerts should be set based on compliance with SOX, PCI, ISO17799, HIPAA, or whatever regulation or best practice you are implementing. Then, reporting can be used to demonstrate compliance. An auditor might want to see the actual report that you are using for demonstrating the segregation of duties, for example.

Substantiate reports and alerts

Alerting and reporting on logs must be substantiated with immutable log archives. It's critical to store logs centrally with a long-term archival solution that preserves the integrity of the data. Immutable logs require time stamps, digital signatures, encryption, and other precautions to prevent tampering, both during transit of the data from the logging device to the storage device, as well as during archival.

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