Compliance Management

Silver Edition

Jancd Associates, Inc.

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

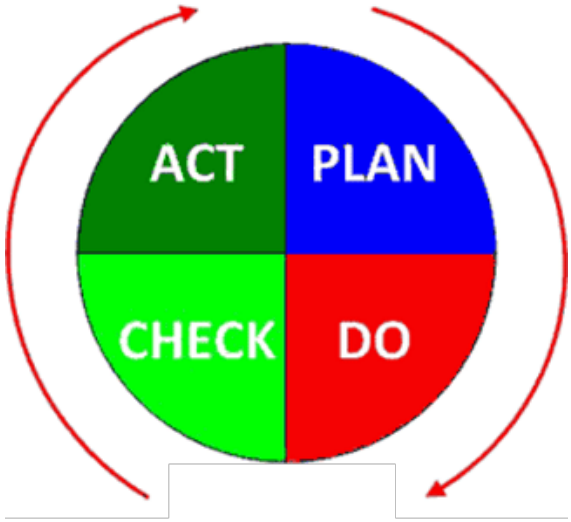
[1] *http://www.27000.org - The ISO 27000 series of standards have been specifically reserved by ISO for information security matters.*

- 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

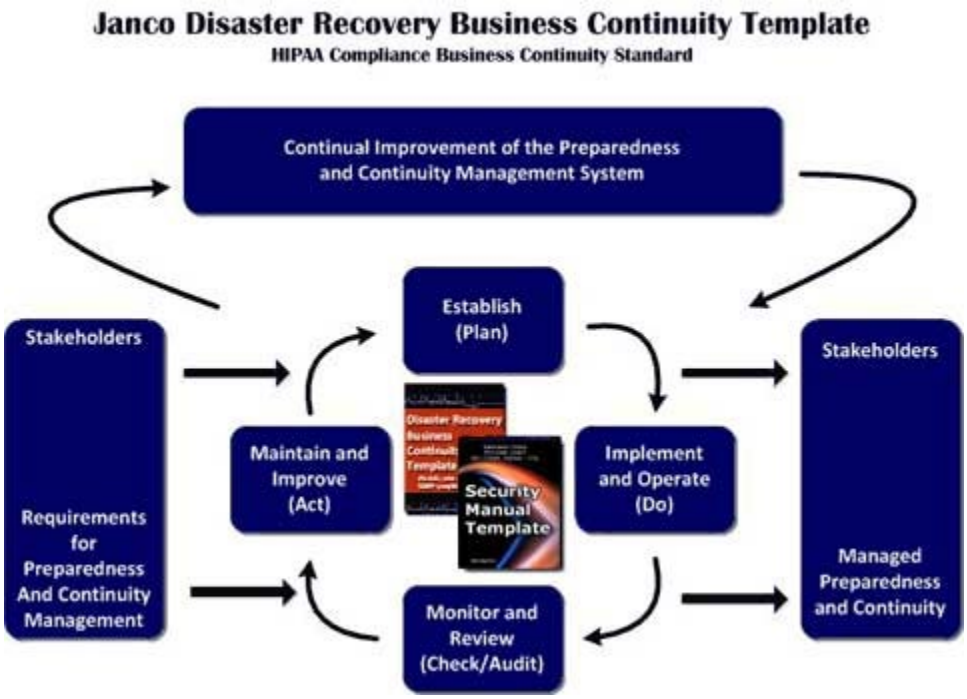
- **Disaster Recovery Plan Test / Audit – Local the enterprise's data center** - Conduct a tabletop test of the local enterprise's disaster recovery/business continuity plan and update as required for change management.

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").

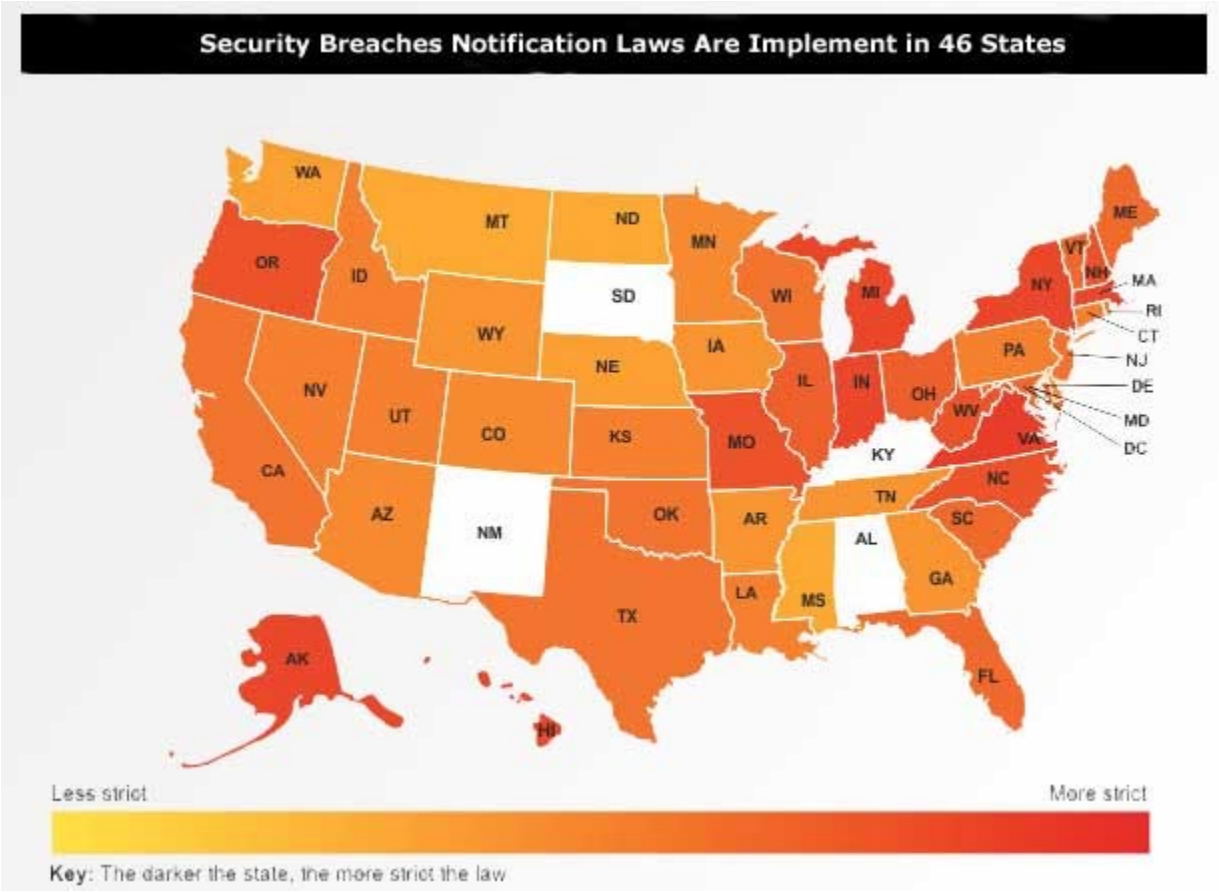


See https://e-janco.com/drp_and_security.htm

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

Compliance Management

Job Descriptions HandiGuide® Bundle

Table of Contents

PCI Audit Program

2025

Janco Associates, Inc.

PCI Audit Program

Table of Contents

PCI Compliance Security Audit Program

Introduction

The PCI Security Audit Procedures[1] are designed for use by assessors conducting onsite reviews for merchants and service providers required to validate compliance with the Payment Card Industry (PCI) Data Security Standard (DSS) requirements. The requirements and audit procedures presented in this document are based on the PCI DSS and the most recent set of privacy mandates – including GDPR.

This document contains the following:

- Introduction
- Policy – Sensitive Information
- Policy – Record Management, Retention, and Disposition
- PCI DSS Applicability Information
- The scope of Assessment for Compliance with PCI DSS Requirements
- Instructions and Content for *Report On Compliance*
- Revalidation of Open Items
- Security Audit Procedures
- Appendices
  - Appendix A: PCI DSS Applicability for Hosting Providers (with Testing Procedures)
  - Appendix B: Compensating Controls
  - Appendix C: Compensating Controls Worksheet/Completed Example

With e regulatory agencies, there are often compe s reason, we have provided "draft" policie olicy" and a "Record Management, Retent

[1] Portions of this test program were extracted from the published PCI requirements and have been enhanced by Janco Associates, Inc. Note we are not attorneys and do not express any legal nor PCI standards opinion in this document. The use of this audit program should consult with their own legal and PCI compliance staff.

PCI DSS Applicability Information

The following table illustrates commonly used elements of the cardholder and sensitive authentication data; whether the storage of each data element is permitted or prohibited; and if each data element must be protected. This table is not exhaustive but is presented to illustrate the different types of requirements that apply to each data element. At the same time, compliance with Record Retention and Disposition standards (see https://e-janco.com/recordmanagementpolicy.html) needs to be coordinated with the PCI DSS requirements. A Sensitive Information policy (see https://e-janco.com/sensitive.htm) for the enterprise should be implemented.

	Data Element	*Storage Permitted*	*Protection Required*	*PCI DSS Requirement 3.4*
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name	Yes	No	No
	Service Code	Yes	No	No
	Expiration Date	Yes	No	No
Sensitive Authentication Data**	CVC2/CVV2/CID	No	N/A	N/A
	Pin / Pin Block	No	N/A	N/A

* These data elements must be protected if stored in conjunction with the PAN (Primary Account Number). This protection must be consistent with PCI DSS requirements for the general protection of the cardholder environment. Additionally, other legislation (for example, related to consumer personal data protection, privacy, identity theft, or data security) may require specific protection of this data or proper disclosure of a company's practices if consumer-related personal data is being collected during business operations. PCI DSS, however, does not apply if PANs are not stored, processed, or transmitted.

** Sensitive authentication data must not be stored after authorization (even if encrypted).

The scope of Assessment for Compliance with PCI DSS Requirements

The PCI DSS security requirements apply to all "system components." A system component is defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data. Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include but are not limited to the following: web, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (internet) applications.

Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from the rest of the network, may reduce the scope of the cardholder data environment. The assessor must verify that the segmentation is adequate to reduce the scope of the audit.

A service provider or merchant may use a third-party provider to manage components such as routers, firewalls, databases, physical security, and/or servers. If so, there may be an impact on the security of the cardholder data environment. The relevant s

1. Each of the third-pa
2. The third-party pro

For service providers require e performed on all system components where c specified.

For merchants required to u s focused on any system(s) or system component(s) related to authorization and settlement where cardholder data is stored, processed, or transmitted, including the following:

- All external connections into the merchant network (for example; employee remote access, payment card company, and third-party access for processing, and maintenance)
- All connections to and from the authorization and settlement environment (for example, connections for employee access or devices such as firewalls and routers)
- Any data repositories outside of the authorization and settlement environment where more than 500 thousand account numbers are stored. Note: Even if some data repositories or systems are excluded from the audit, the merchant is still responsible for ensuring that all systems that store, process, or transmit cardholder data are compliant with the PCI DSS
- A point-of-sale (POS) environment – the place where a transaction is accepted at a merchant location (that is, retail store, restaurant, hotel property, gas station, supermarket, or other POS location)
- If there is no external access to the merchant location (by the Internet, Wi-Fi, Bluetooth, a virtual private network (VPN), dial-in, broadband, or publicly accessible machines such as kiosks), the POS environment may be excluded.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are computer devices that control computer traffic allowed into and out of a company's network, as well as traffic into more sensitive areas within a company's internal network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from the Internet, whether entering the system as e-commerce, employees' Internet-based access through desktop browsers, or employees' e-mail access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

PCI DSS Requirements	Testing Procedures	In Place	Not in Place	Target Date/ Comments
1.1 Establish firewall configuration standards that include the following:	**1.1** Obtain and inspect the firewall configuration standards and other documentation specified below to verify that standards are complete. Complete each item in this section			
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration	**1.** pr… …roval of…			
	1. fi… …e			
	1.1.1c Verify logs are in place and are actively being monitored			
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks	**1.1.2.a** Verify that a current network diagram exists and verify that it documents all connections to cardholder data, including any wireless networks			
	1.1.2.b. Verify that the diagram is kept current			

Appendix C: Compensating Controls Completed Example/Worksheet

Example

1. Constraints: List constraints precluding compliance with the original requirement.

Company XYZ employs stand-alone Unix Servers without LDAP. As such, they each require a 'root' login. It is not possible for Company XYZ to manage the 'root' login nor is it feasible to log all 'root' activity by each user.

2. Objective: Define the objective of the original control; identify the objective met by the compensating control.

onsidered acceptable from a gins makes it impossible to state

3. Identified Risk: Identify any additional risk posed by the lack of the original control.

Additional risk is introduced to the access control system by not ensuring all users have a unique ID and are able to be tracked.

4. Definition of Compensating Controls: Define the compensating controls and explain how they address the objectives of the original control and the increased risk if any.

Company XYZ is going to require all users to log into the servers from their desktop using the SU command. SU allows a user to access the 'root' account and perform actions under the 'root' account but is able to be logged in the su-log directory. In this way, each user's actions can be tracked through the SU account.

What's New

2025

- Upated external links
- Updated graphics
- Updated to meet the latest mandates

2023

- Update to meet the latest requirements
- Updated graphics
- Corrected errata

2022

- Update to meet the latest requirements
- Updated graphics

Version 3.1

- Updated to meet the latest privacy and security requirements

Version 3.0

- Update to meet the latest requirements
- Updated graphics

Security Audit Program

Janco Associates, Inc.

2025

Table of Contents

Security Firewall Policy Checklist

Whether there are firewalls and a security policy or not, it's prudent to regularly evaluate your security approach. Review and answer the following questions before implementing any further firewall technology and/or security policy additions or changes.

Identify which resources must be secure and in which order of priority:

- Mission critical
- Redundant back-up system(s)
- Secondary
- Base systems

Identify minimum security needs for the following WAN connections:

- Employee remote access and dial-up
- Office-to-office VPN
- Employee and vendor bro
- Vendor access
- Business-to-business acce

Does the security team hav

- Network diagrams
- Trending data
- Protocol utilization
- Data points
- Access points
- Major vendors' point of contact information (ISP, telco, firewall vendor)

Does the security team know the order in which systems must be restored?

- The security response team must have a full understanding of which systems need to be restored to full operation and in what order.
- Does this order meet the business' objectives and priorities?

Does the information disclosure policy address the following about a security issue?

- What information is shared with others?
- Is information shared internally, departmentally, externally, etc?
- Under which circumstances?
- Mission critical information?
- Secondary intrusion information?
- Who has the authority to initiate information disclosure (Chief Security Officer, legal, HR)?

Ransomware, WFH, GDPR, CaCPA ISO, Cobit, HIPAA, and SOX Addressed

This audit program contains a list of tasks and and weights assigned to each task. The Excel sheet calculates the value of both positive and negative points. Based on the audit you place an "X" in the yes and/or no box and a value is automatically calculated. When the audit, which is on the worksheet 'Audit Program', is completed all of the results are them posted on the summary worksheet and graphic charts can be generated from those tables (see the attached sample).

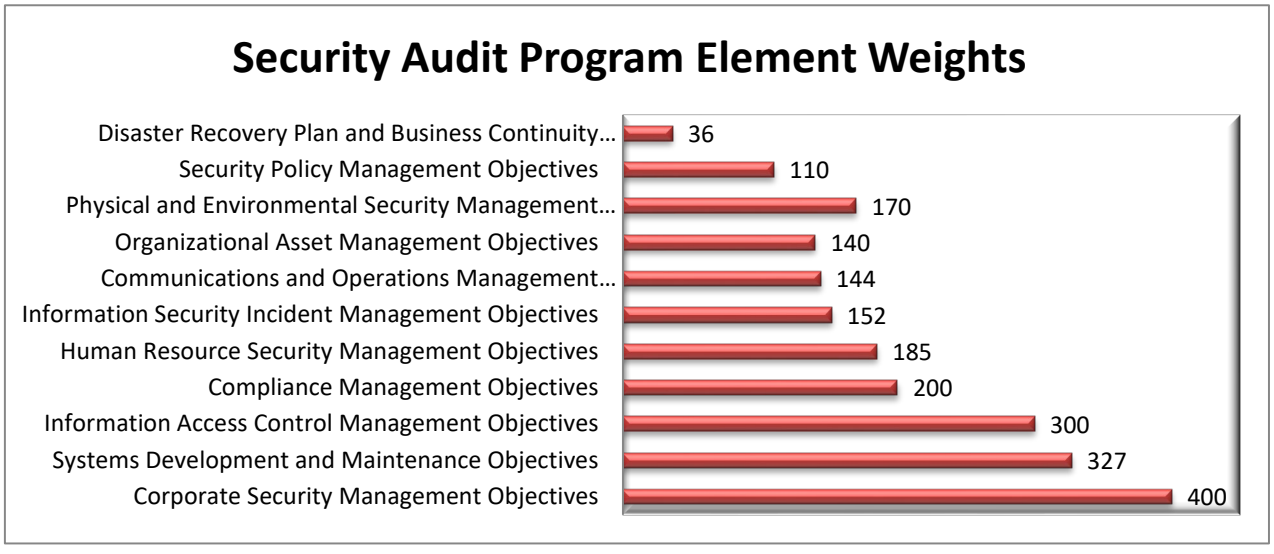
The worksheets Audit Program Summary, Audit Program, and Audit Program Graphic are integrated - if you change the name on the on any of those three worksheets then the Audit Program Summary Sheet and Audit Program Graphic will not be generated correctly. We suggest that you make a copy of the entire excel file and delete the "Sample" worksheets.

We have assigned weights to each element of the audit, you are free to updated to weights to what you think they should be. We assume no liability for the weight assignment and leave that up to the user. Our weights are only recommendations and should be considered as such.

The last three worksheets show a sample of the forms filled out with a set of summary graphic
We assume that the individual completi
Included with the excel spread sheet are
and used in the process. For ease you ca
excel worksheet.

NOTE: An item can be marked both as a
and negative score.

support@e-janco.com https://e-janco.com

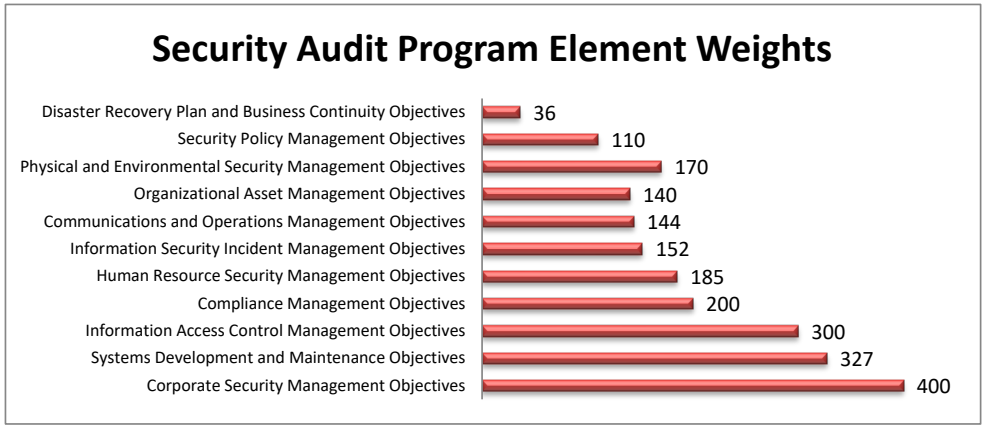


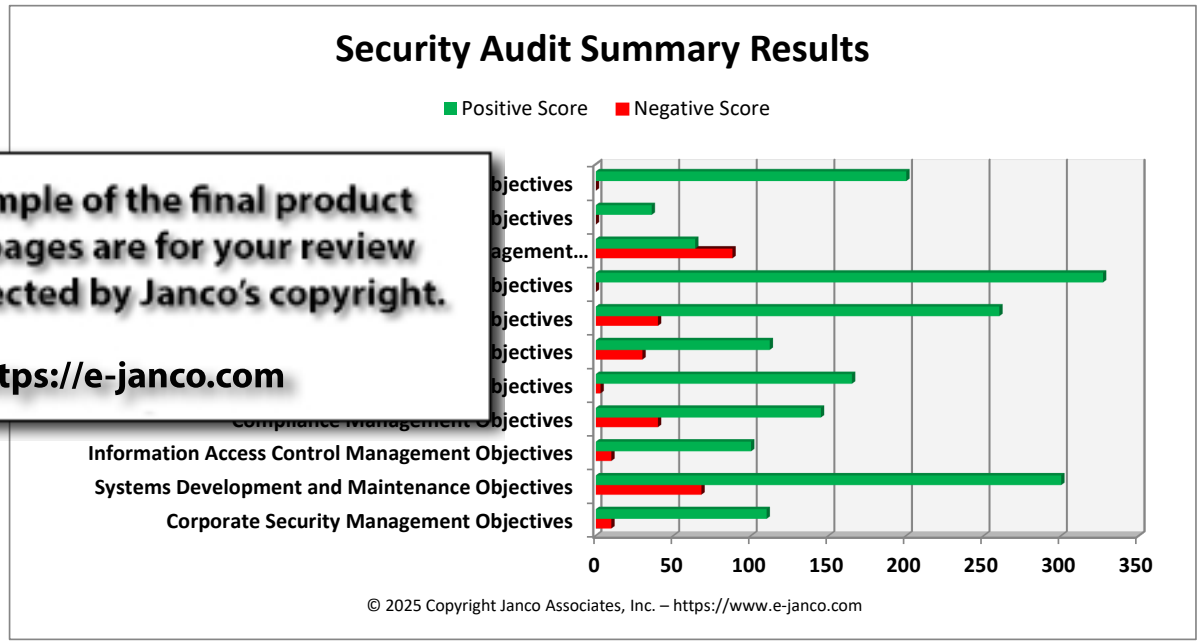
Security Audit Program (Sample)

		Comment	Yes	No	Weight	Negative Score	Positive Score
Compliance Management Objectives					**200**	**0**	**200**
Mandated Security Requirements		https://www.e-janco.com/SarbanesOxley.htm			**80**	**0**	**80**
36.01	Validate that the enterprise's information systems comply with all relevant statutory security requirements.		x		10		10
36.02	Validate that the enterprise's information systems comply with all relevant regulatory security requirements.		x		10		10
36.03	Validate that the enterprise's information sy security requirements.		x		10		10
36.04	Validate the design the enterprise's informat statutory, regulatory, and contractual securi		x		10		10
36.05	Validate the operation of the enterprise's inf statutory, regulatory, and contractual securi		x		10		10
36.06	Validate the management of the enterprise's relevant statutory, regulatory, and contractu		x		10		10
36.07	Validate that the enterprise's users of the en relevant statutory, regulatory, and contractual security requirements.		x		10		10
36.08	Validate with legal experts in order to ensure that the enterprise's information systems comply with all relevant national and international legal security requirements.		x		10		10
Security Compliance Reviews					**70**	**0**	**70**
37.01	Validate that the enterprise's systems comply with the enterprise's security policies.		x		10		10
37.02	Validate that the enterprise's systems comply with the enterprise's security standards.		x		10		10
37.03	Validate the security of the enterprise's information systems.		x		10		10
37.04	Validate that the enterprise's information security reviews are carried out on a regular basis.		x		10		10
37.05	Validate the security of the enterprise's information systems by examining how well they comply with security policies.		x		10		10
37.06	Validate the technical platforms and information systems by examining how well they comply with relevant security implementation standards.		x		10		10
37.07	Validate the technical platforms and information systems by examining how well they comply with documented security control requirements.		x		10		10
Information System Audits					**50**	**0**	**50**
38.01	Validate performance audits are executed on the enterprise's information systems.		x		10		10
38.02	Validate controls to safeguard operational systems while information system audits are being performed are in place.		x		10		10
38.03	Establish controls to safeguard audit software and data files while information system audits are being performed.		x		10		10
38.04	Validate controls to safeguard the integrity of audit tools.		x		10		10
38.05	Validate controls to prevent the misuse of audit tools.		x		10		10

Security Sample Audit Program Summary

	Weight	Negative Score	Positive Score
	2164	289	1819
Corporate Security Management Objectives	400	10	110
Systems Development and Maintenance Objectives	327	68	300
Information Access Control Management Objectives	300	10	100
Compliance Management Objectives	200	40	145
Human Resource Security Management Objectives	185	3	165
Information Security Incident Management Objectives	152	30	112
Communications and Operations Management Objectives	144	40	260
Organizational Asset Management Objectives	140	0	327
Physical and Environmental Security Management Objectives	170	88	64
Security Policy Management Objectives	110	0	36
Disaster Recovery Plan and Business Continuity Objectives	36	0	200





Security Audit Program

ISO 28000 Supply Chain

Jancо Associates, Inc.

2025

Table of Contents

28000 Supply Chain Security Audit Program

	Weight	Negative Score	Positive Score
	2,169	168	2000
Security Risk Assessment and Planning	**120**	**6**	**114**
Risk Assessment	120	6	114
Supply Chain Security Management Objectives	**395**	**13**	**382**
Internal Security Organization	155	8	147
Implementation and Operation of Supply Chain Security	240	5	235
Organizational Supply Chain Security Management Objectives	**140**	**1**	**138**
Responsibility for the Supply Chain	70	0	69
Information Classification System	70	1	69
Human Resource Security Management Objectives	**185**	**131**	**54**
Security Prior to Employment	70	70	0
Security During Employment	60	60	0
Security at Termination	55	1	54
Physical and Environmental Supply Chain Security Management Objectives	**170**	**2**	**168**
Secure Areas	80	0	80
Enterprise Equipment	45	1	44
Remote Devices	45	1	44
Communications and Operations Management Objectives	**144**	**4**	**140**
Procedures and Responsibilities	10	0	10
Third Party Service Delivery	12	1	11
System Planning Activities	6	1	5
Malicious and Mobile Code	26	1	25
Back-up Procedures	6	0	6
Computer Networks	8	0	8
Media	30	0	30
Exchange of Information	18	0	18
Blockchain Interfaces	14	1	13
Information Processing Facilities	14	0	14
Information Access Control Management Objectives	**300**	**0**	**300**
Access to information	55	0	55
User Access Rights	25	0	25
Access Practices	50	0	50
Access to Network Services	40	0	40
Access to Operating Systems	45	0	45
Access to Applications	50	0	50
Mobile, and Remote Users	35	0	35
Systems Development and Maintenance Objectives	**327**	**11**	**316**
Information System Application Security	84	2	82
Applications Processing Information	91	7	84
Cryptographic Controls	60	2	58
System Files	50	0	50
Development and Support Processes.	42	0	42
Information Security Incident Management Objectives	**152**	**0**	**152**
Security Events and Weaknesses	88	0	88
Managing Security Incidents and Improvements	64	0	64
Disaster Recovery Plan and Business Continuity Objectives	**36**	**0**	**36**
Disaster Recovery Plan / Business Continuity	36	0	36
Compliance Management Objectives	**200**	**0**	**200**
Mandated Security Requirements	80	0	80
Security Compliance Reviews	70	0	70
Information System Audits	50	0	50