



As security breaches and identity thefts skyrocket, businesses face increasing scrutiny for how they handle and protect prospect and customer information. Businesses must maintain compliance with numerous regulations such as HIPAA, FISMA, SOX, and GLBA — and standards such as PCI DSS v2, NIST and ISO. These regulations and standards are complex and require ongoing maintenance which creates many challenges.

- Coordinating compliance efforts across multiple departments is difficult
- Efforts are duplicated and time and resources are wasted when security controls are repeated across multiple regulations
- Information security compliance is time-consuming and costly due to hundreds of tasks associated with each regulatory requirement
- Audit inquiries require correlating dozens of documents and evidentiary activities against hundreds of security controls

Solutions For Each Of Your Challenges

- **Manage all information security compliance initiatives through a centralized portal**

The Compliance Automation Portal provides you with an easy-to-use security control system for managing all of your compliance initiatives.

- The portal's centralized location lets you reference security control guidelines and best practices and record your activities as well as attach evidentiary documentation.
- Compliance controls are organized in a structured and logical manner which eliminates searching through documents or folder structures on a network server.
- Managing and documenting compliance activities in one central location makes it easier to monitor compliance activities and due dates.

- **Get automatic correlation of activities across multiple compliance programs**

The Compliance Automation Portal leverages a built-in correlation engine that eliminates the duplication of recorded activities by mapping similar controls across multiple compliance programs including:

- PCI DSS v2
- PCI PA-DSS
- NIST 800-53
- HIPAA
- NERC CIP
- Sarbanes-Oxley (SOX)
- Gramm-Leach-Bliley ACT (GLBA)
- ISO 27001
- SSAE 16
- FISMA

For example, evidentiary activities recorded for “access control authorization” within PCI DSS section 7.1.3 are automatically related to NIST 800-53 AC-2(d) .

- **Reduce complexity and administrative time through management “views” into the compliance programs**

The Compliance Automation Portal condenses control items into logical groups that provide insight into what activities are due when. You'll also see what activities are required to show ongoing management of the compliance program as a whole.

Organizing these activities into line item tasks helps eliminate the complexity and reduces the administration effort required to manage the compliance programs.

- **Streamline the compliance renewal process**

- Provide auditors with the same centralized information to perform compliance renewals. An ordered list of evidentiary documents and records ensures that you're always prepared for both planned and unplanned audits.

Why Choose CompliancePoint?

- CompliancePoint's Information Security Practice group has been a leading provider of information security and risk management consulting services and solutions since 2004. We help our clients safeguard information assets and ensure regulatory compliance.
- Our clients include many of the top tier businesses and respected leaders in the industries that we serve.
- Seasoned staff holds numerous industry certifications including PCI QSA, PCI PA-QSA , CISSP, CISM, CIFI, CSSLP.

Demonstrate ongoing compliance management throughout the entire year; helps streamline audits and renewals

Monitor compliance activities and due dates in the Tasks section of Program Management

Ensure that you are prepared for planned and unplanned audits with evidentiary documents

Provides real-time views into the status of annual assessments for compliance renewals

CompliancePoint
A PossibleNOW Company

Compliance Automation Portal

User Name: Bryan Bell
Authorization Level: Administrator
Company: CompliancePoint
Last Login Date: Fri Jan 27 2012 9:07:00 AM

Compliance Programs | Program Management | Program References | My Account | Logout

HIPAA

General Rules

Administrative Safeguards

164.308(a)(1) Security Management Process

164.308(a)(1)(ii)(A) Risk Analysis

164.308(a)(1)(ii)(B) Risk Management

164.308(a)(1)(ii)(C) Sanction Policy

164.308(a)(1)(ii)(D) Information System Activity Review

164.308(a)(2) Assigned Security Responsibility

164.308(a)(3) Workforce Security

164.308(a)(4) Information Access Management

164.308(a)(5) Security Awareness and Training

164.308(a)(6) Security Incident Procedures

Control Overview | Activity Journal | Documents | Assessment | Relationships

164.308(a)(1)(ii)(A)
Risk Analysis

Payment Card Industry (PCI) v2.0 6.4.5.3.a
For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system.

Payment Card Industry (PCI) v2.0 11.2.3.a
Inspect change control documentation and scan reports to verify that system components subject to any significant change were scanned.

Payment Card Industry (PCI) v2.0 11.3.a
Obtain and examine the results from the most recent penetration test to verify that penetration testing is performed at least annually and after any significant changes to the environment.

Payment Card Industry (PCI) v2.0 12.1.2.a
Verify that an annual risk assessment process is documented that identifies threats, vulnerabilities, and results in a formal risk assessment.

See related compliance requirements

See assigned tasks & due dates

Compliance Programs | Program Management | Program References | My Account | Logout

HIPAA

Next Due Date	Recurrence	Group	Task Owner
Fri Jan 27 2012 9:16:49 AM	Annual	164.306(e)	Security Ops
HIPAA Maintenance			
Tue Jan 24 2012 9:53:00 AM	Daily	164.308(a)(1)(ii)(D)	Network Ops
HIPAA Information System Activity Review			

Control Overview | Activity Journal | Documents | Assessment | Relationships

Program Guidance

Get dashboard views

Compliance Programs | Program Management | Program References | My Account | Logout

Compliance Alerts

PCI 2.3.b Out of Compliance

Tue Jan 24, 2012 2:47:00 PM Bryan Bell

Document Uploaded

Activity Journal

Compliance Status

PCI v2.0

100
99
98
97
96

Jan 23 Jan 22 Jan 21 Jan 20 Jan 19

Legend: In Place, Not In Place, Not Applicable, Compensating Control

Identify all control items with related documents