Achieve HIPAA Compliance with Symantec Control Compliance Suite

If your organization is considered a HIPAA Covered Entity, Health Plan, or Business Associate and handles electronic Protected Health Information (ePHI), demonstrating compliance with the Health Insurance Portability and Accountability Act's (HIPAA) Security Rule can be challenging. Protecting patients' PHI is vital in order to minimize your legal and financial risks as well as prevent damage to your reputation and business.

Yet even with stiff penalties and fines, many health care organizations are at significant risk of failing a HIPAA audit or experiencing a PHI-related security breach – especially as cyber criminals continue to identify the healthcare industry as a lucrative target. 94% of health care organizations admitted to at least one breach of PHI within the past two years. And the financial consequences can be devastating: a national insurer was fined $1.7 million for not securing access to an online database, and a Massachusetts eye and ear clinic was fined $1.5 million for a data breach.[1]

This is further complicated by the fact that healthcare providers often need to comply with additional compliance requirements stipulated under other regulations, like PCI DSS for credit card information, or state laws, which can be even stricter than HIPAA.

Many healthcare organizations rely on Symantec Control Compliance Suite to implement and manage their HIPAA risk and compliance program, assess and prioritize security controls, continuously monitor their risk exposure, and provide a unified view to security as well as business leadership. Control Compliance Suite helps you assess your compliance posture, prepare for the next audit, and understand your organization's compliance with the HIPAA Security Rule and other applicable regulations.

Why It's Difficult to Get a Complete Picture of Your Compliance

Addressing the challenges associated with implementing and managing a HIPAA compliance program is challenging, but also critical, in order to demonstrate your organization is not only satisfying regulations but also successfully translating abstract compliance into actionable security. Many organizations struggle with these common challenges:

Challenge #1: Complying with multiple regulations such as HIPAA, PCI DSS, and SOX

HIPAA isn't the only requirement that many healthcare organizations must satisfy. Most healthcare entities must also comply with PCI DSS, SOX, state laws, and other regulations, which make assessing, managing, and reporting infinitely more complex. Organizations that establish a front-to-back information governance program that connects regulations, via policies and procedures, to the actual technical and procedural controls will minimize duplicate efforts, greatly simplify their compliance processes, and easily demonstrate compliance.

Challenge #2: Getting an up-to-date view of your business and technical risks

Continually getting a clear picture of your business-relevant and technical security risks can be a daunting undertaking. Answering

[1] - "Top 10 Challenges for Meeting HIPAA Security Compliance", NAIIRO, February 1, 2016.

difficult, but essential, questions such as, “Which of our desktops need to be upgraded to satisfy this security standard?” and “How does the new healthcare organization we just acquired stack up in terms of risk posture?” are nearly impossible if you’re manually collecting data. Automating the entire process – from data collection to reporting – gives you continual insights into the status of your technical and business risks.

Challenge #3: Managing Business Associate Agreements and other vendor contracts for compliance

Many healthcare organizations work with a vast number of vendors that process PHI on their behalf and are, therefore, required by HIPAA to manage a Business Associate Agreement (BAA) for each of them. Assessing vendors’ compliance with the terms of a BAA is complex and time-consuming, but also critical, since healthcare organizations are responsible for their vendors’ appropriate protection of PHI.

Challenge #4: Continually managing policies, procedures, and training

Other important aspects of maintaining HIPAA compliance that are often overlooked include regularly updating HIPAA training manuals, tracking which employees across your organization participated in required security training classes, and more. The larger the healthcare organization the more challenging it is to keep this information up-to-date and ready for reporting in case an audit occurs.

How Control Compliance Suite Helps You Attain HIPAA Compliance

A software solution alone can’t make you compliant – it’s your processes and properly secured assets that ensure HIPAA compliance. A solution like Symantec Control Compliance Suite can make attaining and maintaining compliance an easier, more reliable, cost effective, and faster process.

Symantec Control Compliance Suite combines both procedural and technical information to help achieve HIPAA compliance including:

- Supporting end-to-end automation of internal and external assessments of procedural and technical controls.
- Automating the integration of multiple evidentiary sources and supporting multi-regulation compliance such as HIPAA and PCI DSS.
- Providing compliance and risk visibility in a highly complex technical and vendor ecosystem.
- Generating audit-ready reports and dashboards.
- Calculating and aggregating risk scores according to your healthcare organization’s unique thresholds.

End-to-end automation for technical and procedural controls

Proving HIPAA compliance requires collecting and maintaining an enormous amount of data about the controls in your environment. Control Compliance Suite automates assessments of technical controls that require secure configuration settings by using network and asset discovery – including for third-party systems.

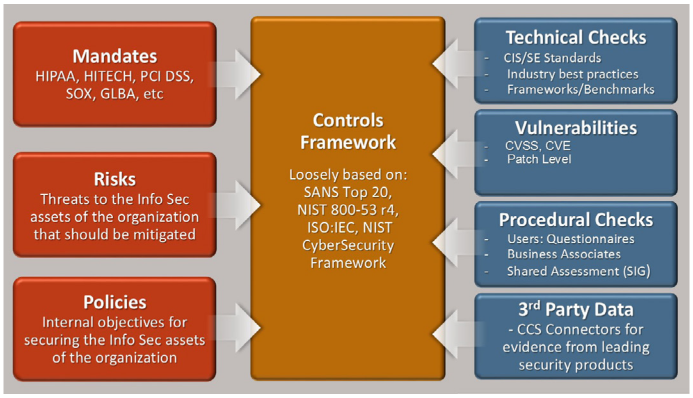

Mandates
HIPAA, HITECH, PCI DSS, SOX, GLBA, etc
Risks
Threats to the Info Sec assets of the organization that should be mitigated
Policies
Internal objectives for securing the Info Sec assets of the organization
Controls Framework
Loosely based on: SANS Top 20, NIST 800-53 r4, ISO:IEC, NIST CyberSecurity Framework
Technical Checks
- CIS/SE Standards
- Industry best practices
- Frameworks/Benchmarks
Vulnerabilities
- CVSS, CVE
- Patch Level
Procedural Checks
- Users: Questionnaires
- Business Associates
- Shared Assessment (SIG)
3rd Party Data
- CCS Connectors for evidence from leading security products

Figure 1: By mapping mandates, policies, and technical and procedural information to a control framework, Control Compliance Suite gives you a complete view into your risk posture.

By automating IT infrastructure assessments, you can quickly identify misconfigured assets and prioritize issues for remediation. If a technical asset requires attention that affects your compliance status, such as a laptop requiring encryption, Control Compliance Suite will list the prioritized issue in a remediation report so you can take appropriate action. It even integrates with Symantec ServiceDesk and third-party service desk tools so your helpdesk can be automatically notified when an issue requires their attention and provide feedback to Control Compliance Suite when the issue is addressed, thus providing closed-loop remediation visibility.

Control Compliance Suite helps you pinpoint gaps in your procedural controls with out-of-the-box support for HIPAA regulations and standards that are translated into user questionnaires. You can use these questionnaires to assess the effectiveness of your procedural security controls, evaluate overall employee awareness, and support security training.

Combining multiple data sources and supporting multi-regulation compliance

Control Compliance Suite can combine evidence from multiple sources, including other solutions such as Symantec Data Loss Prevention or third-party vulnerability scanners, so you have a complete view of your compliance posture. The evidence that Control Compliance Suite collects is formatted appropriately and mapped to HIPAA policies and regulations.

Many organizations that need to comply with HIPAA also have multiple mandates to satisfy, such as state privacy laws (which are often stricter than HIPAA), or PCI DSS if they accept credit card payments. Control Compliance Suite provides templates for over 100+ regulations out-of-the-box. You can assess your technical and procedural controls' status once across all applicable regulations and utilize that information to report on multiple mandates without repeating work.

Generating audit-ready reports and dashboards

Understanding your overall risk posture is critical. With Control Compliance Suite, you can answer specific questions such as, "What's my overall risk score?" while preparing for audits. This type of flexible risk analysis is invaluable for assessing HIPAA compliance and understanding if you're taking the appropriate steps to protect PHI from cyber criminals.

Risk-based, dynamic dashboards show your overall HIPAA compliance status so you can focus on your highest priorities. Control Compliance Suite's risk-ranked results help you determine which risks pose the biggest threats so you can create a prioritized plan for addressing them. You can also setup role-based viewing for reports and dashboards so users view just the information that is appropriate for their role. You can even give auditors access to specific reports while you maintain complete visibility and control over the information they can access and view.

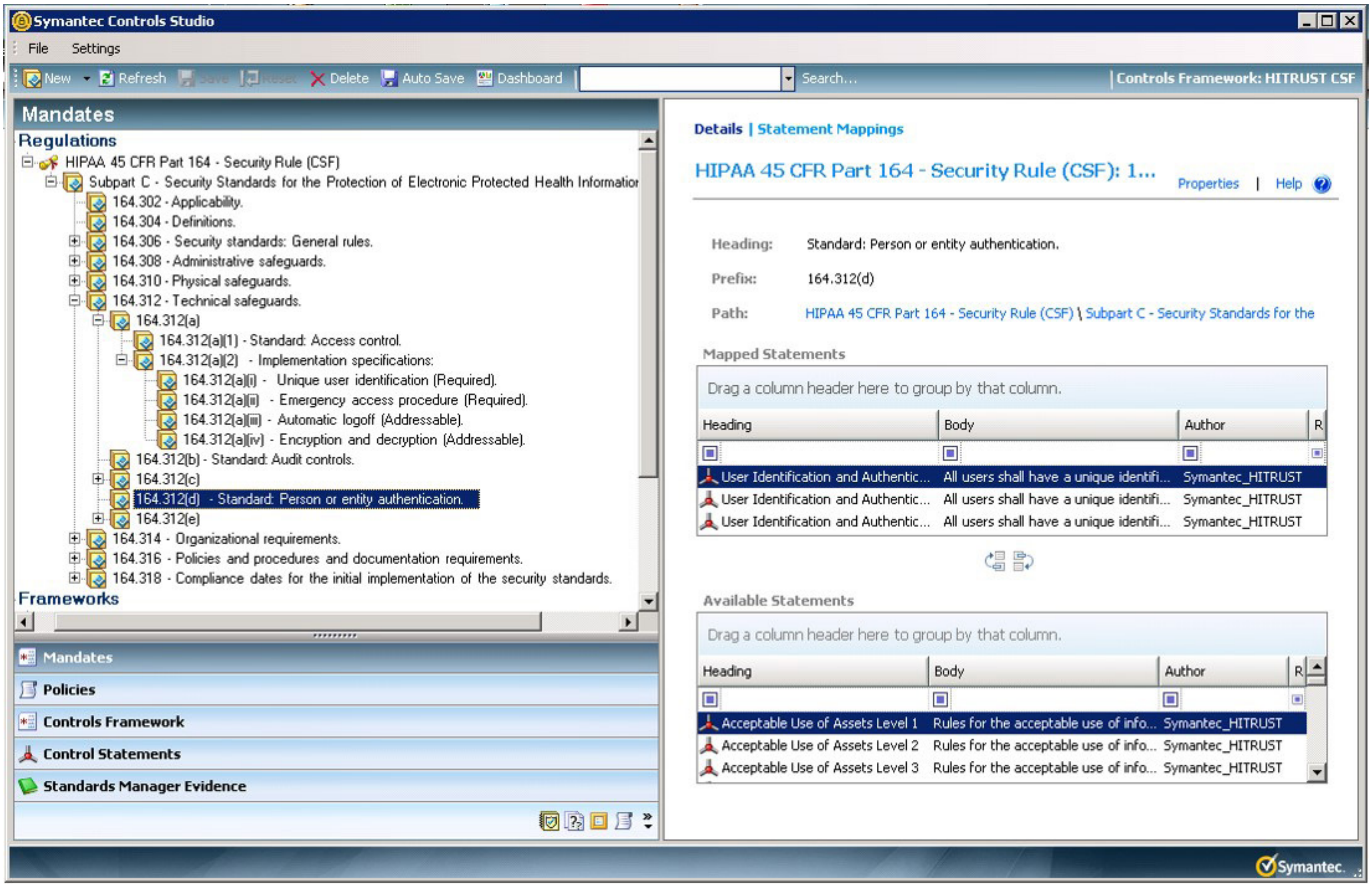
Assessing Business Associate Agreement compliance and vendor risk

Many healthcare organizations have hundreds, or even thousands, of vendors who handle PHI on their behalf. HIPAA requires a Business Associate Agreement (BAA) for each of these vendors. All vendors must also assure you that they are properly securing your PHI data in order to minimize security risks.

Control Compliance Suite simplifies and streamlines the process of managing BAAs including understanding how well your vendors are complying with security requirements. By automating vendor BAA security and risk assessments, you can facilitate secure on-boarding and off-boarding and execute security assessments for third- and fourth-party suppliers.

Business level reporting for executives and boards

With the prevalence of security breaches hitting the news, it's not surprising that executives and board members want to be assured of your organization's security status. Control Compliance Suite fills this gap by answering broad questions such as "What's my overall risk posture?" and more specific queries including, "What are our organization's compliance scores for HIPAA and PCI DSS?" Control Compliance Suite can help build confidence with your board and executive team, by delivering up-to-date risk, security, and compliance information.



Mandates

Regulations

- HIPAA 45 CFR Part 164 - Security Rule (CSF)
  - Subpart C - Security Standards for the Protection of Electronic Protected Health Informatior
    - 164.302 - Applicability.
    - 164.304 - Definitions.
    - 164.306 - Security standards: General rules.
    - 164.308 - Administrative safeguards.
    - 164.310 - Physical safeguards.
    - 164.312 - Technical safeguards.
      - 164.312(a)
        - 164.312(a)(1) - Standard: Access control.
        - 164.312(a)(2) - Implementation specifications:
          - 164.312(a)(i) - Unique user identification (Required).
          - 164.312(a)(ii) - Emergency access procedure (Required).
          - 164.312(a)(iii) - Automatic logoff (Addressable).
          - 164.312(a)(iv) - Encryption and decryption (Addressable).
      - 164.312(b) - Standard: Audit controls.
      - 164.312(c)
      - 164.312(d) - Standard: Person or entity authentication.
      - 164.312(e)
    - 164.314 - Organizational requirements.
    - 164.316 - Policies and procedures and documentation requirements.
    - 164.318 - Compliance dates for the initial implementation of the security standards.

Frameworks

HIPAA 45 CFR Part 164 - Security Rule (CSF): 1...

Heading: Standard: Person or entity authentication.

Prefix: 164.312(d)

Path: HIPAA 45 CFR Part 164 - Security Rule (CSF) \ Subpart C - Security Standards for the

Mapped Statements

Drag a column header here to group by that column.

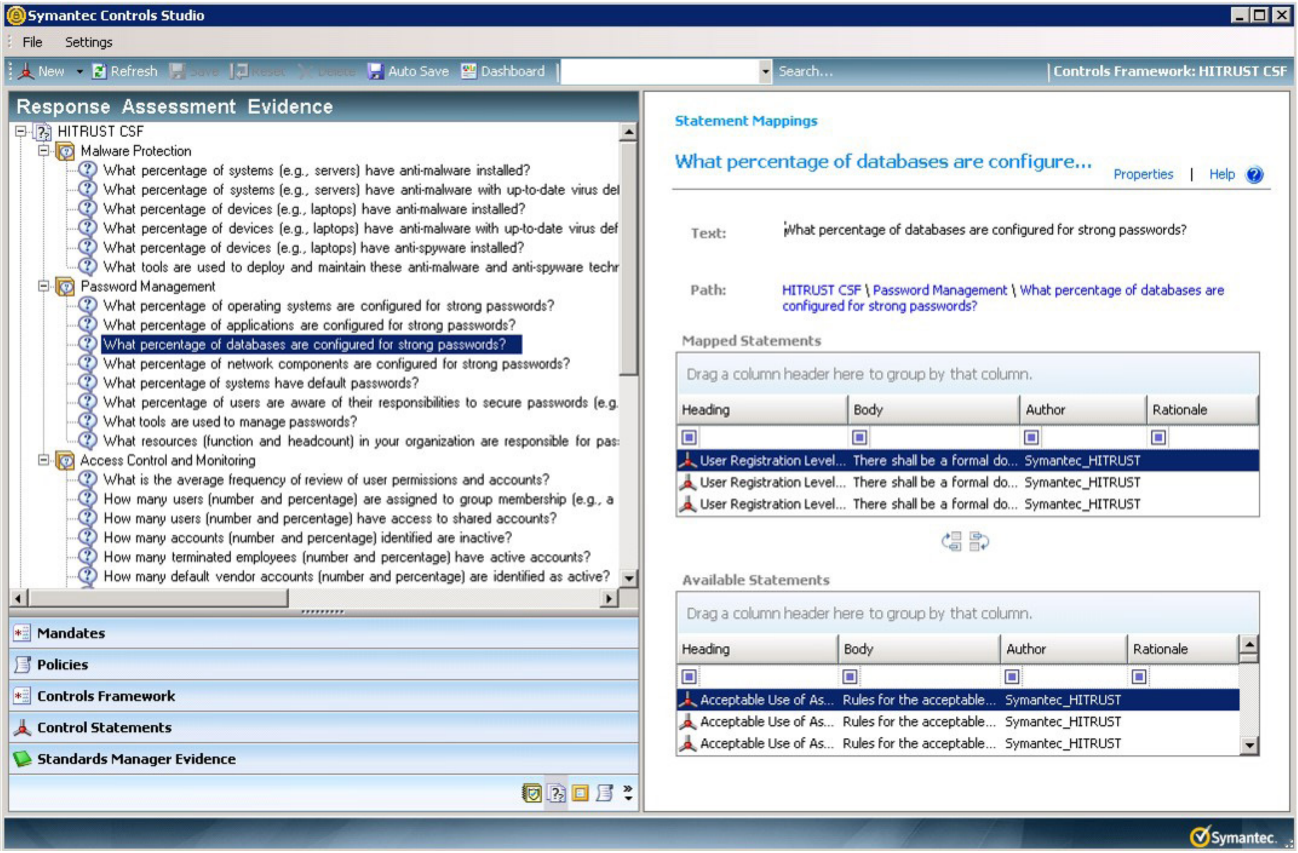
Heading	Body	Author	R
User Identification and Authentic...	All users shall have a unique identifi...	Symantec_HITRUST	
User Identification and Authentic...	All users shall have a unique identifi...	Symantec_HITRUST	
User Identification and Authentic...	All users shall have a unique identifi...	Symantec_HITRUST	

Available Statements

Drag a column header here to group by that column.

Heading	Body	Author	R
Acceptable Use of Assets Level 1	Rules for the acceptable use of info...	Symantec_HITRUST	
Acceptable Use of Assets Level 2	Rules for the acceptable use of info...	Symantec_HITRUST	
Acceptable Use of Assets Level 3	Rules for the acceptable use of info...	Symantec_HITRUST	

Figure 2: All controls are configurable in Control Compliance Suite and each control statement can be mapped to the appropriate HIPAA mandate.


Symantec Controls Studio
File Settings
New Refresh Save Reset Delete Auto Save Dashboard Search...
Controls Framework: HITRUST CSF
Response Assessment Evidence
Mandates
Policies
Controls Framework
Control Statements
Standards Manager Evidence
Statement Mappings
Properties | Help
Symantec.

- HITRUST CSF
  - Malware Protection
    - What percentage of systems (e.g., servers) have anti-malware installed?
    - What percentage of systems (e.g., servers) have anti-malware with up-to-date virus def
    - What percentage of devices (e.g., laptops) have anti-malware installed?
    - What percentage of devices (e.g., laptops) have anti-malware with up-to-date virus def
    - What percentage of devices (e.g., laptops) have anti-spyware installed?
    - What tools are used to deploy and maintain these anti-malware and anti-spyware techr
  - Password Management
    - What percentage of operating systems are configured for strong passwords?
    - What percentage of applications are configured for strong passwords?
    - What percentage of databases are configured for strong passwords?
    - What percentage of network components are configured for strong passwords?
    - What percentage of systems have default passwords?
    - What percentage of users are aware of their responsibilities to secure passwords (e.g.
    - What tools are used to manage passwords?
    - What resources (function and headcount) in your organization are responsible for pas:
  - Access Control and Monitoring
    - What is the average frequency of review of user permissions and accounts?
    - How many users (number and percentage) are assigned to group membership (e.g., a
    - How many users (number and percentage) have access to shared accounts?
    - How many accounts (number and percentage) identified are inactive?
    - How many terminated employees (number and percentage) have active accounts?
    - How many default vendor accounts (number and percentage) are identified as active?

What percentage of databases are configure...

Text: What percentage of databases are configured for strong passwords?

Path: HITRUST CSF \ Password Management \ What percentage of databases are configured for strong passwords?

Mapped Statements

Drag a column header here to group by that column.

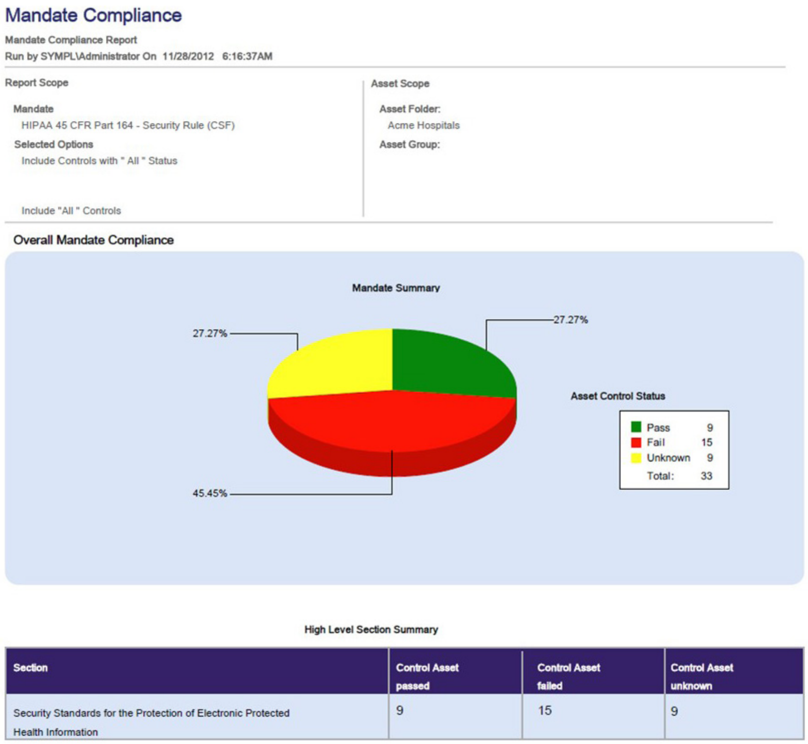
Heading	Body	Author	Rationale
User Registration Level...	There shall be a formal do...	Symantec_HITRUST	
User Registration Level...	There shall be a formal do...	Symantec_HITRUST	
User Registration Level...	There shall be a formal do...	Symantec_HITRUST	

Available Statements

Drag a column header here to group by that column.

Heading	Body	Author	Rationale
Acceptable Use of As...	Rules for the acceptable...	Symantec_HITRUST	
Acceptable Use of As...	Rules for the acceptable...	Symantec_HITRUST	
Acceptable Use of As...	Rules for the acceptable...	Symantec_HITRUST	

Figure 3: Procedural assessment questions are mapped to controls in Control Compliance Suite.



Mandate Compliance

Mandate Compliance Report
Run by SYMPL\Administrator On 11/28/2012 6:16:37AM

Report Scope

Mandate
HIPAA 45 CFR Part 164 - Security Rule (CSF)

Selected Options
Include Controls with " All " Status

Include "All " Controls

Asset Scope

Asset Folder:
Acme Hospitals

Asset Group:

Overall Mandate Compliance

Asset Control Status	
🟩 Pass	9
🟥 Fail	15
🟨 Unknown	9
Total:	33

High Level Section Summary

Section	Control Asset passed	Control Asset failed	Control Asset unknown
Security Standards for the Protection of Electronic Protected Health Information	9	15	9

Figure 4: HIPAA compliance audit report in Control Compliance Suite.

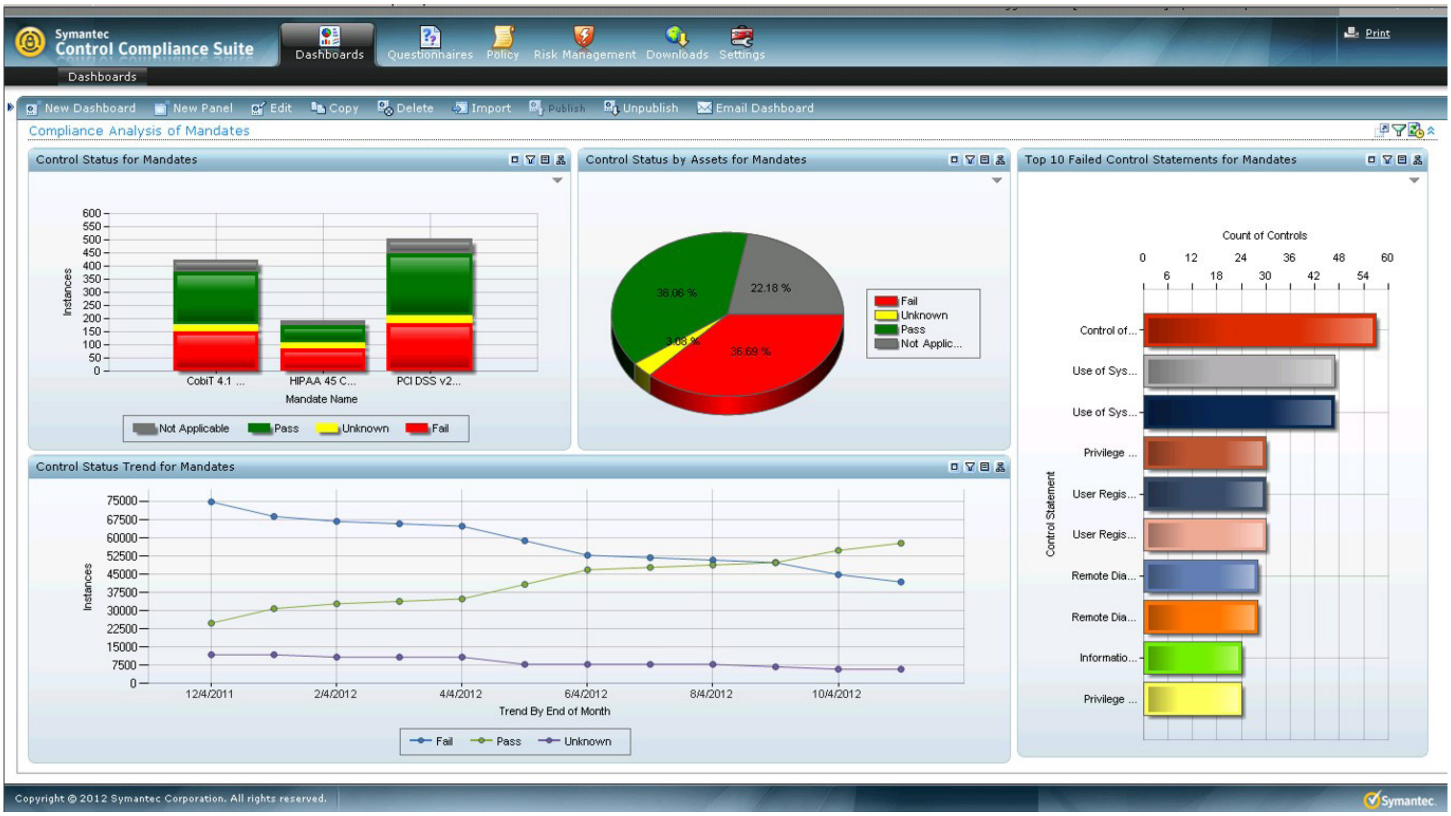


Figure 5: You can easily assess compliance for multiple mandates and overall compliance for all organizational controls.

Next Steps

Take the next step in learning how Control Compliance Suite can help you support HIPAA compliance and protect PHI while giving you a unified view of your security controls and risks. Learn More

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps businesses, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton suite of products for protection at home and across all of their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.