SOLUTION BRIEF

HITRUST Compliance Services Overview

The Challenge

Increasingly, covered entities are requiring that their service providers get HITRUST CSF Certified as a mechanism to substantiate HIPAA compliance and reduce the due diligence burden of multiple audits. Embarking on HITRUST Certification can quickly become complex as organizations need to navigate a new security framework, new reporting requirements, stringent assessment tools and processes, and work with authorized assessors for certification.

In the increasingly complex IT, cyber threat, business and regulatory environments, it is important for healthcare service providers and their business partners to understand risks and adapt security controls to protect electronic protected health information (ePHI). Leveraging the HITRUST CSF not only helps to protect brand reputation and avoid fines due to unfulfilled HIPAA requirements, it also helps streamline compliance processes and evidence a strong security program.

HITRUST CSF

HITRUST Alliance is a for-profit security organization. When formed in 2007 the intent was to establish a voluntary cybersecurity framework known as the HITRUST CSF. The vision was to take ISO, NIST, HIPAA, COBIT and other best practices to establish an authoritative source of healthcare compliance. Unlike certification frameworks like PCI and ISO 27001, the HIPAA statute and subsequent amendments do not outline a finite set of compliance or controls requirements, nor can covered entities or service providers be HIPAA certified by a qualified assessing body; and yet they must both be compliant with HIPAA.

Today, HITRUST CSF is the most widely adopted framework across multiple industries. Not only has it become a requirement in the state of Texas for covered entities and their business associates to obtain CSF Certification, it's increasingly becoming commonplace for covered entities to require their business associates to be HITRUST certified as a HIPAA due diligence mechanism.

The CSF and supporting tools are available from HITRUST; specifically, the MyCSF web-based platform created and managed by HITRUST. The secure platform can be used to perform assessments, manage remediation activities and report and track compliance to HIPAA, as well as 44 other authoritative sources. In addition, given the incorporation of multiple recognized frameworks, it also helps to achieve compliance to other best practice frameworks including ISO, NIST and PCI.

The HITRUST CSF was designed as a risk-based approach to organizational security. Recognizing the breadth of healthcare and information systems today,

The Solution

Secureworks is an authorized HITRUST External Assessor. In addition to conducting the required third party reviews against the HITRUST CSF, our experts can assist on the HITRUST compliance journey by providing advisory, consulting and remediation services to help you navigate the framework, best prepare for the assessments and certifications, and ultimately protect patient data by creating a repeatable compliance program.

the framework is flexible in allowing for the selection of controls that are reasonable and appropriate to individual organizations based on unique organizational, system and regulatory factors. Organizations looking at using HITRUST CSF need to navigate a new security framework, new reporting, stringent assessment tools and processes, and work with authorized HITRUST External Assessors for certification. Without a planned, thoughtful approach and understanding of the scope and requirements, the process can quickly become complex, resource heavy and costly.

How Secureworks Helps

Secureworks Consulting Approach to Compliance

As an Authorized HITRUST External Assessor, Secureworks is qualified to conduct third-party reviews for certification. In addition, we assist with preparation and remediation ahead of a formal certification. Secureworks HITRUST Compliance Services are designed to support you along your compliance lifecycle, whether you are looking to get certified for the first time, are thinking about getting certified or are looking to recertify. Our experts help you tailor your program to achieve business, security, and compliance objectives, from planning your approach, assessing your current state, through to remediation and compliance program development and implementation.

1. Preparatory Workshop: Plan Your Approach

The latest version of HITRUST CSF[1] is organized in 14 Controls Categories, which contain 49 Control Objectives and 156 Control Specifications based on ISO/IEC 27001:2005 and 27002:2005 and includes 3 levels of implementation based on a healthcare organization's unique organizational, system and regulatory factors. Before carrying out any assessment in MyCSF, the first step is to understand your business objectives and define your scope, so that you can determine the number of applicable controls and what to assess against.

The Secureworks HITRUST Preparatory Workshop helps you embark on your HITRUST certification journey with confidence. It is designed to provide expert-led guidance on your overall HITRUST Program approach to reduce cost, resource expense and duplicative efforts. External assessors help to enhance your understanding of the regulation, interpret the controls, define your organization's unique scope and can assist with starting to enter your data in MyCSF ahead of a self-assessment or validation.

Through collaborative sessions, we:

- Discuss and provide an overview on HITRUST CSF, potential obligations and best practices, and how they apply to your environment and your security program.
- Guide a high-level assessment and discussion around your existing controls through documentation reviews and interviews to inform a defined HITRUST scope and compliance requirements.
- Consult on program strategy to help mature your compliance program and prepare for a HITRUST audit. Risk-based, prioritized guidance is provided around: compensating controls, network segmentation, technology implementation, and other initiatives to advance your compliance with applicable requirements.

[1] HITRUST CSF v 9.3

Secureworks®

2. HITRUST CSF Security Controls Assessment: Assess Current State

A Secureworks Security Controls Assessment helps you identify gaps and weaknesses in your existing security controls. A HITRUST CSF Controls Assessment following a Preparatory Workshop helps to identify control-specific corrective action ahead of a HITRUST self-assessment or validated assessment.   Our experts take a security-centric approach to security assessments, with a focus on providing pragmatic, risk-based outcomes. A Controls Assessment includes:

- **Gap Analysis** - Secureworks reviews documentation and conducts a series of interviews with key personnel, and evaluates controls against the applicable Controls Categories, Objectives and specifications of the HITRUST CSF.
- **Controls Validation** - Secureworks validates that existing controls are consistent with those required by the HITRUST CSF and implementation tier outlined in MyCSF. This phase checks that controls are implemented as designed and documented, not merely that they exist.

3. Ongoing Compliance Support

With the Secureworks Compliance Support Retainer, authorized HITRUST External Assessors lend their expertise to provide ongoing compliance assistance, consulting and advisory services. This may include assistance in designing a compliance program, developing detailed plans for remediation, audit preparation and remediation. This may also include developing specific implementation plans or consulting on various remediation needs, including best practice advice and custom control creation to meet the intent of any identified gap.

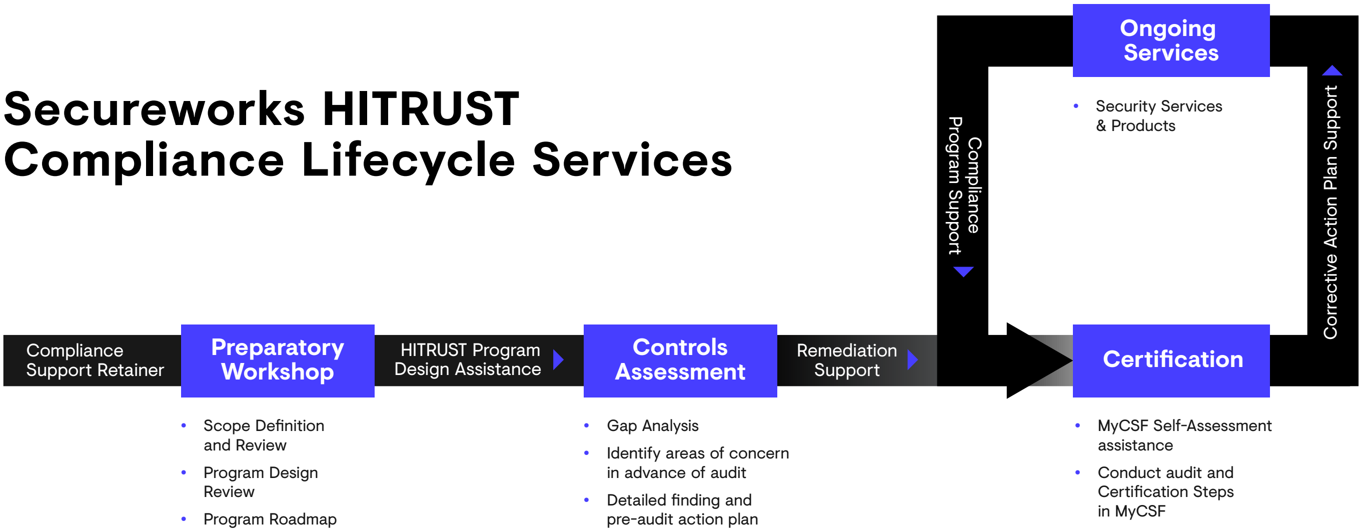
Testing, Operating and Managing your HITRUST Program

In addition, the broader Secureworks portfolio of cybersecurity products, services and expertise can help organizations test, operate and manage your compliance and security program.

1. Test & Exercise Your Program

To help you test, operate and manage your on-going compliance, Secureworks provides a range of technical and specialized consulting services to help you check your posture and conduct program assurance. This includes a suite of Adversarial Security Testing and Proactive Incident Response services to test system security, detection, and incident response capabilities, exercise and train your

Secureworks HITRUST Compliance Lifecycle Services



Compliance Support Retainer

Preparatory Workshop

- Scope Definition and Review
- Program Design Review
- Program Roadmap

HITRUST Program Design Assistance

Controls Assessment

- Gap Analysis
- Identify areas of concern in advance of audit
- Detailed finding and pre-audit action plan

Remediation Support

Certification

- MyCSF Self-Assessment assistance
- Conduct audit and Certification Steps in MyCSF

Corrective Action Plan Support

Ongoing Services

- Security Services & Products

Compliance Program Support

incident response teams, and hunt for targeted threats. These engagements are designed to provide your organization with assurance or highlight any new or further gaps requiring remediation.

2. Monitoring, Detection and Response

In addition to Advisory and Consulting Services, Secureworks offers a portfolio of Monitoring, Detection and Response products and services to support the ongoing management and operation of information security best practice.

Validate Compliance: HITRUST CSF Certification

As an Authorized HITRUST External Assessor, Secureworks can conduct the third-party review during the validated assessment process. Secureworks experts also provide support and guidance with the preparation of the of the Self-Certification Assessment via MyCSF.

HITRUST®
Authorized External Assessor

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist.
secureworks.com

About Secureworks

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world. We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Secureworks®