HITRUST
Self-Assessment ♦ Validation ♦ Certification

HITRUST Self-Assessment

HITRUST Validation & Certification

HITRUST Exec Brief

1000s of Clients | Clients in all 50 States | Clients on 5 Continents
What is the HITRUST CSF?

The HITRUST CSF is a common, standardized methodology to effectively and consistently measure compliance and risk via simplified information collection and reporting, consistent testing procedures and scoring, and demonstrable efficiencies and cost-containment; and additional assurances around the accuracy, consistency and repeatability of assessments due to the use of pre-qualified professional services firms—all of which is designed to meet the unique regulatory and business needs of the healthcare industry. It is a risk-based approach to selecting HITRUST CSF controls for assessment, including management oversight of the assessment. The HITRUST CSF Assurance Program delivers simplified compliance assessment and reporting that addresses healthcare federal, state and industry requirements for both covered entities and their business associates.

HITRUST Self-Assessment

The HITRUST self-assessment process enables your organization to establish a baseline of the current state of your policies, processes and controls—all of which are formally documented. We at ecfirst can assist your organization to go through this process and address HITRUST requirements for self-assessment. The self-assessment provides the foundation to identify key enhancements required to be initiated to improve the organization’s security and compliance profile.

HITRUST Validation & Certification

Self-assessment allows organizations to self-assess using the standard methodology, requirements, and tools provided under the HITRUST CSF Assurance Program. ecfirst supports your efforts to submit and manage the validation process. Validated assessment is conducted by ecfirst, a HITRUST Certified CSF Assessor. The CSF Assurance methodology is used and the controls are scored accordingly. Assessments meeting or exceeding the current CSF Assurance scoring requirements for certification is indicated as CSF Certified on the certification report.

HITRUST Exec Brief | Complimentary

Learn about the HITRUST CSF from the Team of Compliance and Cyber Security experts at ecfirst. Schedule a complimentary executive brief (Webinar) to walk thru key elements of the HITRUST CSF. Understand the process for conducting a HITRUST self-assessment, learn about HITRUST validation, and finally walk-thru the certification process. Knowledge transfer is at the core for all ecfirst client engagements. The journey of addressing HITRUST requirements may be challenging, and the requirements are comprehensive. We look forward to establishing ecfirst as your trusted partner within your enterprise.
HITRUST Services

HITRUST Demystified
Getting Started! A Simple Explanation

What is HITRUST CSF?
- A common, standardized methodology to measure compliance and risk
- Designed specifically for the healthcare industry
- Risk-based approach to selecting controls for assessment, including management oversight
- Simplified compliance assessment and reporting addressing healthcare federal, state, and industry requirements

What is MyCSF?
- User-friendly tool available through HITRUST
- Secure, web-based solution
- Adaptable to all types and sizes of healthcare organizations
- Reporting and tracking compliance

The CSF Framework
- A comprehensive, flexible, and efficient approach to regulatory compliance and risk management
- Consolidates healthcare-related regulations into one overarching security framework
- Provides structure, clarity and consistency, and reduces compliance burden
- Organized into 14 Control Categories, 45 Control Objectives, and 149 Control Specifications

Your HITRUSTed Partner, ecfirst!
- Complimentary HITRUST Exec Brief: Getting Started! (28 minutes, fast-paced facts about HITRUST Process & Timelines)
- Private HITRUST CSF Strategy 1-Day Workshop, ideal for CIO, CTO, ISO/CISO, Compliance, Legal, IT Leadership
- Complimentary seat(s) in industry leading Certified HIPAA Professional (CHP), Certified Security Compliance Specialist (CSCS), and Certified Cyber Security Architect (CCSA) programs
- Knowledge transfer throughout the HITRUST engagement
- Easy & immediate access to the ecfirst chief executive to address any requirements
- Unconditional guarantee of your compliance satisfaction!

Path to HITRUST CSF Certification

+1.515.987.4044 ext 25 | Kris.Laidley@ecfirst.com
Private! Onsite HITRUST Strategy Workshop (1 Day)

HITRUST CSF Controls

Information Security Management Program
Access Control
Human Resources Security
Risk Management
Security Policy
Organization of Information Security
Compliance
Asset Management
Physical & Environmental Security
Communications and Operations Management
Information Systems Acquisition, Development, & Maintenance
Information Security Incident Management
Business Continuity Management
Privacy Practices

Excellence cybersecurity strategy workshop for CIOs, CTOs, CISO/ISO, CEO, COO, CFO, and senior leadership!

+1.515.987.4044 ext 25 | Kris.Laidley@ecfirst.com
HITRUST Services

+1.515.987.4044 ext 25 | Kris.Laidley@ecfirst.com
<table>
<thead>
<tr>
<th>Fact</th>
<th>Myth</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. You don’t have to choose between HITRUST, NIST or ISO as your risk management framework</strong>&lt;br&gt;TRUE. The HITRUST CSF enables organizations to leverage ISO and NIST control standards, obtain the benefits of many other US and international standards, regulations and best practices and successfully address the objectives specified by the NIST Cybersecurity Framework.&lt;br&gt;Also, the CSF Assurance methodology ensures the accuracy, integrity, consistency and transparency of the assessment and enables a single assessment to be leveraged to demonstrate compliance across multiple standards and regulations (HITRUST refers to this as “assess once, report many”).</td>
<td><strong>1. Adopting and complying with the HITRUST CSF is more complicated compared to other frameworks</strong>&lt;br&gt;FALSE. In fact, by harmonizing the relevant US and international standards, regulations and best practices into a single privacy and security framework that is tailor able based on risk and regulatory factors, gives it many advantages over others.&lt;br&gt;The design ensures organizations select the requirements relevant to their environment which means organizations can minimize the need to address irrelevant requirements. It also allows organizations to implement controls that satisfy multiple requirements, unlike other governance frameworks. Making it more efficient and certainly no more complicated while reducing waste and costs compared to the adoption of other frameworks.</td>
</tr>
<tr>
<td><strong>2. The HITRUST CSF is a Risk-Based framework</strong>&lt;br&gt;TRUE. To understand why, one must understand the intent of selecting and implementing any specified set of controls, whether it’s a custom set developed from a traditional risk analysis or one tailored from a pre-defined control baseline developed from such a risk analysis (e.g., ISO/IEC 27001 or NIST SP 800-53, both of which HITRUST leverages in the CSF). This risk analysis, tailored to specific risk factors and updated regularly, is part of the unique elements of the HITRUST CSF.</td>
<td><strong>2. You can adopt the NIST cybersecurity framework by itself</strong>&lt;br&gt;FALSE. If you adopt the NIST Cybersecurity Framework, you must either design your own controls or select controls from a suitable Risk Management Framework (RMF) to achieve the objectives specified by the framework. The HITRUST CSF is an integral part of the HITRUST RMF, which fully supports an organization’s implementation of the NIST Cybersecurity Framework’s Core Subcategories.&lt;br&gt;The HITRUST CSF Assurance Program helps organizations provide reliable assurances to internal and external stakeholders (e.g., executive management and government regulators) about its information protection program through the lens of the NIST Cybersecurity Framework.</td>
</tr>
<tr>
<td>Fact</td>
<td>Myth</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td><strong>3.</strong> NIST doesn’t provide a certification against the NIST cybersecurity framework</td>
<td><strong>3.</strong> Getting assessed against the HITRUST CSF is more expensive than other assessments</td>
</tr>
<tr>
<td><strong>TRUE.</strong> While NIST doesn’t provide a certification, HITRUST provides a viable alternative by mapping the NIST Cybersecurity Framework Core Subcategories into the HITRUST CSF. Also, HITRUST has added an addendum to the HITRUST CSF Assessment report to provide a scorecard of the HITRUST controls by NIST Subcategory for use as a management reporting tool. So, while NIST does not provide for certification, HITRUST gives organizations a level of assurance they are meeting the objectives specified by the NIST Cybersecurity Framework.</td>
<td><strong>FALSE.</strong> By designing the HITRUST CSF Assurance program to allow a single CSF Assessment report to support multiple objectives, organizations can ‘assess once, report many.’ One assessment can be used to produce a HITRUST CSF Certification, AICPA SOC 2 and NIST Cybersecurity Scorecard. One assessment can also support attestations of compliance with other standards and regulations such as ISO 27001, NIST SP 800-53 and HIPAA. HITRUST provides the most cost-effective approach to providing assurances to customers, business partners and regulators in the industry.</td>
</tr>
<tr>
<td><strong>4.</strong> A SOC 2® by itself is not a valid means for a third party to understand the information security controls in place at an assessed entity or to determine the assessed entity’s adequacy in protecting its data</td>
<td><strong>4.</strong> A HITRUST CSF Assessment won’t meet the requirement for a HIPAA Risk Assessment</td>
</tr>
<tr>
<td><strong>TRUE.</strong> The SOC 2 itself does not provide the full context for the controls needed to achieve the objectives specified by the AICPA® Trust Criteria for Security, Confidentiality and Availability versus being based on a comprehensive set of prescriptive yet tailorable controls such as those provided by the HITRUST CSF information protection framework. Without this context, it would be difficult for an organization to determine if the controls presented in the SOC 2 report are appropriate for the organization. A SOC 2 report leveraging the HITRUST CSF ensures organizations address the AICPA Trust Criteria with a reasonable and appropriate set of security and privacy controls. Also, it ensures organizations provide an industry-acceptable level of residual risk and satisfy their contractual and regulatory compliance requirements.</td>
<td><strong>FALSE.</strong> But it is not black and white. To be HIPAA-compliant, an organization must conduct a risk analysis and implement a reasonable and appropriate set of information safeguards—aka information security controls—to provide for the adequate protection of ePHI against all reasonably anticipated threats. HITRUST addresses this requirement by completing a control framework-based risk analysis and creating a new industry-level security control baseline, which organizations can then tailor to address their specific clinical and business needs. And since HITRUST provides an extensive mapping of the CSF controls to the HIPAA Security Rule’s standards and implementation specifications, it’s easy to see how the control requirements address each and every standard and implementation specification in the Security Rule. In fact, OCR has previously accepted an organization’s implementation of the HITRUST CSF its subsequent use of CSF validated assessments as evidence of its compliance with the HIPAA Security Rule, including the risk analysis requirement.</td>
</tr>
<tr>
<td>Fact</td>
<td>Myth</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>HITRUST expanded CSF V9.1 to address GDPR and New York state cybersecurity regulations</td>
<td>HITRUST is not an Industry Standards Organization.</td>
</tr>
<tr>
<td>TRUE. In March of 2018, HITRUST made the HITRUST CSF – a widely used information privacy and security framework for organizations – more open and comprehensive, so that it could be applied more effectively across a variety of global industries.</td>
<td>FALSE. HITRUST is and has been widely recognized as a standards organization and developer of the HITRUST CSF, an information security and privacy controls framework used by a variety of industry sectors. We operate similarly to ISACA, ISO and NIST, are governed by a Board of Directors, and receive guidance from multiple industry councils. The work of the HITRUST standards organization is also supported by multiple industry working groups to ensure the HITRUST CSF continues to address a constantly changing risk environment and meet the needs of industry.</td>
</tr>
<tr>
<td>HITRUST CSF Version 9.1 incorporates both the EU General Data Protection Regulation (GDPR) and New York State Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500). Incorporation of the EU General Data Protection Regulation (GDPR) is part of HITRUST’s initiative towards internationalization of the CSF and increased support for global organizational privacy programs. The updated framework allows organizations to easily manage and report on the controls intended to address GDPR requirements.</td>
<td></td>
</tr>
<tr>
<td>Integrating the New York State Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500) into the HITRUST CSF enables the financial industry to leverage the framework to achieve better cybersecurity resilience and protection. The requirements for Financial Services Companies not only affects financial institutions but also healthcare organizations such as health insurers and their business associates, including those outside of New York.</td>
<td></td>
</tr>
</tbody>
</table>
Learning Objectives

In this one-day strategy workshop focused on security and compliance, you will:

- Examine business compliance priority based on 2019 regulatory enforcement
- Learn how to align cyber and compliance priorities with the HITRUST CSF framework
- Leverage the HITRUST CSF standard to establish a credible cybersecurity program
- Walk thru HITRUST CSF fundamentals
- Identify next steps to launch initiatives to achieve HITRUST CSF certification

Private On-Site Workshop

Target Audience

- Senior IT & Security Professionals
- CISO
- Compliance Officer(s)
- Risk Management
- IT Managers & Directors

Review select HITRUST CSF policies, live, in-class!
Distinguish Yourself in the Marketplace

Get the CSCS™ Credential! Just having a background in IT or information security is not sufficient anymore for the challenges of business today. Employers are looking for individuals who not only have IT skills but also understand compliance regulations that impact their industry and business – because these are priorities that must be met.

Learning Objectives

- Learn about FISMA, NERC CSS, HIPAA Security Rule.
- Examine business critical standards & requirements such as PCI DSS, SOC 2 and more.
- Learn about authentication requirements in published guidance documents.
- Examine California's SB 1386, SB 541, AB 1950, AB 1298, AB 211 & other U.S. State information security related regulations.
- Step through processes for conducting a comprehensive risk analysis and vulnerability assessments.

Target Audience

The complete two-day CSCS™ program is of value to compliance professionals and managers, information security officers, security practitioners, privacy officers, internal compliance auditors and senior IT professionals.

Modules

Module 1: Introduction
Module 2: PCI DSS
Module 3: Healthcare Information Security
Module 4: ISO 27000
Module 5: ISO 27001
Module 6: ISO 27002
Module 7: U.S. Federal & State Regulations
Module 8: NIST Standards & Guidance
Module 9: Business Continuity Planning (BCP)
Module 10: Cyber Security Strategy

Partial Client List

- U.S. Air Force
- Brookshire Brothers
- U.S. Army Reserve
- Aultman Health Foundation
- BrightOutcome, Inc.
- Northwest Community Healthcare
- Wells Fargo Services
- National Health Insurance Authority
- Essex County Hospital
- Outcomes Health Information Solutions

Program Testimonials

"CSCS™ is a detailed information security program that will expose you to not only the basics in information security but also content to put you on the road to excellence. This is a real loaded course. I recommend all take this program. I consider Ali Pabari as a very knowledgeable person in this field."

Dennis Silsobe Kuame
National Health Insurance Authority (NHIA)
CCSA™ is an instructor-led 1-day program. It validates knowledge and skill sets in cyber security with particular focus and emphasis on the development of an applicable cyber security incident response and an enterprise cyber security program.

Learning Objectives

- Examine and build a practical and applicable cyber security program for an organization
- Step through core components of an actionable incident response plan
- Identify policies that reflect an organization’s priority for security in the areas of risk assessment, mobile devices, cloud computing, encryption, and more
- Walk thru incident management and other checklist documents to establish consistency in monitoring enterprise security capabilities
- Learn about key reference sources vital for managing an enterprise cyber security program

Target Audience

The complete one-day CCSA™ program is of value to compliance professionals and managers, information security officers, security practitioners, privacy officers, and senior IT professionals.

Industry Thought Leadership

“Best class I have ever taken! Instructor was very prepared for the CCSA™ Program. The strength of the program is that it beautifully covers the area of cybersecurity. The course made a complex area logical and simple. Provides me with ability to qualify questions to assess my clients. I am now able to articulate to all stakeholders in the corporate office why this program will be important to them – CEO, Legal, Compliance, InfoEngineering, CIO, CSO, CTO, Privacy Officer, even HR. Overall rating of the course: 10. Overall rating of instructor: 10.”

Katherine Finley
Konica Minolta

“The course was very beneficial and with in-depth cybersecurity information. This helped enhance the security knowledge of the attendees. Mr. Patrai highlighted and covered most areas starting from the history of security and included relevant examples. Overall rating of instructor: 10. Overall rating of course: 10.”

Mohammad Ali Al Hallami
Etisalat

www.ecfirst.com
Client Reference

"I just wanted to take a moment and say thank you. Thank you and the excellent team at ecfirst for hard work, late hours and diligence during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an exceptional partner that labored incredibly hard for us, with us. The ecfist insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time. We look forward to deeper collaboration with ecfist in the cybersecurity space in the future. I continue to recommend ecfist highly and often!"

Chip Goodman | Vice President of Information Technology

"The ecfist team literally helped us build our HIPAA practices from ground up since 2012, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfist to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfist as an integral part of our business strategy and have been extremely satisfied with the quality and value of the services that ecfist has rendered."

DerShung Yang | Founder & President

"Provant Health partnered with ecfist to build a plan and assist in executing it with the goal of achieving HITRUST certification. Ali Pabrai and his team were flexible, collaborative and most importantly patient as we worked to educate our management team and key employees on the meaning and value of HITRUST. I'd recommend ecfist to any company who wants to understand HITRUST or work on assessing and remediating their processes and systems in preparation for certification."

Tom Basillere | Chief Information Officer
Corporate Office
295 NE Venture Drive
Waukee, IA 50263
United States

Kris Laidley
Inside Sales Support Coordinator
ecfi rst/HIPAA Academy
Phone: +1.515.987.4044 ext 25
Email: Kris.Laidley@ecfirst.com

www.ecfirst.com
© 2019 All Rights Reserved | ecfi rst