

Founding members:



The Security Division of EMC



HITRUST is experiencing significant demand from healthcare organizations requiring assistance and guidance in identifying information security products that aid in compliance with the myriad of security regulations and the HITRUST Common Security Framework (CSF). Driving this demand is the uncertainty organizations face when selecting products that will aid in their compliance efforts and the lack of clarity found in product descriptions and claims.

The CSF Ready Program has been established in response to this need and designed to develop criteria and provide consistency for how information security products and services are evaluated; thus, reducing the complexity and aiding in the procurement process for both large and small organizations faced with identifying and implementing security solutions.

The program is coordinated by a steering committee comprised of leaders from the security assurance and information security communities. HITRUST and these industry leaders are committed to providing the necessary guidance and resources to support healthcare organizations in making informed purchasing decisions.

In addition, an advisory committee, consisting of security professionals representing healthcare organizations, has been established to provide guidance and interact with the other committees. The program is seeking additional participants from the security assurance, information security and healthcare communities to ensure that input from a variety of organizations and the industry overall is considered.

What is the mandate of the CSF Ready Program?

The CSF Ready Program is centered on the creation of criteria focused to aid organizations in determining a product's capabilities, functionality, effectiveness and support of security practices, and aid in CSF compliance. The criteria developed will provide acceptable capability guidance for the healthcare industry as well as HITRUST Assessors so that organizations can make informed purchasing decisions when selecting security controls. The steering- and sub-committees will take into account both the functional and technical requirements for protecting personal health information.

The criteria developed will be the basis for which products or services are evaluated by independent entities to achieve CSF Ready status. The CSF Ready designation will enable organizations to more quickly assess that a product or service does what is expected of it and meets the requirements of the CSF.

What role will existing certifications play in the CSF Ready Program?

The output from the CSF Ready Program is not intended to replace other high-security certifications, but is meant to establish an alternative for organizations trying to streamline compliance costs while at the same time working to comply with the numerous evolving state and federal regulations and industry standards. As part of this effort, the committee members will identify and leverage acceptable capabilities and existing independent certifications that meet or exceed them. Thus, products already obtaining various certifications will be able to more easily obtain CSF Ready status, as well as allow those obtaining the CSF Ready designation to have a stepping stone to other high-security certifications.

Specifically, this will involve:

1. The prioritization of security control categories for which criteria should be generated.
2. The creation and oversight of sub-committees for setting criteria for products and services in specific security control categories.
3. The acceptance or rejection of recommendations from those sub-committees.

What is the role of a sub-committee?

Sub-committees will be created by security control category to establish acceptable capability criteria for products and services in each category and to provide recommendations on actions necessary to achieve CSF Ready status. The resulting criteria will be presented to the steering committee for acceptance.

How do I get involved?

Visit www.HITRUSTalliance.net/csfreeady to express interest in participating in the program or contact HITRUST at info@HITRUSTalliance.net.

Information security organizations must also be participants in the HITRUST Leadership Roundtable or the CSF Products and Services Guide to be eligible for membership in the steering committee or associated sub-committees. Visit www.HITRUSTalliance.net to learn more.

About HITRUST

The Health Information Trust Alliance (HITRUST), in collaboration with healthcare, business, technology and information security leaders, has established the Common Security Framework (CSF), a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information. Beyond the establishment of the CSF, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy and other outreach activities.

“With security becoming a pillar of every healthcare organization, the industry warrants attention and criteria directed at information security products that are applicable to their unique needs. The success of an organization’s information security efforts should not be deterred by a complicated evaluation and selection process. It is this group’s intent to provide acceptable capability guidance for organizations of all sizes so they can achieve a higher level of confidence that a product does what it claims it can do for them.”

– Stuart McClure,
Vice President, Operations &
Strategy
McAfee Risk & Compliance
Business Unit