

Frequently Asked Questions: HITRUST and Common Security Framework Value Proposition

Q. Why should I pay to reference another new standard, when we have access to HIPAA, ISO and other standards?

A. Significant return on investment

The HITRUST Common Security Framework (CSF) is a security controls framework and not a new standard; this is a misconception. The HITRUST CSF is a framework that normalizes the security requirements of healthcare organizations including federal (e.g., ARRA and HIPAA), state, 3rd party (e.g., PCI and COBIT) and government (e.g., NIST, FTC and CMS). The CSF also supplements and provides the clarity and consistency lacking in many standards and regulations.

HITRUST has a number of toolsets developed and others planned, which are immediately needed by healthcare organizations to understand security risks, protect their environments, and comply with regulatory requirements. Organizations may incur up to ten times the cost of these initial HITRUST toolsets to develop them independently:

- Integrated security and privacy training
- Security configuration checklists for applications, such as EHRs
- Guidelines for security professionals with respect to the FTC Red Flags rule
- Security classifications for clinical systems
- RFP security requirements list for medical device manufacturers
- Assessment capabilities against the CSF

Because of HITRUST's close collaboration with the industry, we can quickly identify and respond with solutions to those issues that consistently present the greatest challenge for organizations.

For no charge, qualified* organizations can use the CSF to ensure that their policies are aligned with all of these requirements and continuously stay updated with new requirements. An average organization would incur \$24,000 to \$50,000 to do this independently and would additionally incur a minimum of \$6,000 per year to maintain their policies.

A. Reduced regulatory exposure through industry-wide effort

Despite the prevalence of standards, organizations are still struggling with the discrepancies and ambiguities between the requirements. By registering with HITRUST, an organization can rely on the joint decisions of an industry group as validation for their positions and obtain guidance on leading practices. Organizations in this industry all need to tackle similar challenges; there is limited competitive advantage versus the risk exposure to addressing these

issues independently. If organizations with million-dollar security budgets perceive value in leveraging industry resources to collaborate on these challenges, why would smaller organizations watch from the sidelines?

By registering on HITRUST Central, the only professional networking forum dedicated to healthcare information security, organizations get access to the CSF, related tools and can collaborate with experienced security professionals across the nation.

Q. The CSF standard is too burdensome for healthcare organizations and beyond the requirements of HIPAA.

The HITRUST Common Security Framework (CSF) is not a new standard. The HITRUST CSF is a framework that normalizes the security requirements of healthcare organizations including federal (e.g., HITECH Act and HIPAA), state, 3rd party (e.g., PCI and COBIT) and government (e.g., NIST, FTC and CMS), so the burden of compliance with the CSF is no more than what already applies to healthcare organizations. HIPAA is not prescriptive, which makes it difficult to apply and open to interpretation. Organizations will need to reference additional standards for specific guidance on requirements specified by HIPAA. It is also not the only set of security requirements healthcare organizations will need to address (e.g., PCI, state or business partner requirements). The CSF was built to simplify these issues by providing direction for security, tailored for the needs of the organization. The CSF is the only framework that is built to provide scalable security requirements based on the different risks and exposures of organizations in the industry. The CSF also makes security manageable and practical by prioritizing 1/3 of the controls as a starting point for organizations. These priorities are based on industry input and analysis of breach information in the industry. There is no other relevant resource for healthcare organizations to reference for prioritizing their initiatives and validating their investments in security.

Q. How do I leverage the CSF for managing business partner security especially when many of them are not healthcare organizations?

Simplifying efforts and containing the cost of managing business-partner security is a primary deliverable of the CSF and the HITRUST CSF Assurance Program. When you ask your business partners to report or accept compliance with the CSF, you are asking them to align and accept the regulatory and statutory requirements of healthcare organizations as well as internationally recognized standards, such as ISO 27001 and 27002. This structure makes the CSF applicable to any organization. The framework also enables business partners to determine the requirements that are specifically related to their organizations. This allows both covered entities and business partners to reduce the time, resources and confusion regarding applicable controls in reporting and monitoring compliance. There's just no other practical option that is sustainable, can help contain cost, and actually improve security compliance over time.

Q. Why should I subscribe now and not wait until there is broader adoption in the industry?

There is already broad adoption by organizations from all segments of the industry. For these organizations, there is a range of reasons they joined HITRUST Central now:

- For those organizations that were originally taking a wait-and-see approach, not proactively adjusting their security programs to the new regulatory environment, they found that they were falling behind the curve and exposed to regulatory scrutiny and penalties. Adopting the CSF has helped these organizations jump-start their security efforts.
- Organizations that are just starting to realign policies, training and their overall programs, significantly enhance the value of their organization's investments in security by subscribing to the CSF, providing them with clear guidance on sound security practices.
- Organizations that are consistently driving to a higher standard of information security and compliance joined to leverage the combined resources of other industry leaders in tackling significant security challenges. These organizations are leading the way for themselves and the rest of the industry to achieve a higher standard for security in healthcare. Their leadership is critical because security is only as effective as the weakest link in the chain of organizations with access to healthcare information.

Q. How does HITRUST Central or the CSF help us better or more efficiently address security issues in my applications?

HITRUST's objectives include simplifying and assisting organizations with securing applications within their environment. The challenges expressed by HITRUST-participating members and our associated solution content and tools are described below.

A lack of prescriptive direction on controls, such as password strength requirements, level of logging, use of encryption, and many others.

- The CSF provides prescriptive direction for controls that are aligned with security requirements of healthcare organizations including federal (e.g., ARRA and HIPAA), state, 3rd party (e.g., PCI and COBIT) and government (e.g., NIST, FTC and CMS). The CSF also supplements and provides the clarity and consistency lacking in many standards and regulations.
- By aligning with the CSF, organizations can configure security for systems based on the joint input of an industry group.

A lack of information for implementing and managing security controls

- The HITRUST Security Configuration packs provide step-by-step guidance on how to securely deploy, configure and manage application security.

- HITRUST partners that provide automated configuration and vulnerability analysis tools will add these checks to their products. Finally, healthcare organizations will have access to tools for proactively assessing and managing the security configuration of their healthcare applications.

Confusion about adopting compensating controls and confusing guidance from audit firms

- HITRUST developed the alternate controls process and associated data repository to simplify how the industry addresses compensating controls. Organizations can submit requests for alternate controls to a review board comprised of a cross section of industry organizations and assessment firms. Approved requests are added to the CSF so other organizations seeking options for alternate controls can leverage the analysis and decisions of peer organizations in the industry. For the first time, assessment firms, healthcare organizations and business associates will have a point of reference provided by HITRUST for decisions and dialogue around alternate controls.

The CSF and associated processes and tools described above are accessible via HITRUST Central, which provides a community platform for organizations to share their experiences and challenges.

Summary of HITRUST Central and the CSF’s return on investment for subscribing organizations

By leveraging resources from across the industry, organizations will realize the following benefits by subscribing to HITRUST:

HITRUST Value	Cost	Value to organizations ¹
HITRUST CSF - Requirements normalized for healthcare organizations	No charge for qualified* organizations	Initial alignment of \$24,000 to over \$50,000 for medium sized organizations On-going alignment \$6,000 per year
HITRUST Central - Reduced regulatory exposure by leveraging the prescriptive recommendations of the CSF developed through industry collaboration		Priceless
Toolsets to support the assessment and adoption of security <ul style="list-style-type: none"> • Commonly adopted report of the organization’s security program validated by HITRUST • Guidelines for security professionals with respect to the FTC Red Flags rule • Business associate and overall vendor management guidelines • RFP security requirements list for medical device manufacturers • Security classification for clinical systems 	\$3,100 for qualified* organizations \$10,000** for unqualified organizations <i>*a qualified organization is defined as any organization employing a function or activity involving the use or disclosure of individually identifiable health information, provided that said organization does not provide technology or security products or services. Additionally, as any federal, state, or local agency or department is considered a qualified organization. HITRUST has the right to verify eligibility. ** includes one seat in HITRUST Training for Practitioners</i>	10 times the cost for each toolset
Self assessment with CSF Validated report for single-use	\$1,000	Single assessment vs. multiple proprietary assessments
Self assessment with CSF Validated report for unlimited use	\$2,500	

¹ High level estimates based on a resource cost of \$78,000 per year and feedback from HITRUST subscribers