

## CSF Assessment for Small Organizations

### New risk assessment approach simplifies data collection process and improves accuracy

In today's world of electronic health records and health information and data exchanges, the need for information protection is more important than ever. Evaluating information security risk based on the number of records, employees and facilities is no longer a valid model. The adoption of electronic information systems and the resulting outcome of interconnectivity and electronic data exchange between organizations exponentially increases risk and requires an entirely new approach to protecting personal health information.



The passing of the HITECH Act and introduction of health information exchanges has led to greater automation and interconnectivity between organizations that historically operated very independently. Healthcare organizations and business associates with annual revenue less than \$25 million represent the largest market segment working with protected health information (PHI). The segment includes U.S. physician practices, of which there are more than 400,000 clinics and outpatient centers, and business partners that serve covered entities of all sizes.

The vast number of small organizations and the immense volume of PHI they process, combined with their use of electronic systems, make this small-business segment susceptible to unique risk and challenges for protecting PHI due to lack of security knowledge and devoted security personnel, limited budgets and resources, and the need for continuous access to patient data by physicians.

Having an accurate understanding of an organization's information protection environment is critical for both the individual organization and those with which they conduct business. The inability of small organizations to implement cost-effective and manageable information security programs can have a harmful industry effect.

It's imperative organizations understand the expectations placed on them by various regulations and third parties and that they are able to translate these expectations into information protection requirements. A correctly performed risk assessment provides valuable information about the safeguards and policies an organization has in place to protect its own level of information security and for its partners assessing the risk associated in conducting business with the organization.

Unfortunately, performing a risk assessment around information protection requires certain knowledge of information security, privacy and technology that isn't always available, especially in smaller organizations. Because of this, the assessment results can be meaningless or not provide an accurate picture; whereby, providing no value to the assessed entity and an incorrect perspective to its business partners.

### Inadequate reporting of security controls

Analysis has shown small organizations often provide inaccurate or incomplete information when using self-assessment questionnaires to communicate the status of their security controls to third parties. The reality is a large portion of the segment lacks the resources and knowledge to respond accurately and thoroughly to complex questionnaires. The assessments that are completed are often incomplete, inaccurate and do not provide a complete picture of an organization's security controls. Most small organizations do not have the programs in place to assess, monitor and improve their security environments or seek the help they need. This leaves third parties that rely on these assessments to operate with incorrect perceptions of the risk posed by their business partners.

## Security risk assessment tailored to unique needs of small organizations

The healthcare industry requires a user-friendly risk assessment approach with understandable and actionable results. HITRUST created the CSF Assessment for Small Organizations for healthcare organizations and business partners with annual revenue less than \$25 million. The solution equips these organizations with the tools needed to conduct an effective and valuable assessment and provides them with a HITRUST CSF Validated report that can be used to seek remediation assistance and communicate the state of their security controls to third parties, including state and federal agencies, health information organizations, customers, health organizations and business partners.

The solution is a component of the HITRUST CSF Assurance program and leverages the HITRUST Common Security Framework (CSF), the most comprehensive and widely adopted healthcare security control framework. The CSF Assurance program includes approaches for onsite, remote and self assessments and is already the most widely used approach for documenting risk assessment information in the healthcare industry.

### HITRUST CSF Assessment for Small Organizations

Recognizing that existing self-assessment approaches were not able to effectively and accurately assess small organizations, HITRUST customized its standard and cost-effective assessment approach to meet the unique needs of small organizations. The tools used to collect the data analyzed for the assessment report include the HITRUST small business questionnaire and automated internal and external scans conducted with technology powered by nCircle.

The combination of a forms-based questionnaire and automated data collection through the vulnerability scans makes this the only service that delivers a complete internal and external assessment of security risk and verification of security controls.

### User-friendly tools accurately capture data for assessment report

A simpler yet more accurate and effective method of garnering information, the CSF Assessment for Small Organizations does not require any special skills, resources or additional hardware or software.

The questionnaire is tailored for small organizations and asks simple, straightforward questions that focus on key areas of risk that are most likely to result in a breach such as wireless security and secure information transmission. The simplified questionnaire contains approximately 50 questions that require only basic knowledge of technologies used and general information on security policies and practices.

The screenshot shows the HITRUST CSF Assessment for Small Organizations dashboard. At the top, there is a 'Tunnel Connected' status indicator and a 'Scan in progress...' progress bar. The main content area is divided into several sections:

- Start Scan:** A button to initiate a scan, accompanied by instructions: "Click start to begin your assessment. A wizard will walk you through the assessment process. Please note that your browser must stay open to complete your scan. Once your scan has completed, your report will be available from HITRUST."
- Scan History:** A table listing previous scans with columns for Scope, Scan, Risk, Date, Status, and Actions.
- Scan Details:** A table for viewing details of a specific scan, with columns for IP Address, DNS, Found, OS, and Risk.

Navigation links at the top right include: [CHIP Dashboard](#) | [Buy](#) | [Purchase History](#) | [My Account](#) | [Logout](#). The HITRUST logo (Health Information Trust Alliance) and the nCircle logo (powered by nCircle) are also present.

Scope	Scan	Risk	Date	Status	Actions
test group 3	12	0		Canceled	<a href="#">Retry</a>
test group 3	11	0	12/02/2010 10:07:58	Submitted	<a href="#">Retry</a> <a href="#">Help</a>
test group 3	10	0	12/01/2010 17:13:24	Submitted	<a href="#">Retry</a> <a href="#">Help</a>

IP Address	DNS	Found	OS	Risk

The internal and external vulnerability scans are an automated method of gathering information about an organization's security environment that most small organizations are not equipped to answer accurately when completing a self-assessment questionnaire. To further ensure ease-of-use, no additional hardware or software is required by the organization conducting the scan. By incorporating a vulnerability scanning capability with the small-business questionnaire, HITRUST is able to provide organizations with a faster and more accurate method of collecting assessment information and offer third parties the information required to accurately and effectively evaluate the risks to their own organizations.

The questionnaire and scan results are analyzed by HITRUST and incorporated into a CSF Validated report, which can aid an organization in complying with the HITRUST CSF, addressing meaningful use, and meeting regulatory requirements such as HIPAA. The report also provides a consistent representation of risk exposure and benchmarking results against similar organizations. In addition to the assessment report, an organization will be provided with the detailed vulnerability scanning information collected during the assessment so that it has the complete details on any gaps in its information protection environment and can address or seek assistance as appropriate.

The standard report, already accepted and understood by many organizations, can be used to meet the risk assessment requirements of meaningful use, communicate an organization's state of security to third parties and can also be used, along with the scan results, to seek remediation assistance and solutions from third-party information security consultants and technology vendors. HITRUST is allowing organizations to run additional scans free of charge during the first 90 days following the initial scan so as to verify the status of their remediation efforts.



## Get Started

The CSF Assessment for Small Organizations offers organizations the benefits of a remote assessment for the low cost of a self assessment. HITRUST offers two pricing options for small organizations choosing to conduct a self assessment and communicate the assessment results to third parties.

Self assessment report distribution options	Pricing
Conduct an assessment and receive a CSF Validated report for unlimited distribution when purchased with a Professional subscription to HITRUST Central.	\$500.00 <sup>1</sup>
Conduct an assessment and receive a CSF Validated report for unlimited distribution.	\$2,500.00

To purchase, visit [hitrustalliance.net/portal](http://hitrustalliance.net/portal) to register for the service or contact HITRUST at [sales@HITRUSTalliance.net](mailto:sales@HITRUSTalliance.net).

<sup>1</sup>Total bundled price for Professional subscription to HITRUST Central and unlimited distribution of a CSF Validated report is \$6,000. Bundled option available only to qualified organizations.<sup>2</sup>

<sup>2</sup>A qualified organization is 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**. HITRUST has the right to verify eligibility.

## 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.