Frequently Asked Questions About
the HITRUST Risk Management Framework

Addressing common questions and misconceptions about the HITRUST CSF,
CSF Assurance Program and supporting methods and tools, and their value to industry

August 2016
Introduction

The Health Information Trust Alliance (HITRUST) was formed in mid-2007 to ensure that information security is a core pillar of, rather than an obstacle to, the healthcare industry. The original HITRUST Board of Directors, which included Chief Information, Security and Privacy Officers from leading healthcare providers, insurers, and vendors understood that information security was critical to the broad adoption of healthcare technologies and systems necessary to provide a greater quality of care.

With the advent of the HITRUST CSF (CSF), organizations were given a consensus-driven solution to address problems with security in the industry. The CSF not only provides the prescriptiveness needed for healthcare organizations to effectively implement controls to meet regulatory, third-party and business requirements, it also did it in a way that was scalable based on key organizational, system and regulatory risk factors. These factors, which were developed through industry working groups representing a variety of healthcare sectors, allow large, highly complex healthcare insurers as well as smaller, resource-constrained providers to adopt an approach to security that may be tailored to their risk and compliance needs.

Today, the CSF is the most widely adopted information security and compliance risk management framework in the healthcare industry. Through annual updates and significant community engagement, the CSF has evolved to effectively align the requirements and controls of over 15 standards, regulations, and leading practice frameworks. Organizations are also proactively seeking certification and validation of their CSF-based information protection programs through the CSF Assurance Program due to the value it provides, especially with regard to third-party assurances for regulators and other external stakeholders.

However, the HITRUST approach is not always well understood by healthcare organizations, including some advisory and consulting firms. This is because the HITRUST approach has some unique aspects that are not always understood by those commenting or offering their opinion. Unlike others, HITRUST takes a rigorous approach to the selection and assessment of controls by leveraging federal and industry leading practices that fully support the type of robust and comprehensive information protection program required under the HIPAA Security Rule. HITRUST also looks at underlying risk exposures to ensure the CSF, CSF Assurance Program, and supporting methodologies and tools align with industry requirements.

Recent improvements to the CSF include the alignment of cyber threat intelligence to CSF control requirements, which helps ensure controls remain effective despite an evolving cyber threat environment. HITRUST has also mapped the CSF controls to the American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria, which allows CSF Assurance Program assessments to be leveraged for Service Organization Control (SOC) 2® reports.

The following Frequently Asked Questions (FAQs) are provided to address common misconceptions about the CSF, CSF Assurance Program, and supporting methods and tools that constitute the HITRUST Risk Management Framework (RMF).
Introduction

The HITRUST CSF

Why does healthcare need a security framework?

What were the industry’s goals for the CSF?

How is the CSF structured?

Is the CSF an industry standard for healthcare?

Is the CSF a compliance-based or risk-based framework?

Does the CSF take a “one-size-fits-all” approach to information security?

Is the scope of the CSF too large for most healthcare organizations?

Why choose the CSF over other control frameworks like NIST SP 800-53 and ISO/IEC 27001?

How many organizations have adopted the CSF?

Has the CSF been adopted internationally?

The CSF Assurance Program and Certification

What is the HITRUST CSF Assurance Program?

What types of assessments are available in the CSF Assurance Program?

What is the process for an organization to achieve HITRUST CSF Certification?

Is a HITRUST CSF validated assessment more expensive than comparable assessments?

How many organizations have completed a HITRUST CSF assessment?

If I’m HITRUST CSF certified, does that mean I’m HIPAA-compliant?

How does a CSF assessment meet the HIPAA requirement for a risk analysis and can it be used to support an OCR audit?

Do HITRUST Certification programs provide safe harbor in the event of a breach?

Does the use of alternate controls diminish the value of HITRUST Certification?

What methods are used to evaluate the effectiveness of CSF controls?

Does CSF Assurance take a compliance-based approach to information protection?

Does a CSF Assurance assessment weight all controls equally?

Can assessors use sampling to improve the efficiency of the assessment?
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is the HITRUST CSF Assurance Program a one-size-fits-all approach?</td>
<td>21</td>
</tr>
<tr>
<td>Are HITRUST assessments only useful for formal certification against the CSF?</td>
<td>21</td>
</tr>
<tr>
<td>Does the CSF Assurance Program support an “assess once, report many” approach?</td>
<td>22</td>
</tr>
<tr>
<td>How can I use the CSF Assurance Program for third-party risk management?</td>
<td>23</td>
</tr>
<tr>
<td>How often do I need to get a HITRUST CSF assessment report to support my third-party assurance requirements?</td>
<td>23</td>
</tr>
<tr>
<td>Since ISO/IEC provides an internationally recognized information security standard, can I use my ISO 27001 certification to satisfy customer and business partner requirements for a HITRUST CSF Validated or Certified Report?</td>
<td>24</td>
</tr>
<tr>
<td>How can my organization utilize the HITRUST CSF framework for an AICPA SOC 2 report?</td>
<td>24</td>
</tr>
<tr>
<td>SECURETexas Covered Entity Privacy and Security Certification</td>
<td>25</td>
</tr>
<tr>
<td>What exactly is the SECURETexas certification?</td>
<td>25</td>
</tr>
<tr>
<td>Why did Texas provide a vehicle for certification when the federal government does not?</td>
<td>25</td>
</tr>
<tr>
<td>What is the relationship between the Texas Health Services Authority (THSA) and the Health Information Trust Alliance (HITRUST)?</td>
<td>25</td>
</tr>
<tr>
<td>Does the SECURETexas certification measure compliance with HIPAA?</td>
<td>25</td>
</tr>
<tr>
<td>Also, will obtaining the SECURETexas certification help with an OCR audit?</td>
<td>25</td>
</tr>
<tr>
<td>Since the SECURETexas certification is voluntary, what are the benefits of obtaining certification?</td>
<td>26</td>
</tr>
<tr>
<td>Do you expect small organizations to seek certification?</td>
<td>26</td>
</tr>
<tr>
<td>The HITRUST RMF</td>
<td>26</td>
</tr>
<tr>
<td>Can risk be calculated based on a control’s maturity level?</td>
<td>26</td>
</tr>
<tr>
<td>Do non-contextual impact ratings for controls provide any real value?</td>
<td>27</td>
</tr>
<tr>
<td>How does the RMF fit into the NIST Framework for Critical Infrastructure Cybersecurity?</td>
<td>28</td>
</tr>
<tr>
<td>Why can’t I just adopt the NIST CsF without leveraging additional guidance or frameworks?</td>
<td>29</td>
</tr>
<tr>
<td>Will HITRUST incorporate the NIST Cybersecurity Practice Guides into the HITRUST RMF?</td>
<td>31</td>
</tr>
</tbody>
</table>
The HITRUST CSF

Why does healthcare need a security framework?

For better or worse, the HIPAA Security Rule (HSR) applies to all covered entities and business associates regardless of their size, location or resources. Fortunately, the federal government recognized there is no “one-size-fits-all” approach to securing sensitive information by writing many, if not most, of the standards and implementation specifications at the objective-level, rather than at the level of prescription necessary for organizations to implement a comprehensive and robust information security program. The HSR also provides organizations a certain latitude or “flexibility of approach” (45 CFR § 164.306(b)) with respect to the determination of the “security measures that allow the [organization] to reasonably and appropriately implement the standards and implementation specifications” based on:

1. The size, complexity and capabilities of the [organization]
2. The [organization’s] technical infrastructure, hardware and software security capabilities
3. The costs of security measures
4. The probability and criticality of potential risks to [ePHI]. (45 CFR § 164.306(b)(2))

Subsequently, the HSR helps ensure organizations develop this necessary level of prescription by requiring a risk evaluation to support the selection of these reasonable and appropriate safeguards that provide for the adequate protection of ePHI.

Covered entities and business associates must “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (45 CFR § 164.308(a)(1)) … [created, received, maintained or transmitted (45 CFR § 164.306(a)(1)) to] … “protect against any reasonably anticipated threats or hazards to the security or integrity of such information” (45 CFR § 164.306(a)(2)).

Unfortunately, risk analysis is not something with which the healthcare industry was intimately familiar. The textbook approach to risk analysis includes threat and vulnerability assessments, information asset valuation and the selection of specific risk treatments for the enumerated threat-vulnerability pairs (a process sometimes referred to as threat modeling). This is all designed to support the selection of cost-effective controls that will manage risk at a level determined acceptable by the organization. From a quantitative viewpoint, this process is virtually impossible for most organizations due to the general lack of actuarial-type data for security-related threats. One could take a semi- or quasi-quantitative approach or even a purely qualitative approach; however, it would still be difficult for an organization—especially one in healthcare—to perform the analysis for a comprehensive set of risk responses.

This level of difficulty is borne out by Department of Health and Human Services (HHS) Office of Civil Rights (OCR) HIPAA security and privacy audits, which have shown that many healthcare organizations have not conducted a valid risk analysis, assuming one was even performed.
An alternative approach is to rely on a control framework developed by an organization that does have the resources needed to conduct such a risk analysis. From this, an organization may establish one or more sets of security safeguards, also referred to as control baselines, which are intended to address similar threats to common classes of information using similar technologies. This happens to also be the approach used by the federal government for its own information system security certification and authorization process. Organizations can then easily select an appropriate control baseline to help “protect against any reasonably anticipated threats or hazards to the security or integrity of [protected health] information” (45 CFR § 164.306(a)(2).

For more information on the history behind HITRUST and creation of the CSF, refer to the HITRUST Key Programs and Services guide.

For more information on risk analysis and tailoring, refer to the Risk Analysis Guide for HITRUST Organizations and Assessors and the HITRUST – University of Fairfax webinar presentation on risk analysis Leveraging Control-based Risk Management Frameworks to Support a HIPAA Compliant Risk Analysis.

**What were the industry’s goals for the CSF?**

Through HITRUST, the healthcare industry sought to create a control framework that was:

- Built specifically for the unique needs of healthcare
- Relevant through regular maintenance of supporting authoritative sources and changes in the threat environment
- Scalable to various sizes and types of organizations or systems in a controlled manner
- Tailorable through managed approvals of alternative (compensating) controls
- Based on compliance with control baselines intended to manage risk to an industry accepted level
- Capable of providing certifiable risk assurances to internal and external stakeholders, including regulators
- Supported by appropriate guidance and tools

For more information on HITRUST and the CSF, refer to the HITRUST Key Programs and Services guide.

**How is the CSF structured?**

HITRUST recognized the global nature of healthcare and the need to gain assurances around the protection of covered information from non-U.S. business associates, which led to the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001:2005, Information technology – Security techniques – Information security management systems – Requirements, being used as the foundation upon which the CSF controls were built. ISO/IEC 27001:2005, provides an international standard for the implementation and maintenance of an information security management system (ISMS) with high-level controls designed to suit almost any organization, in any industry and in any country.
HITRUST then incorporated much of the high-level baseline (later reduced to moderate) from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 2, Recommended Security Controls for Federal Information Systems into the CSF. Although NIST controls were designed specifically for U.S. government agencies, both ISO/IEC 27001 and NIST SP 800-53 provide information security controls that are applicable to a broad scope of environments and organizations. ISO/IEC 27002:2005, Information technology – Security techniques – Code of practice for information security management, was also used to provide additional prescription. And while neither addresses the specific needs of any single industry, both ISO and NIST discuss the application of their frameworks in a healthcare setting in separate documents: ISO/IEC 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002, and NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, respectively. Elements of ISO/IEC 27799 were incorporated into the original CSF published in 2009 and NIST SP 800-66 helped guide subsequent revisions. Additional sources considered relevant to healthcare, such as HIPAA and the Payment Card Industry Digital Security Standard (PCI-DSS) were also integrated into the 2009 framework.

A detailed set of risk factors were then developed to support scaling and tailoring of the CSF to different types and sizes of organizations, system and data-related exposures, and regulatory obligations. The intent was to help HITRUST determine relative risks and capabilities so that organizations could be assigned an appropriate control baseline.

The actual baselines were created by (1) dividing the consolidated requirements amongst up to three levels per control, with references to the authoritative sources provided for each level, and (2) assigning criteria for one or more of the three risk factors (organizational, system and regulatory) at each level. Organizations could then be assigned a scaled and tailored set of controls based on their individual risk factors as scoped to their particular needs, e.g., generally across their organization in support of an enterprise risk management program or targeted to specific business units, systems or regulatory requirements.

The CSF is structured along the lines of ISO 27001:2005 with the 11 control clauses (or categories) but adds an additional control category to address implementation of an Information Security Management Program, similar to that of the ISMS of ISO 27001:2005, and another category to address risk management in particular. HITRUST also added a 14th control category to address specific privacy practices, such as HIPAA and NIST, that are otherwise not addressed in the previous 13 categories.

- **Control Categories**: Topical information protection areas
- **Control Objectives**: States the desired result or purpose of what is to be achieved
- **Control Specifications**: The policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature to meet the Control Objective
• **Control Implementation Requirements**: Detailed information to support the implementation of the control and meeting the Control Objective. Multiple levels (1, 2, and 3) of Implementation Requirements may be defined depending on an organization's or system's environment and risks, which is the set of minimum-security controls defined for an information system. Any additional, but related, functionality to a Level 1 control, and/or increase in the strength of a Level 1 control is placed in Level 2; and any additional, but related, functionality to a Level 2 control and/or increase in the strength of a Level 2 control is placed in Level 3.

• **Standard Mapping**: The cross-reference between each Implementation Requirement level and the requirements and controls of other common standards and regulations

There are 135 control specifications with associated implementation requirements (referred to simply as "controls") that cover security and some privacy-related requirements and 14 controls that cover specific privacy practices in the CSF. Of the 135 controls focused on security, 66 are required for HITRUST CSF Certification as of the 2016 CSF v8 release.

For more information, refer to the *Introduction to the HITRUST CSF* brochure.

**Is the CSF an industry standard for healthcare?**

The CSF is not a standard in the same sense as ISO/IEC 27001:2013 and other, similar security standards given the CSF is a derivative work based on such standards. However, the CSF provides a consensus-driven standard of due care and due diligence for the protection of electronic protected health information (ePHI) in the healthcare industry.

For more information, refer to *HITRUST Key Programs and Services* guide and the joint HCSC and Children's Health analysis of risk management frameworks *Selecting a Healthcare Information Security Risk Management Framework in a Cyber World*.

**Is the CSF a compliance-based or risk-based framework?**

The CSF is a risk-based framework. 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). Regardless of the method used, an organization must implement all the selected controls to manage risk at a level deemed acceptable by its leadership. Failure to fully implement all the specified controls necessarily results in excessive residual risk, which then implies that an organization would take a compliance-oriented approach to implementing and maintaining the selected controls, which were of course selected based on an analysis of risk.

For more information, refer to the *Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection* brochure.
Does the CSF take a “one-size-fits-all” approach to information security?

The CSF is actually one of the most flexible information protection frameworks ever developed. First, the CSF was created by integrating multiple legislative, regulatory and leading practice guidelines and frameworks and tailoring the integrated requirements specifically for the healthcare industry. The resulting controls are then tailored further by selecting them based on specific organizational, system and regulatory risk factors. But while this approach provides more granular tailoring ‘out of the box’ than any other framework, HITRUST understands that no two organizations—even (quote) similar ones—are exactly alike.

Although information may have a common classification (e.g., ePHI), differences such as organizational culture, infrastructure, technology and risk appetite could result in a slightly different set of controls, had the organizations conducted a textbook risk analysis and designed its controls from the beginning. Subsequently, organizations leveraging a framework are expected (1) to perform a risk analysis on threats it considers unique to it and (2) select additional controls to address those threats. Organizations must also consider options for controls that may not be suitable for it to implement (e.g., based on constraints placed by existing or planned information architectures and infrastructure). Fortunately, this supplemental risk analysis addresses fewer threats and other issues considered unique to the organization and is subsequently more tractable. The end result is something NIST SP 800-53 r4 refers to as an overlay, which is a formally documented set of justified modifications to a control baseline.

For more information, refer to the Risk Analysis Guide for HITRUST Organizations and Assessors.

Is the scope of the CSF too large for most healthcare organizations?

Although HITRUST specifically provides for significant tailoring of the CSF based on an organization's specific risk factors, any framework can be applied inappropriately. An organization should not apply the CSF broadly unless it is scoped and tailored to the specific types of information, systems and/or business and clinical units requiring protection. However, given the relatively uncontrolled sprawl of ePHI in many healthcare organizations, the CSF can—and should—be applied as broadly since HIPAA security requirements must be addressed anywhere ePHI is “created, received, maintained or transmitted” (45 CFR § 164.306(a)(1)). Even so, an organization can scope the CSF more narrowly in much the same way as the PCI-DSS by limiting the sprawl of the information requiring protection. This can be done by ensuring that work flows requiring the use of ePHI are understood and uses are restricted to the minimum necessary, as required under HIPAA. Information assets and data flows with ePHI can also be isolated from other asset and data flow types, e.g., through network segmentation.

For more information, refer to the CSF Assessment Methodology and the Risk Analysis Guide for HITRUST Organizations and Assessors.
Why choose the CSF over other control frameworks like NIST SP 800-53 and ISO/IEC 27001?

Many of the elements for the argument are presented in FAQs throughout this section. But more specifically, the HITRUST CSF is specific to the healthcare industry, built and maintained by the healthcare industry, and simply better for the healthcare industry. Many of the reasons for choosing the CSF are presented in the following table:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>CSF</th>
<th>COBIT</th>
<th>PCI DSS</th>
<th>ISO</th>
<th>NIST</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive coverage</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
</tr>
<tr>
<td>Harmonizes relevant business and compliance requirements</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Prescriptive controls</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Practical and scalable controls</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Risk-based rather than compliance-based</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial</td>
</tr>
<tr>
<td>Supported and maintained by a third party</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Vetted by healthcare and industry experts</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes**</td>
<td>Yes**</td>
<td>No</td>
</tr>
<tr>
<td>Open and transparent update process</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Detailed audit or assessment guidance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Consistency and accuracy in evaluation</td>
<td>Yes</td>
<td>Partial</td>
<td>Partial</td>
<td>Partial</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Certifiable for implementing organizations</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial*</td>
<td>No</td>
</tr>
<tr>
<td>Assess once and report many</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Partial***</td>
<td>Partial***</td>
<td>No</td>
</tr>
<tr>
<td>Support for third-party assurance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Partial*</td>
<td>No</td>
</tr>
</tbody>
</table>

*NIST controls are typically certified by a specific information system or type of system rather than at the organizational-level

** ISO 27799 and NIST SP 800-66 both subject to comment period prior to release

*** ISO and NIST are considered “benchmark” frameworks by which many other frameworks are measured and often mapped

For more information on why one would choose the CSF, refer to the Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53 brochure or, for a healthcare organization’s perspective, a joint presentation by HCSC and Children’s Health Selecting a Healthcare Information Security Risk Management Framework in a Cyber World.

How many organizations have adopted the CSF? Do you have a breakdown by type, size, location, etc.?

The HITRUST CSF is the most widely adopted security framework in the healthcare industry: 83 percent of hospitals and 82 percent of health plans with over 500,000 members have adopted the framework. HITRUST can provide detailed benchmarking data by request. If you have further adoption questions relating to your organization, please contact sales@hitrustalliance.net or call 855-HITRUST.

For additional information, refer to HITRUST Key Programs and Services.
Has the CSF been adopted internationally?
Yes, organizations outside of the U.S.—typically business associates providing services to U.S. healthcare organizations—have implemented the CSF. However, other countries have expressed an interest in HITRUST in the past, and we expect this interest to grow as adoption continues to increase within the U.S.

For more information, refer to Understanding and Leveraging the CSF Webpage.

The CSF Assurance Program and Certification

What is the HITRUST CSF Assurance Program?
Designed to meet the unique regulatory and business needs of the healthcare industry, the HITRUST CSF Assurance Program provides 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. The Program also provides additional assurances around the accuracy, consistency and repeatability of assessments due to the use of pre-qualified professional services firms; a risk-based approach to selecting HITRUST CSF controls for assessment, including management oversight of the assessment; and simplified compliance assessment and reporting that addresses multiple federal, state and industry requirements for both covered entities and their business associates.

For more information, refer to the HITRUST CSF Assurance Program Webpage and the HITRUST CSF Assurance Program Requirements brochure.

What types of assessments are available in the HITRUST CSF Assurance Program?
HITRUST offers two types of CSF Assessments – a self-assessment and a validated assessment.

- **Self-assessments** allow organizations to assess themselves using HITRUST’s standard methodology, requirements, and tools provided under the CSF Assurance Program. HITRUST performs limited validation on the results of the self-assessment to provide a limited level of assurance to relying entities.

- **Validated assessments** are conducted by a HITRUST Approved CSF Assessor. The CSF Assurance Program’s assessment methodology is used and the controls are scored using HITRUST’s maturity approach to control implementation. Assessments meeting or exceeding the current CSF Assurance Program requirements receive a HITRUST validated report indicating they are HITRUST CSF Certified.

For more information, refer to the HITRUST Webpage Which Assessment is Right for Me? and the CSF Assurance Program Requirements brochure.
What is the process for an organization to achieve HITRUST CSF Certification?

Before starting the certification process, HITRUST recommends a self-assessment or readiness assessment be performed to prepare organizations for the validated assessment. To begin the certification process, please select a HITRUST Assessor. Once you select an Assessor, you will need to purchase a validated assessment from HITRUST. Complete the validated assessment using the MyCSF tool and then the Assessor will perform the validation/audit work. Please note access to the MyCSF is granted for 90 days. Once the Assessor’s work is complete, it submits to HITRUST for review. HITRUST will create a report and, depending on the scores in the report, will issue a letter of certification.

Note: HITRUST strongly recommends organizations conduct readiness assessments against all 135 CSF controls (149 if the CSF is used to support the organization’s privacy program), rather than only those controls required for certification. This will help ensure both the approved HITRUST CSF Assessor and the assessed organization are always aware of the status of the information protection program and can readily support a CSF controls assessment, regardless of type (e.g., a security assessment used for certification or a comprehensive security assessment used to generate a regulatory scorecard).

For more information, refer to the HITRUST CSF Assurance Program Requirements brochure.

Is a HITRUST CSF validated assessment more expensive than comparable assessments?

No, and this is a common misconception. In many cases the overall assessment costs associated with information security and privacy assessments conducted under the HITRUST CSF Assurance Program are less than other third-party assessments. The alignment between the HITRUST CSF and CSF Assurance programs allows a single CSF assessment report to support multiple objectives, such as a HIPAA risk assessment, an assessment against the NIST Cybersecurity Framework, and AICPA SOC 2® reports. In addition, the same report can be accepted by multiple external parties (such as business partners, government agencies), thereby reducing the costs in comparison with the multiple assessments organizations must normally support.

For a fair comparison of costs, one should consider various factors such as:

- **Scope of the assessment:** Are both assessments reviewing the same scope?
- **Applicability of the control requirements to the environment:** Are the controls requirements applicable to the organization or scope of assessment? Are they prescriptive and do they take into account relevant risk factors?
- **Ability to audit:** Does the framework have audit procedures to ensure consistency of assessment?
- **Level of assurance:** How well does the assessment and evaluation process ensure the control requirements are fully implemented?
- **Caliber of organization performing assessment:** Is the assessment being performed by a third party? What are the qualifications of the firm performing the assessment?

For more information, refer to the HITRUST CSF Assurance Program Overview and HITRUST CSF Assurance Program Requirements documents.
How many organizations have completed a HITRUST CSF assessment?

38,000 CSF Assessments have been performed in the last three years with 15,000 CSF Assessments in 2015 alone. HITRUST anticipates a continued demand for CSF Certification due to third-party assurance requirements from several major health organizations, the SECURETexas program and requests for combined CSF-SOC 2 reports.

For more information, refer to the HITRUST Key Programs and Services overview.

If I’m HITRUST CSF Certified, does that mean I’m HIPAA-compliant?

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. In practice, organizations that want to demonstrate HIPAA compliance must generally show that they have addressed each standard and implementation specification in the Security Rule, including risk analysis.

Unfortunately, the HIPAA Security Rule’s numerous standards and implementation specifications for administrative, technical and physical safeguards, despite what the terms imply, lack the prescription necessary for actual implementation by a healthcare organization. However, this approach was necessary as no two healthcare organizations are exactly alike, which means no single set of information protection requirements could possibly apply across the entire industry. In other words, one size truly does not fit all.

Regardless, this lack of prescription, along with a general lack of guidance from HHS on how organizations should interpret “reasonable and appropriate safeguards” and “adequate protection” resulted in wildly varying information protection programs amongst healthcare entities, including those of similar size and scope. Yet all these organizations likely believed they were “HIPAA compliant” because they had done something around each of the HIPAA standards and implementation specifications. By checking the box against the general requirements in the Rule’s implementation specifications, organizations subsequently checked the box—albeit inappropriately—for the risk analysis without actually conducting one.

OCR has publicly stated that it would not accept an assessment based on the original OCR Audit Protocol, which addressed each of the Security Rule’s standards and implementation specifications, as a valid risk assessment as required under the Rule. Further, an analysis of NIST SP 800-66 indicates that the Security Rule’s standards and implementation specifications do not map to many of the controls specified in NIST SP 800-53 for the low-level control baseline, which indicates that HIPAA itself does not address all reasonably anticipated threats as required by the Rule.

The position that simply focusing on the HIPAA standards and implementation specifications will not yield a valid risk analysis also appears to be supported by HHS, which states in their Guidance on Risk Analysis Requirements under the HIPAA Security Rule that “Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule.” Implementing the standards and specifications will not ensure compliance with the risk analysis requirement; but a risk analysis will help ensure compliance with the standards and implementation specifications.
Subsequently, we address the risk analysis requirement in a separate FAQ and compliance with the remaining requirements here.

To fully address the Rule's standards and specifications, organizations must design or select multiple information security controls to provide the level of prescription necessary for implementation in the system or within the organization. For example, HIPAA § 164.312(a)(2)(iii) states organizations should “implement electronic procedures that terminate an electronic session after a pre-determined time of inactivity.” It’s left to the organization to decide how much time must lapse before terminating the session. But what's appropriate? Five minutes? Ten? Thirty? Another example is HIPAA § 164.312(b), which requires organizations to “implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.” What types of mechanisms are appropriate? What type of activity should be logged? Who should have access to the logs? How long are the logs retained? An organization must ask and answer these types of questions thoroughly for each standard and implementation specification if they are to adequately address the threats for which these safeguards were designed.

The HITRUST CSF helps healthcare organizations address these questions by providing an extensive mapping of the CSF controls to the HIPAA Security Rule’s standards and implementation specifications, many of which are mapped to multiple controls. And the CSF controls themselves consist of multiple, specific requirements contained in multiple levels. By implementing the HITRUST CSF control requirements that are applicable to an organization based on its specific organizational, system and regulatory risk factors, each and every standard and implementation specification in the Security Rule is addressed in a very complete and robust way.

To provide the most complete assurances that the HIPAA Security Rule’s standards and implementation specifications have been addressed, organizations may conduct a comprehensive assessment of all their applicable CSF requirements in MyCSF, HITRUST’s online, GRC-based assessment tool. However, organizations may also use a baseline assessment used for CSF Certification as part of the HITRUST CSF Assurance Program to provide reasonable assurances the organization has satisfied the Rule’s requirements. This is because the assessment addresses 65 high-risk controls (out of a total of 135 for security) that map to each and every standard and implementation specification in the Rule.

In addition, the HITRUST CSF and CSF Assurance Program are used as the basis for SECURETexas, the first state program of its kind in the country offering privacy and security certification for compliance with state and federal laws that govern the use of PHI, including the HIPAA Security, Data Breach Notification and Privacy Rules. Managed by the Texas Health Services Authority (THSA) in conjunction with HITRUST, the program offers individuals and entities involved in the use of PHI an affordable and officially sanctioned process to ensure they have recognized protections in place. SECURETexas certified organizations also receive “limited safe harbor,” as Texas regulators and courts are directed by law to consider past and current certification under the program as mitigating factors when assessing fines and other penalties in the event of a data breach.

For more information on the use of targeted assessments like the baseline assessment for CSF Certification, refer to the FAQ on risk analysis. For additional information on risk vs. compliance-based assessments, refer to the guide to
Understanding HITRUST’s Approach to Risk vs. Compliance-based Information Protection. A complete mapping of the HITRUST CSF to the HIPAA Security, Data Breach and Privacy Rules can be found in a spreadsheet provided in HITRUST’s downloadable CSF package via the License Agreement landing page. More information on SECURETexas can be found on THSA’s SECURETexas Website.

How does a CSF assessment meet the HIPAA requirement for a risk analysis and can it be used to support an OCR audit?

HITRUST bases its framework on how risk management is defined, i.e., the process of managing risk to organizational operations, organizational assets or individuals resulting from the operation of an information system (the definition of which is quite broad), and includes (1) the conduct of a risk assessment, the implementation of a risk mitigation strategy, and employment of techniques and procedures for the continuous monitoring of the security state of the information system.

The conduct of a risk assessment and the implementation of a risk mitigation strategy (through the application of security controls) is generally the focus of OCR audits. Note the terms risk assessment and risk analysis are considered synonymous by the U.S. government, so the risk assessment is for all intents and purposes the risk analysis required under the HIPAA Security Rule.

HHS describes the risk analysis process as follows:

- Scope the assessment to include all ePHI
- Identify & document all assets with ePHI
- Identify & document all reasonably anticipated threats to ePHI
- Assess all current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of a threat occurrence
- Determine the level of risk
- Document assigned risk levels and corrective actions

Using this process would require the complete enumeration of threat-vulnerability pairs and the design of controls to address these pairs, an exercise that is typically beyond the capability of many organizations, especially in the private sector. In fact, the U.S. government doesn’t use this approach either.

Instead, federal civilian agencies rely on the application of a control-based risk management framework developed by NIST, the controls for which are specified for three different levels of sensitivity and criticality of information: low, moderate and high. The assumption is that NIST has performed the underlying threat and vulnerability assessments necessary to support a “standard” risk analysis for these common types of information for common types of threats against a common type of organization (in this case, a federal agency).
Consistent with the flexibility of approach provided under 45 CFR § 164.306(b), HITRUST leverages the same type of approach in the HITRUST CSF the federal government uses. By using the international security standard, ISO 27001, as the basis of the CSF control structure and incorporating relevant regulations, standards and leading practices such as HIPAA, ISO 27002, and NIST SP 800-53, respectively, and some state-level requirements, the CSF provides a comprehensive set of harmonized controls relevant to the healthcare industry. With the assistance of the healthcare industry, these requirements were further refined and separated into three levels of implementation and specific categories for special types of organizations or information (e.g., CMS contractors or FTI custodians). Their selection is then dependent upon specific organizational, system and regulatory risk factors, which results in multiple control overlays as defined by NIST, and the overlay becomes the initial control baseline for that organization.

HITRUST modified the HHS risk analysis process to accommodate this control framework-based approach as follows:

- Conduct a complete inventory of where health information ‘lives’
- Perform an impact analysis on all systems with health information (criticality)
- Categorize & valuate systems based on sensitivity & criticality
- Select an appropriate framework baseline set of controls
- Apply an overlay and/or tailor based on a targeted risk analysis
- Evaluate residual risk using control maturity & impact ratings
- Rank risks and determine risk treatments
- Make contextual adjustments to likelihood & impact, if needed, as part of the corrective action planning process

HITRUST also encourages organizations to further tailor their control selection (their overlay) based on risks unique to the organization with respect to the criteria for the selected baseline, identify gaps in the protections specified and risks managed by the baseline controls, and then select or design additional controls or enhancements as needed.

It’s important to note that what has been discussed here is relevant to the risk analysis required by HIPAA and of course the implementation of an organization’s entire information protection program. However, this is not the same as the baseline assessment used by HITRUST for the purposes of certification and the sharing of assurances with third parties. NIST allows for targeted assessments to address specific questions an organization may have, which in the case of HIPAA compliance would mean assessing the CSF requirements that map the Security Rule’s standards and implementation specifications.

However, HITRUST’s goal—and the goal of many, if not most—healthcare organizations is to achieve the best trade-off between the costs incurred in examining all the controls that support the Security Rule requirements and the level of assurance around the state of compliance that the assessment provides. Obviously assessing all the controls in the CSF would provide the highest level of assurance but cost the most, and assessing none of the controls would cost the least but provide no assurance. HITRUST’s subset of controls required for CSF Certification provide a “sweet spot”
between cost and assurance by addressing each and every one of the Rule’s requirements, including the requirement
for risk analysis through the use of the HITRUST risk management framework to help specify an organization’s target
profile based on their organizational, system and regulatory risk factors.

DHHS specifically references HITRUST and the CSF with respect to risk management and risk assessment in its
*Guidance on Risk Analysis Requirements under the HIPAA Security Rule*. And although OCR does not endorse “any
particular credentialing or accreditation program,” an OCR spokesperson stated the following:

> We certainly encourage covered entities and business associates to build strong compliance programs internally.
> Many of these credentialing/accreditation programs can help them do so. OCR considers mitigation and
> aggravating factors when determining the amount of a civil monetary penalty, and these include the entity’s
> history of prior compliance. An entity with a strong compliance program in place, with the help of a credentialing/
> accreditation program or on its own, would have that taken into account when determining past compliance.

Implementation of the CSF as the basis for an organization’s information protection program and subsequent use
of HITRUST CSF Validated or Certified Assessments has also been accepted by OCR as evidence of their compliance
with the HIPAA Security Rule, assuming the assessment addresses the appropriate scope relevant to OCR’s audit or
investigation. The HITRUST CSF and CSF Assurance Program have also been used in resolution agreements with OCR.

For more information on risk analysis, refer to the *Risk Analysis Guide for HITRUST Organizations and Assessors*.
A complete mapping of the HITRUST CSF to the HIPAA Security, Data Breach and Privacy Rules can be found in a
spreadsheet provided in HITRUST’s downloadable CSF package via the *License Agreement* landing page. The article
from which the OCR spokesperson was quoted can be found on the *Healthcare Information Security* Website.

**Do HITRUST Certification programs provide safe harbor in the event of a breach?**

Certification is not required by any regulatory body, nor has any regulatory body sanctioned certification as a
mechanism to provide safe harbor in the event of a breach. This is true not just for the HITRUST CSF but for other
standards and frameworks as they apply to regulatory compliance requirements (e.g., NIST, ISO, and PCI). However,
OCR recently stated that credentialing/accreditation programs like the CSF can help organizations build strong
compliance programs. “OCR considers mitigation and aggravating factors when determining the amount of a civil
monetary penalty, and these include the entity’s history of prior compliance. An entity with a strong compliance
program in place, with the help of a credentialing/accreditation program or on its own, would have that taken into
account when determining past compliance.”

Certification is one of the best ways regulators have to determine if an organization has made a good faith effort to
meet their legal and regulatory requirements (i.e., provide a mitigating factor when considering financial penalties or
other punitive or corrective actions). A HITRUST Certification can convey to third parties (e.g., regulators, auditors,
business partners, customers) in a standard, structured and clear way that controls are in place, to what level they
are applied, and how they were chosen, including any risk management decisions for risk acceptance or the use of
alternate (i.e., compensating) controls.

© 2016 HITRUST Alliance. All rights reserved.
The State of Texas also provides for the consideration of past compliance as a mitigating factor in the event of a data breach through SECURETexas, a covered entity privacy and security certification program, which is based on the HITRUST CSF. Title 2, Texas Health and Safety Code (THSC) § 181.205, specifically allows a covered entity to introduce certification as evidence of its good faith efforts to comply with HIPAA and other federal and state requirements specified in Title 1, Texas Administrative Code (TAC) § 390.2 in an action or proceeding imposing an administrative penalty or assessing a civil penalty related to an unauthorized disclosure. In determining the penalty imposed by other law in accordance with THSC § 181.201, a court or state agency must also consider several factors, including the covered entity’s compliance history and whether the covered entity was certified at the time of the violation.

For more information on risk vs. compliance, refer to the HITRUST whitepaper *Understanding HITRUST’s Approach to Risk vs. Compliance-based Information Protection*.

For more information on the SECURETexas program and its benefits, visit the SECURETexas Website or review the following presentations:

- **Texas Certification**: Review the Program Basics
- **Texas Certification**: Undergo an Onsite or Remote Assessment
- **Texas Certification**: Submit Certification Recommendations to THSA

**Does the use of alternate controls diminish the value of HITRUST Certification?**

Alternate (or compensating) controls, by definition, mitigate a similar type and amount of risk as the control it’s intended to replace. This is illustrated in the *Risk Analysis Guide for HITRUST Organizations and Assessors* by an example proposing the extension of password expiration to one year by increasing the complexity of the password. Part of that analysis is to evaluate the impact on related controls or other unintended consequences, such as the effect of extending password expiration on a key logger vulnerability. Although this is a quantitative example based on entropy calculations, other controls may require a quasi-quantitative or qualitative approach to the risk analysis.

Alternate controls may be developed and implemented by a single organization, or the alternative may be applied broadly across the industry if submitted and approved by the HITRUST Alternate Controls Review Committee. Review by the Committee ensures the control adequately addresses a similar type and amount of risk; however, alternate controls that are not approved must be evaluated by the assessor organization to verify the analysis, which is documented in the HITRUST assessment report. Thus, alternate controls provide organizations additional flexibility in selecting and implementing controls without impacting the organization’s overall risk posture or the value of CSF Certification.

For more information on alternate controls, refer to the *Risk Analysis Guide for HITRUST Organizations and Assessors*. 
Does HITRUST rely too heavily on the Assessor’s opinion of control effectiveness?
Assessors and auditors generally determine control effectiveness regardless of what controls are specified, albeit there is usually a negotiation between the auditor/assessor and the organization before the final report is issued.

However, assessors actually have more leeway in assessing the effectiveness of an organization’s controls—and actually determining what those controls should be—when a framework like the HITRUST CSF is not used. Before an assessor can become a HITRUST-approved CSF Assessor organization, it undergoes a vetting process for their assessment methods and the experience and qualifications of its staff. They are also required to adhere to HITRUST guidelines for CSF assessments, and each validated or certified assessment undergoes a quality review by HITRUST to ensure consistency and repeatability regardless of the CSF Assessor doing the work.

For more information, refer to the CSF Assessor Datasheet.

What methods are used to evaluate the effectiveness of CSF controls?
The HITRUST assessment methodology specifically requires:

- Assessors to gather and examine documentation (e.g., policies, procedures, records, logs, vulnerability assessment reports, risk assessment reports)
- Examine configuration settings, physical surroundings, processes and other observable information protection practices
- Conduct interviews with the business unit stakeholders, where applicable
- Perform system tests to validate the implementation of controls, as applicable

Technical testing by the assessor is encouraged but not always necessary. If not performed, the review of internal and third-party technical testing, e.g., vulnerability scanning and penetration testing, would then be needed if related controls are to receive any credit for implementation.

For more information, refer to the CSF Assessor Datasheet and the CSF Assessor Requirements Brochure.

Does CSF Assurance take a compliance-based approach to information protection?
From its inception, HITRUST chose to use a risk-based rather than compliance-based approach to information protection and help mature the healthcare industry's approach to safeguarding information. By integrating NIST’s moderate-level control baseline into the CSF, which is in-turn built upon the ISO 27001:2005 control framework, HITRUST leverages the comprehensive threat analyses employed by these frameworks to provide a robust set of prescriptive controls relevant to the healthcare environment. The CSF also goes beyond the three baselines for specific classes of information and provides multiple control baselines determined by specific organizational, system and regulatory risk factors. These baselines can be further tailored through formal submission, review and acceptance by HITRUST of alternative controls, what PCI-DSS refers to as compensating controls, to provide healthcare with additional flexibility in the selection of reasonable and appropriate controls while also providing assurance for the adequate protection of PHI.
The risk analysis guidance from HHS can subsequently be modified to support the use of a comprehensive control framework—built upon an analysis of common threats to specific classes of information and common technologies—as follows:

- Conduct a complete inventory of where ePHI lives
- Perform a BIA on all systems with ePHI (criticality)
- Categorize and evaluate these systems based on sensitivity and criticality
- Select an appropriate framework baseline set of controls
- Apply an overlay based on a targeted assessment of threats unique to the organization
- Evaluate residual risk
  - Likelihood based on an assessment of control maturity
  - Impact based on relative (non-contextual) ratings
- Rank risks and determine risk treatments
- Make contextual adjustments to likelihood and impact, if needed, as part of the corrective action planning process

For more information, refer to the *Understanding HITRUST’s Approach to Risk vs. Compliance-based Information Protection* brochure and the *Risk Analysis Guide for HITRUST Organizations and Assessors*.

**Does a HITRUST CSF Assurance assessment weight all controls equally?**

Although all CSF controls placed in scope after the tailoring process must be implemented by the organization to effectively manage excessive residual risk, not all controls are assessed for a HITRUST CSF Validated or Certified Report. This is consistent with NIST guidance that allows for focused assessments to address specific issues or answer specific questions. “Organizations have maximum flexibility on how risk assessments are conducted and are encouraged to apply the guidance in this document so that the various needs of organizations can be addressed and the risk assessment activities can be integrated into broader organizational risk management processes” (NIST SP 800-30 r1, Guide for Conducting Risk Assessments, pg. ix). For purposes of certification, control selection is based on an analysis of breach data, leading practices and regulatory requirements (most notably the HIPAA Security Rule).

With respect to the way an assessment is conducted, one control does not have more weight or importance than another. This is because, by definition, all the controls that the organization has determined it must implement—regardless of whether they were designed from a custom risk analysis or tailored from a control baseline by a supplemental analysis—must be implemented in order to manage risk to an acceptable level. But the HITRUST CSF Assurance Program only requires this level of “completeness” for purposes of certification and, even then, organizations can remove controls that do not apply to them or accept a small amount of risk for partial implementations of those that do.
HITRUST also encourages the prioritization of remediation activities based on relative risk by providing impact ratings and their relationship with each other with the inclusion of priority codes. Although examples have not yet been provided in the Risk Analysis Guide, HITRUST encourages organizations to modify the impact ratings based on an evaluation of their control environment and consider other factors, such as existing infrastructure, budget constraints and organizational culture when developing and prioritizing corrective actions.

For more information, refer to the Understanding HITRUST’s Approach to Risk vs. Compliance-based Information Protection brochure and the Risk Analysis Guide for HITRUST Organizations and Assessors.

Can assessors use sampling to improve the efficiency of the assessment?
Sampling methodologies can be a bit arcane, but sampling is actually very commonly used in the healthcare industry, especially by auditors. HITRUST also provides guidance to CSF Assessor organizations on the use of sampling in the HITRUST CSF Assessment Methodology brochure, and of course anyone can refer to multiple texts on the subject.

For more information, refer to the HITRUST CSF Assessment Methodology brochure.

Is the HITRUST CSF Assurance Program a one-size-fits-all approach?
As we’ve seen, the CSF is not a one-size-fits-all approach due to (1) an organization’s ability to tailor the initial selection of the control baseline in accordance with defined risk factors and (2) the requirement for additional tailoring based on unique threats, their specific environment, and the use of alternate controls. HITRUST simply requires organizations to justify their decisions to eliminate or modify the baseline. The HITRUST CSF Assurance Program is no different. The only impact tailoring may have is the ability to receive a HITRUST Certified Assessment Report as controls must meet certain implementation requirements (scores) for required controls. A HITRUST Validated Assessment Report will provide the same level of assurance for the selected controls, while providing the transparency needed for those controls that were modified or not selected. The HITRUST CSF Assurance Program subsequently provides a common, consistent and repeatable means of assessing all types of organizations and sharing assurances with internal and external stakeholders, including regulators.

For more information, refer to the Understanding HITRUST’s Approach to Risk vs. Compliance-based Information Protection brochure.

Are HITRUST assessments only useful for formal certification against the CSF?
Certification is only one of the ways the HITRUST CSF can be used. Not all organizations need to pursue certification, and validation will provide assurances that specific controls are implemented, which ones are not or may have been changed, and how well they are implemented. If an organization chooses not to implement a specific control requirement or address a requirement at a particular maturity level, this is simply identified in the assessment report. Relying entities can then decide whether or not the controls implemented by the organization meet their needs.
Organizations are free to assess specific controls for other purposes, such as Texas certification, FISMA compliance, or audits of specific risk areas like access control. Other organizations may simply choose to view the CSF as a source of industry leading practices, which they would evaluate and determine whether or not they are appropriate for their organization. Such an organization could still conduct a formal self-assessment or retain a CSF Assessor organization to evaluate the selected controls and receive a validated assessment report.

For more information, refer to the brochure on *Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53* and the *HITRUST CSF Assurance Program Detailed Overview.*

**Does the HITRUST CSF Assurance Program support an “assess once, report many” approach?**

HITRUST has recognized for some time that the current model used in the industry for Third-Party Assurance is fraught with inefficiencies and unnecessary costs by requiring duplicative questionnaires and assessments, which tend to distract organizations from monitoring controls and remediating identified deficiencies. Organizations can streamline the compliance process and reduce costs with a standardized approach to performing assessments and reporting security controls by utilizing the HITRUST CSF Assurance Program. The tools and methodologies organizations utilize to complete assessments as part of the HITRUST CSF Assurance Program are built around the HITRUST CSF and allow organizations to assess and report against multiple sets of requirements. The result allows assessing organizations to undergo one assessment and report to multiple entities, providing the industry with a consistent and effective standard. In fact, several large healthcare entities now require their business associates to provide a HITRUST CSF Validated or Certified Report. For more information, refer to the *HITRUST Third Party Assurance Program FAQ* and the *HITRUST CSF Assurance Program FAQ.*

**How can I use the HITRUST CSF Assurance Program for third-party risk management?**

The HITRUST CSF Assurance Program is specifically designed to streamline the third-party risk management process by using a single comprehensive framework harmonizing multiple standards and leading practices to support a single assessment that may be reported out in multiple ways, e.g., to support PCI SAQ development, the issuance of SOC 2 reports against specific AICPA Trust Services Principles, or scorecards of HIPAA or NIST Cybersecurity Framework compliance. Organizations using the CSF Assurance Program for third-party risk management experience significant reductions in cost and level of effort required to evaluate third-party reports or issue their own reports to their own stakeholders, including business partners and regulators. This is the fundamental reason why several large healthcare entities have moved from simply accepting HITRUST Validated and Certified Reports to requiring them.

For more information on the organizations now requiring HITRUST CSF assessment reports, refer to the *joint news release.* For more information on managing third-party compliance, refer to the *HITRUST Third Party Assurance Program FAQ* and the *HITRUST CSF Assurance Program FAQ.*
How often do I need to get a HITRUST CSF assessment report to support my third-party assurance requirements?

HITRUST CSF Validated Reports with Certification are valid for two years given the successful completion of an interim review (typically 12 months after the original assessment), that no breach and no significant changes have occurred relating to the scoped control environment. However, check with your business partner(s) to ensure this meets their requirements. Validated Reports not resulting in certification are point-in-time reports.

For more information, refer to the HITRUST CSF Assurance Program Detailed Overview.

Since ISO/IEC provides an internationally recognized information security standard, can I use my ISO 27001 certification to satisfy customer and business partner requirements for a HITRUST CSF Validated or Certified Report?

The best discussion of why one would choose the HITRUST CSF over ISO 27001 and NIST SP 800-53 is provided in an earlier FAQ, but to address the question about accepting one in lieu of another, we’ll need to expand a little further.

The biggest difference between the two certifications is what they intend to certify.

In the case of ISO 27001, the focus of the certification is on the information security management system (ISMS), which includes an evaluation of the information security risk assessment and treatment processes. However, “organizations can design controls as required, or identify them from any source” (ISO 27001, § 6.1.3.b, p. 4). Further, although ISO 27001 Annex A contains a list of control objectives and controls, they are not exhaustive and additional control objectives and controls may be needed” (Ibid., § 6.1.3.c, p. 4). And although the ISO assessor must produce a “Statement of Applicability that contains the necessary controls (see 6.1.3 b and c) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A” (Ibid., § 6.1.3.d, p. 4), it doesn’t extend beyond what’s required in Annex A. Subsequently, organizations have wide latitude in the controls they specify to address the risks they identify at a level suitable to their risk appetite. ISO certification assessors also have some latitude in how they assess the effectiveness of the controls, and there is no quality control of the assessments other than a general requirement that consultants that help organizations prepare for ISO certification do not perform the certification assessment.

In effect, we’re left with the same problems that existed before the creation and implementation of the HITRUST CSF—which is actually structured on ISO 27001 and contains additional guidance from ISO 27002 and multiple other relevant authoritative sources such as HIPAA, NIST SP 800-53, CMS IS ARS, PCI DSS and the NIST Cybersecurity Framework—and its assessment through the HITRUST CSF Assurance Program: a lack of comprehensiveness and prescription in the control requirements; little or no U.S. healthcare industry context; lack of comprehensiveness related to regulations, legislation and other relevant requirements such as leading practice frameworks; and uncertain rigor and approach to the assessments including limited quality control.
The HITRUST CSF on the other hand provides a minimal baseline of comprehensive, prescriptive control requirements tailored to a healthcare organization’s specific organizational, system and regulatory risk factors. And the specific focus of HITRUST Certification is on the maturity of this control baseline’s implementation using a specific, rigorous assessment approach and scoring model in order to gauge the level of excessive residual risk to ePHI in the organization. HITRUST also provides detailed assessment procedures for each control requirement, and ensures assessments are performed by trained, qualified assessor organizations and requires each assessment undergo a quality assurance review to ensure accuracy and completeness before awarding certification.

As an example of how high-level control requirements can benefit from the context, comprehensiveness and rigor of the HITRUST CSF and CSF Assurance Program, one only has to look at the ongoing joint initiative between AICPA and HITRUST on using the HITRUST CSF to support SOC 2 assessments against the Trust Principles and Criteria. This ensures a standardized set of healthcare-relevant control requirements are identified for each criterion, and the assessment of these controls are conducted with a specific approach and level of rigor that provides relying entities, including regulators and other third parties, with accurate, consistent and repeatable assurances.

The best treatment on why one would choose the HITRUST CSF over ISO can be found in the risk framework analysis presented by HCSC and Children’s Health Dallas Selecting a Healthcare Information Security Risk Management Framework in a Cyber World. For more information on the HITRUST RMF, refer to the HITRUST RMF Whitepaper.

How can my organization utilize the HITRUST CSF framework for an AICPA SOC 2 report?

HITRUST and AICPA collaborated on the mapping of HITRUST CSF controls to AICPA Trust Principles and Criteria for Security, Confidentiality and Availability. Subsequently, any AICPA firm can perform a SOC 2 examination leveraging the CSF framework. This allows the client to receive in a combined format HITRUST Certification and a SOC 2 report. The next collaborative effort will be mapping the HITRUST CSF to the privacy principle.

For more information, refer to the SOC 2: Leveraging the CSF Webpage, the Deloitte article “SOC 2 for HITRUST – A Complementary Reporting Option” and the HITRUST CSF to AICPA Trust Services Principles and Criteria mapping on the AICPA website.
SECURETexas Covered Entity Privacy and Security Certification

What exactly is the SECURETexas certification?
The certification allows Texas covered entities to show they have met privacy and security standards in order to reduce regulatory penalties, manage risk and increase confidence in how they protect health information. In Texas House Bill 300 (SB 300), as codified in Texas Health and Safety Code Section 182.108(d), the Texas Legislature directed the Texas Health Services Authority (THSA) to establish a process by which a covered entity may apply for certification by the THSA of a covered entity’s past compliance with privacy and security standards ratified by the Texas Health and Human Services Commission (HHSC) for the electronic sharing of protected health information. Those standards can be found at Title 1, Chapter 390, Texas Administrative Code.

Why did Texas provide a vehicle for certification when the federal government does not?
Texas has always gone above and beyond federal law in protecting patients’ health information. Texas strengthened the protections found in HIPAA by creating the Texas Medical Records Privacy Act in 2001, and again strengthened the protections found in the HITECH Act by passing House Bill 300 in 2011. This included creating a robust certification program that could measure a covered entity’s compliance with the myriad of state and federal laws relating to the privacy and security of protected health information. This helps an organization know proactively if it complies with federal regulations and state level medical privacy laws.

What is the relationship between the Texas Health Services Authority (THSA) and the Health Information Trust Alliance (HITRUST)?
The THSA and HITRUST have partnered to help improve the protection of healthcare information for Texas residents. The THSA is leveraging the HITRUST CSF, the most widely-adopted security framework in the U.S. healthcare industry, to form the basis of the SECURETexas: Health Information Privacy & Security Certification Program, as created in accordance with Texas House Bill (HB) 300 passed in 2011. HITRUST was awarded the exclusive contract to provide certification recommendation and related services to the THSA in support of the program but the criteria for certification and the award of certifications under the program are determined by the THSA in conjunction with the Texas Health and Human Services Commission, which codifies the standards in rule.

Does the SECURETexas certification measure compliance with HIPAA? Also, will obtaining the SECURETexas certification help with an OCR audit?
Yes, SECURETexas certification includes compliance with both federal and state laws. Therefore, obtaining the SECURETexas certification will help with an OCR audit by providing the covered entity with a tool to display prior compliance with HIPAA privacy, data breach notification and security rules, thus potentially reducing any civil money penalties under HIPAA in compliance with 45 CFR 160.408(c).
Since the SECURETexas certification is voluntary, what are the benefits of obtaining certification?

Obtaining the THSA’s SECURETexas certification will benefit Texas covered entities in many ways, including better compliance with HIPAA and other federal privacy and security standards, as well as mitigation of civil and administrative penalties for violations of the Texas Medical Records Privacy Act. It will also clearly demonstrate to business partners, healthcare providers, and patients that the covered entity cares about privacy and security.

Do you expect small organizations to seek certification?

Yes, absolutely. The benefits of certification apply to small organizations as well as to larger organizations; small organizations are more likely to need help ensuring that they are aware of, and meeting, all state and federal requirements. THSA, HITRUST and the Texas Medical Association (TMA) are currently piloting the Small Organization Health Information Assurance (SOHIA) Program with small practices in Texas and anticipate making the Program more widely available after it is fully incorporated into the SECURETexas program.

The HITRUST RMF

Can risk be calculated based on a control’s maturity level?

HITRUST evaluates likelihood based on an assessment of the control’s maturity level. To understand the approach, one must understand that a control framework is based on a broad risk analysis that considers threats to similar types of organizations for specific classes of information using common types of technology. Control baselines are then established based on specific factors. In the case of the (now legacy) Department of Defense (DoD) Information Technology Security Certification and Accreditation Program (DITSCAP) control framework, estimates of the information’s confidentiality and criticality requirements resulted in up to nine specific control baselines. The current NIST framework takes a high watermark approach and provides three baselines. HITRUST takes a similar approach based on organizational, system and regulatory risk factors, which can result in dozens of possible baselines.

By implementing an appropriate control baseline that meets the confidentiality, integrity and availability requirements of the information, the organization is then able to manage risk to the organization to an acceptable level. With certain exceptions (such as for payment card information), HITRUST adopts a single security baseline and then tailors the controls to the organization based on organizational, system and regulatory risk factors. This process provides for the flexibility allowed under HIPAA with respect to the determination of the “security measures that allow the [organization] to reasonably and appropriately implement the standards and implementation specifications” (45 CFR § 164.306(b)) based on organizational size, complexity, capabilities, and infrastructure constraints.

Organizations may then simply focus on the implementation and maintenance of the selected controls to manage excessive residual risk. Since it’s intuitively obvious that well-implemented controls are less likely to fail than those that are poorly implemented, the evaluation of the maturity of the control then provides a likelihood estimator.
for the probability (likelihood) that a threat will successfully exploit a vulnerability and potentially compromise the confidentiality, integrity and/or availability of the information protected.

One should note that evaluating a control's implementation is one of the most common methods used to help organizations determine security risk, and the HITRUST approach is very similar to the maturity model described in NIST Interagency Report (NISTIR) 7358, Program Review for Information Security Management Assistance (PRISMA). Subsequently, maturity is a valid method for evaluating the relative effectiveness of a control, which in turn provides an estimate of how likely the control will fail.

- **Policy:** Requirements stated in a policy or standard are understood by the organization. If not stated, there is little guarantee that it will be implemented or continue to be implemented

- **Procedures:** Processes are necessary to ensure the control can be implemented in a repeatable and consistent way. They may be ad hoc, documented or automated

- **Implemented:** Evaluation of the control's implementation across the breadth and depth of the organization is the most common way of assessing a control's effectiveness

- **Measured and Managed:** These last two levels of HITRUST's version of the PRISMA model, which together have the same value as the first three levels when scoring out the control, simply address the concept of continuous monitoring. “One can’t manage what one doesn’t measure.” The idea is to avoid past practices of ‘implementing and forgetting’ a control to monitoring the effectiveness of the control and taking action should problems occur. This level of maturity beyond implementation provides additional assurance the control will not fail

For more information, refer to the *Risk Analysis Guide for HITRUST Organizations and Assessors.*

**Do non-contextual impact ratings for controls provide any real value?**

The term “non-contextual” is used to indicate that the rating does not consider the state of existing controls in a particular organization’s environment. The problem HITRUST is addressing with the non-contextual ratings is that most organizations have significant difficulty with the risk analysis process and do not truly understand the impact a particular control failure may have to the organization. So the impact ratings, which are based on work by the U.S. Department of Defense (DoD) with respect to the impact and severity codes used under the Defense Information Assurance Certification and Authorization Program (DIACAP), are used to provide an indication of the relative impact of the controls in the framework should they fail. The key to understanding this approach is that controls are designed to address one or more threats to the organization, which arguably present(s) a certain amount of additional risk should one or more vulnerabilities be successfully exploited. Since the assets in question are information assets of a specific type, i.e., ePHI and other information with similar confidentiality and criticality requirements, estimates of the impact of a control failure can be legitimately made (again as demonstrated by the DoD). The organization would then adjust the impact ratings for their own use (outside of the MyCSF tool) based on a contextual analysis for those
controls that require some sort of remediation. By limiting the scope of the analysis to a subset of controls in the environment, the analysis becomes more tractable. The Risk Analysis Guide provides the impact ratings along with an example of how an organization can help prioritize corrective actions for control deficiencies using these ratings. The example also includes the use of priority codes derived from NIST SP 800-53 r4, which indicate relative dependence of the controls upon each other.

For more information, refer to the *Risk Analysis Guide for HITRUST Organizations and Assessors*.

**How does the HITRUST RMF fit into the NIST Framework for Critical Infrastructure Cybersecurity?**

The HITRUST RMF, which consists of the HITRUST CSF, CSF Assurance Program and supporting tools, methods and services, is actually a model implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework, or NIST CsF) for the healthcare industry, as discussed in a recent HITRUST presentation to the Department of Homeland Security (DHS) Cross-Sector Cyber Security Working Group (CSCS WG).

The NIST framework is intended to provide guidance to critical infrastructure industries on the development of industry, sector or organization-specific cyber security programs and help ensure a minimum level of consistency and rigor. The HITRUST RMF maps completely to the sub-categories in the NIST framework and is further supported by an implementation maturity model that also maps to the NIST model. However, HITRUST goes beyond the NIST framework recommendations by providing a fully functional cyber threat intelligence and response program to enable the U.S. healthcare industry to protect itself from disruption by these attacks. The HITRUST Cyber Threat Xchange (CTX) is the single best source of intelligence on threats targeted at healthcare organizations and medical devices, providing actionable information for strategic planning and tactical preparedness and coordinated response for both large and small organizations.

HITRUST CTX also facilitates critical intelligence sharing between the healthcare industry, the U.S. Department of Homeland Security (DHS) and the U.S. Department of Health and Human Services (HHS), while supporting monthly threat briefings and C3 alerts. In addition, HITRUST and HSS evaluates the industry’s preparedness and HITRUST CTX effectiveness through industry-wide cyber-attack and response exercises, CyberRX, in which participating organizations examine both broad and segment-specific scenarios targeting information systems, medical devices and other essential technology resources of the healthcare industry.

HITRUST and the Office of the National Coordinator (ONC) Office of the Chief Privacy Officer (OCPO) also co-chair the Risk Management Sub-working Group (RMSG) of the Joint Healthcare and Public Health (HPH) Cybersecurity Working Group (WG), part of the Critical Infrastructure Protection (CIP) Public and Private Partnership. The RMSG is chartered to coordinate the development of (1) a tailored, Sector-wide HPH Cybersecurity Framework Implementation Guide, leveraging existing documents and efforts, and (2) supplemental guides tailored to different levels of users and different types of technology, as needed, which may include but is not limited to small organization implementation and medical device security. The guidance developed by the RMSG for HPH Sector-wide use is based on the HITRUST
RMF, of which the HITRUST CSF and CSF Assurance Program are a part, and is available as a 508-compliant PDF from the US-CERT Cybersecurity Framework Webpage or downloaded directly here.

For more information, refer to the NIST and HITRUST CSF Webinar presentation and the Healthcare Sector Cybersecurity Framework Implementation Guide.

For more information on the CIP initiative, refer to the Websites on CIP Partnerships and Information Sharing, Critical Infrastructure Sector Partnerships, and HPH: Council Charters and Membership.

**Why can’t I just adopt the NIST CsF without leveraging additional guidance or frameworks?**

For an industry sector or organization to implement the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework, or NIST CsF), one must understand that it relies on existing standards, guidance, and leading practices to achieve specific outcomes meant to help organizations manage their cybersecurity risk.

Specifically, the NIST CsF provides a common language and mechanism to:

- Describe their current cybersecurity posture
- Describe their target state for cybersecurity
- Identify and prioritize opportunities for improving the management of risk
- Assess progress toward the target state
- Foster communications among internal and external stakeholders

The NIST CsF is intended to complement rather than replace an organization’s existing business or cybersecurity risk management process and cybersecurity program. Instead, organizations should use their current processes and leverage the framework to identify opportunities to improve their management of cybersecurity risk. Alternatively, an organization without an existing cybersecurity program can use the framework as a reference to establish one. In other words, the NIST CsF provides an overarching set of guidelines to critical infrastructure industries to provide a minimal level of consistency as well as depth, breadth and rigor of industry’s cybersecurity programs.

These overarching guidelines are presented through the NIST CsF Core, which provides the structure upon which a cybersecurity program may be built. The lowest level of the Core, the Subcategories, provides high-level requirements—essentially control objectives—that organizations should strive to implement. However, these Subcategories lack the prescription necessary for an organization to actually implement them, which is why NIST provides examples of controls from other, lower-level and generally more prescriptive frameworks such as ISO/IEC 27001:2013 and NIST SP 800-53 r4.
For example, NIST maps PR-PT-1 for audit/log records to ISO/IEC 27001:2013 A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, and A.12.7.1, and to the entire NIST SP 800-53 r4 AU family. The healthcare industry’s HITRUST CSF is mapped as follows:

<table>
<thead>
<tr>
<th>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</th>
<th>PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>06.c Protection of Organizational Records</td>
<td>06.i Information Systems Audit Controls</td>
</tr>
<tr>
<td>09.aa Audit Logging</td>
<td>09.ab Monitoring System Use</td>
</tr>
<tr>
<td>09.ac Protection of Log Information</td>
<td>09.ad Administrator and Operator Logs</td>
</tr>
<tr>
<td>09.ae Fault Logging</td>
<td>09.af Clock Synchronization</td>
</tr>
<tr>
<td>09.h Capacity Management</td>
<td>10.i Protection of System Test Data</td>
</tr>
<tr>
<td>10.m Control of Technical Vulnerabilities</td>
<td></td>
</tr>
</tbody>
</table>

It's clear multiple requirements that provide additional specificity are required to satisfy the objectives provided by the NIST CsF Subcategories. And for a healthcare entity to select a reasonable and appropriate set of administrative, physical and technical safeguards to provide for the adequate protection of ePHI, it must “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information” it holds, as required by HIPAA § 164.308(a)(ii)(A). To learn more about how the HITRUST risk management framework (RMF) satisfies this requirement, refer to the guide on Understanding HITRUST’s Approach to Risk vs. Compliance-based Information Protection.

As mentioned in a previous FAQ, HITRUST and the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) recognized the need for additional guidance to sector organizations on how to properly implement the NIST CsF and established the development of such guidance as one of four core tasks for the Joint (SCC/GCC) HPH Cybersecurity WG. The result is the Healthcare Sector Cybersecurity Framework Implementation Guide, the 508-compliant version of which is available as one of seven sector-specific guides on the US-CERT Cybersecurity Framework Webpage. For more information on the Critical Infrastructure Protection (CIP) initiative under which the healthcare implementation guidance was developed, refer to the Websites on CIP Partnerships and Information Sharing, Critical Infrastructure Sector Partnerships, and HPH: Council Charters and Membership.

And to understand why the HITRUST RMF, which consists of the HITRUST CSF and CSF Assurance Program and supporting methods and tools, is the most widely used approach in healthcare, refer to the joint presentation by the Health Care Services Corporation and Children’s Health Dallas CIOs, Selecting a Healthcare Information Security Risk Management Framework in a Cyber World.
Will HITRUST incorporate the NIST Cybersecurity Practice Guides into the HITRUST RMF?

HITRUST works closely with NIST and we constantly analyze their documentation to see what additional guidance can be utilized. Many guidelines—most often those that are very technical or technology-specific—are typically outside the scope of the HITRUST CSF; however, HITRUST will review these practice guides, determine how HITRUST CSF adopters can best leverage this type of documentation, and provide supporting guidance to the healthcare community, e.g., through HITRUST Implementation Advisories, as needed.

For more information on the HITRUST approach to risk management, refer to the HITRUST Risk Management Frameworks brochure and Understanding HITRUST’s Approach to Risk vs. Compliance-based Information Protection brochure.