HITRUST®

# Risk Management Frameworks

How HITRUST provides an efficient and effective approach to the selection, implementation, assessment and reporting of information security and privacy controls to manage risk in a healthcare environment

2019

# Contents

# Introduction

Healthcare organizations continue to face a multitude of challenges with regards to information security and privacy. At the forefront of these challenges is the need to apply 'reasonable and appropriate' safeguards to provide 'adequate' protection of sensitive information to demonstrate compliance with a growing number of continuously evolving federal, state and industry requirements. However, given the general lack of definition and prescriptiveness of these requirements, organizations are left with the task of deciding what actions would be considered 'reasonable and appropriate' and what level of protection would be 'adequate' in the eyes of federal, state and industry regulators, business partners, patients and their families, and other interested third-parties.


**Figure 1**

This complex challenge is the basis for why the healthcare industry came together and formed HITRUST. HITRUST did the 'heavy lifting' by integrating multiple international, federal, state and industry legislation, regulations, standards, and best practice frameworks; adapted them to the healthcare environment in particular; and determined an industry standard of due diligence and due care that can be tailored to an individual organization based upon its specific business requirements. The result of these efforts is the HITRUST CSF, an industry-wide framework of security and privacy controls that is based on, and cross-referenced with, existing requirements. In addition, the HITRUST CSF Assurance Program provides organizations with a single approach for conducting an assessment and reporting against these multiple requirements. Both the HITRUST CSF and CSF Assurance Program are updated at least annually to account for changes in legislation, regulations, standards, guidance and best practices, such as with the 2014 release of the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*, more commonly known as the NIST Cybersecurity Framework (CsF). Further, all changes to the HITRUST

CSF are provided to the industry for review and comment, ensuring transparency and openness. HITRUST provides the CSF free to qualified organizations that wish to implement the framework.

So, why does the HITRUST CSF increase in value as new/updated requirements or guidance are released? Because the more complex the security and regulatory landscape becomes, the more difficult it is for organizations to maintain compliance, protect information, and protect themselves against breaches. HITRUST established a flexible control structure from its inception and continuously adds and updates the framework in response to changing legislation, regulations, standards and guidance.

Part of the process is to analyze each new source and map its requirements to the control structure, which can also be performed with the assistance of a cross-industry working group. In addition, the HITRUST CSF was structured in such a way that allows additional tailoring based on risk factors such as organizational type or a specific system characteristic. HITRUST also continues to develop and publish guidance and tools like the HITRUST CSF assessment methodology and MyCSF as part of an overall risk management framework (RMF), which is essentially a common taxonomy and standard set of processes, procedures, activities and tools that support the identification, assessment, response, control and reporting of risk. This provides organizations with one set of requirements irrespective of new or updated regulations, guidance or best practices, and one compliance approach to implement and manage 'reasonable and appropriate' safeguards that demonstrate the level of due care and due diligence required to ensure 'adequate' protection of the information with which they are entrusted.

What would organizations need to do without HITRUST and the CSF? The alternative is to continually review changes to legislation, regulations, guidance and standards to determine the requirements that are appropriate based on each organization's risk profile, identify industry best practices to address the requirements, and develop an approach to assess its compliance against these requirements. Because each organization would be working independently, each interpretation and implementation of the requirements would be unique if not proprietary, impeding the ability to form trusted, third-party business relationships and the healthcare industry's progress in the digital age.

This paper describes:

- How organizations struggle with the constantly changing security and regulatory landscape,
- How the most efficient and effective way to deal with these changes is by adoption of an appropriate RMF,
- The NIST and HITRUST RMFs using a 4-step risk management process, and
- How the HITRUST RMF is more practical and provides more value for non-federal healthcare entities.

The more the security and regulatory landscape changes, the more an RMF is needed, and the better value HITRUST offers the industry—the heavy lifting is already done.

# Background

## Overview

Healthcare organizations are facing multiple challenges with regards to information security and privacy. Redundant and inconsistent requirements and standards increase complexity and drive up costs. Confusion around acceptable safeguards and the lack of defined security requirements result in critical systems without appropriate administrative, physical and technical safeguards. Further, the increased scrutiny from regulators, auditors, underwriters, customers and other third parties leaves the industry coping with additional exposure, increased liability, and growing risks to patients, their families and healthcare organizations. In addition, organizations are challenged with appropriately managing the sharing of information due to the wide range of business partners and other third parties with different capabilities, requirements and risk profiles.

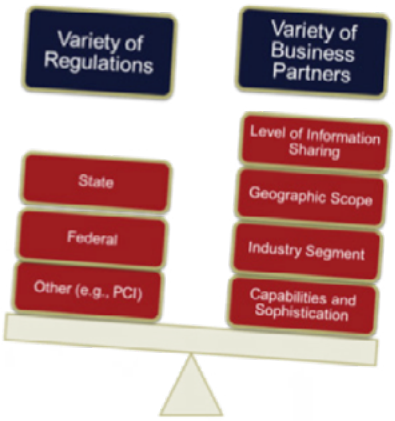



**Figure 2**

These issues led to a growing need and broad desire for a common security framework—a set of common standards and supporting methodologies—that would provide a minimum baseline set of security requirements. Due to the varied nature of organizations in healthcare in particular, this framework also needed to be tailorable to a specific size and type of organization, which would improve adoption and implementation, and subsequently improve stakeholder trust as well as further mitigate potential liability from breaches of sensitive information.

Thus, HITRUST was born out of the belief that information security and privacy are critical to the broad adoption, utilization and confidence in health information systems, medical technologies and electronic exchanges of health information. The HITRUST CSF® provides the needed fundamental and holistic change in the way industry manages information security and privacy-related risk. It rationalizes legislation, regulations, standards and best practices into a single overarching framework and provides a consistent approach to certification and risk acceptance.

## HIPAA

The principle driver behind security and privacy in healthcare for many years was without a doubt the Health Information Portability and Accountability Act (HIPAA), which incorporates specific privacy and security requirements for providers, payers and other covered entities in the healthcare industry. HIPAA's Security Rule provided numerous implementation specifications that essentially required covered entities to implement reasonable and appropriate administrative, technical and physical safeguards for protected health information (PHI).

Unfortunately, the implementation specifications in the Rule generally lack the level of prescriptiveness necessary to determine a standard of due care or diligence, i.e., safeguards that would be considered 'reasonable and appropriate.' Organizations were subsequently left to determine these safeguards for themselves but often found them difficult to justify given the costs associated with their implementation. It is

notoriously difficult to quantify a return on investment for new security investments unless existing technologies or processes are being replaced, allowing such costs to be calculated. Unless specifically required by a business partner or regulator, security investments are most often justified based on 'cost avoidance' calculations, or what has been referred to by some security experts as 'fear, uncertainty and doubt.'

To compound matters, healthcare is a service industry focused on quality of care as well as efficiency and cost. Given that patients and others have found it difficult to evaluate this quality of service, it is subsequently difficult for organizations to calculate their return on investment for any initiative, let alone those with significant security and privacy requirements. Fortunately, it only took three years after compliance with the Security Rule was mandatory for the federal government to realize the difficulties engendered with the Rule's practical application and issue additional legislation.

### HITECH

As part of the national initiative to improve quality and lower the cost of healthcare through the meaningful use of electronic health record (EHR) systems and health information exchanges (HIEs), Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act of 2009. In addition to the privacy and security requirements for meaningful use, in which covered entities are expected to conduct or review a security risk analysis and correct identified deficiencies, the most significant changes stemming from HITECH were the establishment of a federal breach notification requirement and increased enforcement of the HIPAA Security Rule through the Office of Civil Rights (OCR).

Unfortunately, the HITECH Act did not provide significant additional guidance to organizations on what levels of due diligence and due care are reasonable and appropriate. It was not until a few years later when OCR and NIST began cooperating on providing guidance on the HIPAA Security Rule's requirements that covered entities began to get a real indication of the increased level of rigor the federal government expected. OCR and NIST began hosting a series of annual joint conferences on security and privacy, and worked together to produce the NIST HIPAA Security Rule (HSR) Toolkit in 2011. OCR also published additional guidance in 2012 on the audit protocol being used as part of the overall HIPAA enforcement effort. (Note a much anticipated second version of the protocol was published in 2016, providing more specific guidance on the types of activities OCR expected covered entities to undertake for each of the Rule's standards and implementation specifications.)

### Omnibus Rule

The HIPAA Final Omnibus Rule published in January of 2013—10 years after the Security Rule was released—provides final modifications to the HIPAA Privacy, Security and Enforcement Rules embedded in the HITECH Act, a final rule on tiered monetary penalties, and a Breach Notification Rule. One of the most significant aspects of the Omnibus Rule is its application to business associates, which are now directly liable for failure to comply with the all the Rule's requirements, including the HIPAA Security Rule as mandated by HITECH.

### Other Drivers

While legislation and regulation are arguably the principle driver for security and privacy in healthcare, there are numerous other legislative, regulatory, industry and best practice requirements that healthcare entities must address. Examples include the Privacy Act of 1974, the Genetic Information Non-discrimination Act (GINA) of 2008 (later incorporated into the HIPAA Omnibus), the Federal Trade Commission (FTC) Red Flags Rule and Fair Information Practice Principles, Federal Drug Administration (FDA) requirements for EHRs and electronic signatures, multiple state-level security and privacy legislation and regulations, and the Payment Card Industry Digital Security Standard (PCI-DSS).

### Summary

Organizations have faced, and will continue to face, multiple challenges with regards to information security and privacy, including the growing need to demonstrate compliance with multiple federal, state and industry requirements. However, given the general lack of definition and prescriptiveness of these requirements, organizations are left with the task of deciding what actions would be considered 'reasonable and appropriate' and what level of protection would be 'adequate' in the eyes of federal, state and industry regulators, business partners, customers, and other interested third parties. Implementing the right framework, processes and tools is the only efficient and effective way to manage information risk and compliance.

The HITRUST CSF provides the needed fundamental and holistic change in the way industry manages information security and privacy-related risk. It rationalizes legislation, regulations, standards and best practices into a single overarching framework tailored for industry —healthcare in particular— and provides a consistent approach to assessment, certification and risk acceptance.

## Risk Management Frameworks

### Overview

So, how can an organization determine 'reasonable and appropriate' safeguards to provide 'adequate' protection for sensitive information? Or stated another way, how can an organization select and implement a specific set of controls to manage information security and privacy-related risk at an acceptable level?

The textbook answer is through a comprehensive risk analysis that (1) includes threat and vulnerability assessments, information asset valuation, and the selection of a comprehensive set of information security and privacy controls that addresses the enumerated threat-vulnerability pairs (a process sometimes referred to as threat modeling), (2) is cost-effective, and (3) manages risk at a level deemed acceptable by the organization.

From a quantitative viewpoint, this process is virtually impossible for many—if not most—organizations to perform. For example, unless actuarial-type information is available, the likelihood a threat-source will successfully exploit one or more vulnerabilities cannot be calculated with any level of precision. In the case of a human actor, likelihood is also dependent on the motivation of the threat source and the difficulty or cost associated with exploiting one or more vulnerabilities to achieve the threat actor's objectives. As a result, it is similarly difficult to develop a valid business case for a specific risk response or treatment based on a return on investment. Organizations could take a semi- or quasi-quantitative approach or even a purely qualitative approach; however, it would still be difficult for an organization to develop a valid business case, particularly for a comprehensive set of risk responses.

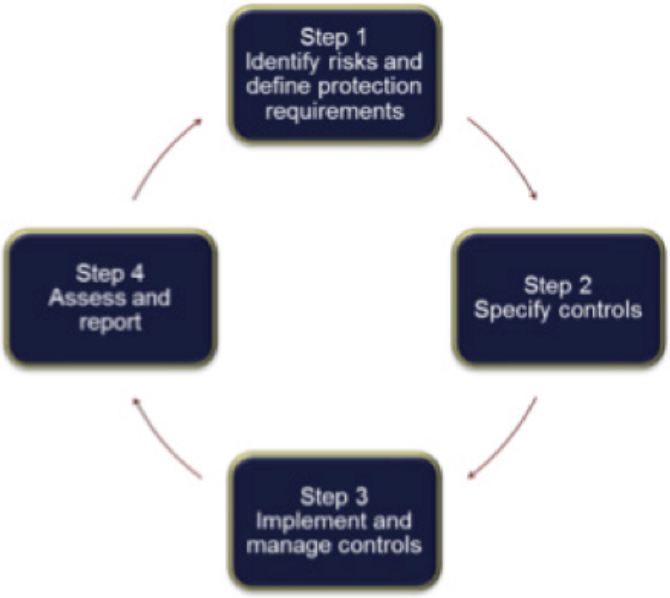



**Figure 3**

An alternative approach is to rely on other organizations that do have the resources to develop a set of controls that addresses similar threats to similar technologies employed by their own organization. This is the approach employed by the intelligence community (IC), defense department and civilian agencies of the federal government with their respective information security control frameworks, all of which are now based on the NIST RMF. It is the HITRUST RMF, which consists of the HITRUST CSF combined with CSF Assurance Program-related documents and tools, such as the HITRUST CSF Assurance Program requirements, HITRUST Authorized External Assessor requirements, HITRUST CSF assessment methodology, and HITRUST's comprehensive online tool, MyCSF.

## General RMF

Risk management frameworks support a basic 4-step risk management process model:

- Step 1—Identify risks and define protection requirements
- Step 2—Specify controls
- Step 3—Implement and manage controls
- Step 4—Assess and report

## Step 1 - Identify Risks and Define Protection Requirements

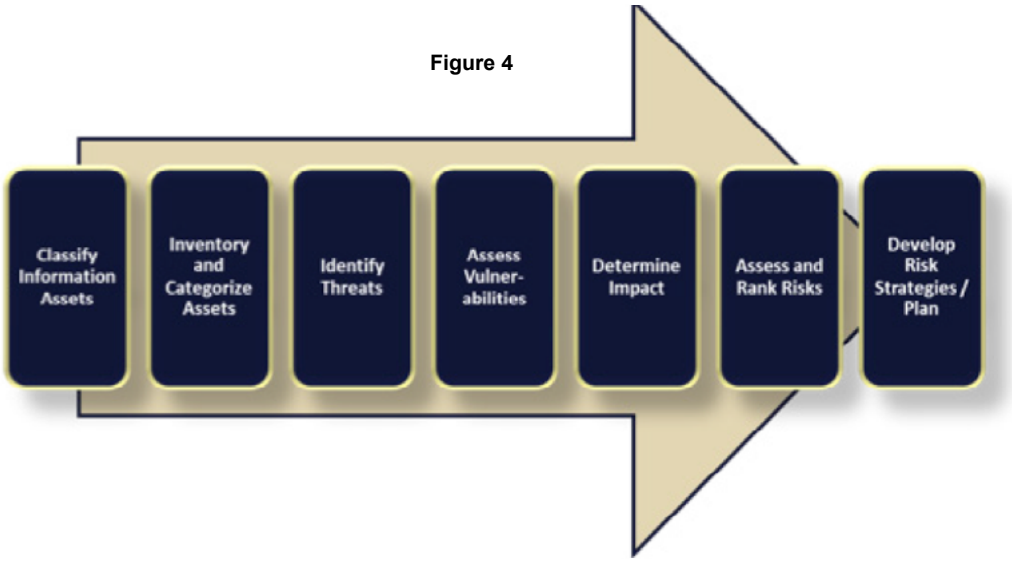
The objective of this step is to determine the risks to information and information assets that are specific to the organization. Risks can be identified through the analysis of regulations and legislative requirements, breach data for similar organizations in the industry, as well as an analysis of current architectures, technologies and market trends. The end result of this analysis should be a prioritized list of high-risk areas and an overall control strategy to minimize the risk to the organization from the use of sensitive or business critical information in terms of overall impact to the organization.

This step is supported by seven sub-processes, which range from the classification of information assets to the development of specific risk treatments. As indicated previously, this is one of the more problematic aspects of risk analysis that a control-based risk management framework will help an organization address.

### Step 2 - Specify Controls

The next step is to determine a set of reasonable and appropriate safeguards an organization should implement to adequately manage information security risk. The end result should be a clear, consistent and detailed or prescriptive set of control recommendations that are customized for the organization.

**Figure 4**




A control-based risk management framework will provide a comprehensive control catalog derived from the seven sub-processes outlined earlier as well as specific criteria for the selection of a baseline set of controls, which is performed in this step.

### Step 3 - Implement and Manage Controls

Controls are implemented through an organization's normal operational and capital budget and work processes with board-level and senior executive oversight using existing governance structures and processes. A risk management framework will provide guidance and tools for implementation of the framework, including the controls specified earlier in step 2.

### Step 4 - Assess and Report

The objective of this last step is to assess the efficacy of implemented controls and the general management of information security against the organization's baseline. The result of these assessment and reporting activities is a risk model that assesses internal controls and those of business associates based on well-defined risk factors. It should also provide common, easy-to-use tools that address requirements and risk without being burdensome, support third-party review and validation, and provide common reports on risk and compliance.

### Summary

Unless skilled personnel and other resources are available to determine a comprehensive set of 'reasonable and appropriate' safeguards to provide 'adequate' protection for sensitive information, healthcare organizations should leverage existing control and risk management frameworks. This is the same approach used by the federal government, and it is also the approach used by the healthcare industry through HITRUST.

But regardless of the source, a risk management framework is supported by a risk management process, which at a basic level incorporates four distinct steps.

- Step 1—Identify risks and define protection requirements
- Step 2—Specify controls
- Step 3—Implement and manage controls
- Step 4—Assess and report

Although structured on International Standards Organization and International Electrotechnical Committee (ISO/IEC) Standard 27001 and incorporates guidance from ISO/IEC 27002, the HITRUST CSF relies heavily on NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and integrates other NIST and federal security guidance such as the Centers for Medicaid and Medicare (CMS) Information Systems (IS) Acceptable Risk Safeguards (ARS). As such, the rest of this white paper will focus on the NIST and HITRUST risk management frameworks in the context of this four-step process and identify some of the differences between them.

## NIST RMF

NIST provides a structured process and a significant amount of guidance to help federal organizations identify and assess risk to their information and information systems and take steps to reduce risk to an acceptable level. This is accomplished through the publication of various NIST SP 800-series documents, Federal Information Processing Standards (FIPS) documents, and Inter-agency Reports (NIST IRs), which help guide federal agencies through a six-step risk management process designed to minimize the risk of harm from the unauthorized access, use, disclosure, disruption, modification or destruction of sensitive information. NIST SP 800-37 Revision 1 outlines the process and provides additional guidance by mapping other NIST documents in the framework to each step of the process.

The six-step NIST risk management process can be mapped to the basic four-step process as follows: Categorize Information System to step 1; Select Security Controls to step 2; Implement Security Controls, Assess Security Controls and Authorize Information System to step 3; and Monitor Security Controls to step 4. (Note, we consider the security assessment performed as part of system authorization to be different from the ongoing assessment and monitoring of security controls post-implementation.)

### Step 1- Identify Risks and Define Protection Requirements

The first step of NIST's risk management process, Categorize Information Systems, categorizes an information system and the information being processed, stored and transmitted by the system based on the potential impact to the organization should a threat-source successfully exploit a vulnerability. FIPS 199 requires organizations to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity and availability. The potential impact values

assigned to the respective security objectives are the highest value (high-water mark) from among the security categories determined for each type of information processed, stored, or transmitted by the information system(s) considered in scope. Related publications include NIST SP 800-60.

Note for healthcare organizations: although not technically part of the NIST RMF publications, NIST SP 800-66 provides links from the NIST RMF to the HIPAA Security Rule's implementation specifications. However, the publication doesn't specify a security categorization for ePHI; this exercise is left to the federal healthcare organization.

### Step 2 - Specify Controls

The first step in selecting security controls for the information system is to choose an initial set of baseline security controls from NIST SP 800-53 based on the impact level of the information system as determined by the security categorization performed in step 1. The organization selects one of three sets of baseline security controls from the security control catalog corresponding to the low-impact, moderate-impact, or high-impact rating of the information system. Note, NIST foregoes the traditional security objectives of confidentiality, integrity and availability used in FIPS 199, *Standards or Security Categorization of Federal Information and Information Systems*, and uses sensitivity and criticality instead. NISTIR 7298 r2, *Glossary of Key Information Security Terms*, defines sensitivity as a "measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection," and criticality as a "measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function." For the protection of PHI and systems processing ePHI, HITRUST considers confidentiality (and privacy) requirements an indication of sensitivity, and integrity and availability requirements an indication of criticality.

After selecting the initial set of baseline security controls, the organization starts the tailoring process to appropriately modify and more closely align the controls with specific conditions within the organization (i.e., conditions specific to the information system or its environment of operation). The tailoring process includes:

- Applying scoping guidance to the initial baseline security controls to obtain a preliminary set of applicable controls for the tailored baseline;
- Selecting (or specifying) compensating security controls, if needed, to adjust the preliminary set of controls to obtain an equivalent set deemed to be more feasible to implement; and
- Specifying organization-defined parameters in the security controls via explicit assignment and selection statements to complete the definition of the tailored baseline.

Although the security control selection process is generally focused on the information system, NIST states the selection process is also applicable at the organizational and mission/business process levels. General guidance in applying the NIST RMF at these levels may be found in NIST SP 800-39 , *Managing Information Security Risk: Organization, Mission, and Information System View*. However, the tailoring process described in NIST SP 800-53 is neither prescriptive nor managed, which does little to guarantee tailoring is performed consistently from one organization to the next or, more often than not, that tailoring is performed at all. Related publications include FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

Additional guidance for healthcare organizations can be found in NIST SP 800-66, *An Introductory Resource Guide for Implementing the [HIPAA] Security Rule*, as it addresses key activities for each of the Rule's standards and implementation specifications, e.g., section 4.1.1 is "Identify Relevant Information Systems," which supports HIPAA § 164.308(a)(1), Security Management Process. An organization may also look up the associated NIST controls and NIST RMF documents referenced in each section for more information. For example, NIST SP 800-66 § 4.1.1 maps 164.308(a)(1) to NIST SP 800-53 control RA-1 and crosswalks to the following publications: FIPS 199, NIST SP 800-37, NIST SP 800-39, and NIST SP 800-53, among others. However, it's up to the organization to parse the references among the nine key activities, as well as read through and apply information from each of the referenced publications.

A healthcare organization can use NIST SP 800-66 to determine all the possible NIST controls that support the implementation specification and come up with additional controls that map to the implementation specifications but not explicitly provided in the NIST tool- kit. However, it is similarly left to the organization to parse through the NIST SP 800-53 controls and determine the subset of requirements that directly support the HIPAA Security Rule's implementation specifications.

NIST SP 800-66 also provides some additional tailoring recommendations for healthcare organizations by mapping controls from NIST SP 800-53 to the HIPAA Security Rule's standards and implementation specifications and describing key activities for each; however, this would only address an organization's obligations under the Rule. Other controls may be needed to support other legislative, regulatory, industry or best practice requirements.

In addition, there is little if any prescriptive guidance on control selection based on risk factors such as organizational size/capability or assignment of acceptable organization-defined parameters. However, healthcare organizations may refer to the CMS IS ARS for additional guidance on the selection of organization-defined parameters for low-, moderate- and high-level NIST control baselines.

### Step 3- Implement and Manage Controls

NIST provides guidance on various information security controls in an extensive library of NIST SP 800-series, FIPS and NIST IR documents, and provides a guide for selecting documents organized by specific topics such as biometrics (e.g., FIPS 201-1 and NIST SP 800-116, *A Recommendation for the Use of PIV Credentials in Physical Access Control Systems*) and cryptography (e.g., FIPS 198-1, *The Keyed-Hash Message Authentication Code*) or specific NIST control families such as access control (e.g., FIPS 200 and NIST SP 800-114, *User's Guide to Securing External Devices for Telework or Remote Access*) and Contingency Planning (e.g., NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*). NIST also provides guidance on capital planning in NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, and system development in NIST SP 800-64, *Security Considerations in the System Development Life Cycle*; however, there is little in the way of specific guidance or tool support on how the NIST control framework can be implemented in industry. Related RMF publications include NIST SP 800-37 and 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, among others.

NIST SP 800-66 does not provide information on how to implement or manage security controls in a healthcare environment.

### Step 4 - Assess and Report

NIST provides general assessment guidance for the NIST SP 800-53 control catalog in NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, a technical assessment guidance in NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, and targeted assessment guidance in documents like NIST IR 7316, *Assessment of Access Control Systems*. NIST also provides a process maturity-based security assessment methodology in NIST IR 7358, *Program Review for Information Security Management Assistance (PRISMA)*. Although not formally incorporated in the NIST RMF, PRISMA provides an intuitive approach to the evaluation of information security controls by considering whether the requirement is specified in policy, supported by formal processes, implemented across the organization, tested to ensure continued effectiveness, and that activities supporting the first four levels are fully integrated with each other and the organization's control environment. The NIST IR also provides guidance on how to prepare for and execute a PRISMA-based assessment as well as information around the practical application of the formal report. Related RMF publications include NIST SP 800-37.

NIST SP 800-66 provides specific questions for healthcare organizations to consider when assessing one's information protection program, organized by HIPAA Security Rule standard and implementation specification, but provides limited guidance on the risk assessment process that could help address requirements that may not be directly related to the HIPAA Security Rule standards and implementation specifications.

In 2011, NIST published the HIPAA Security Rule "HSR" Toolkit, which provides 472 questions for "standard" organizations and 809 questions for "enterprise"-level organizations. NIST also references other sources for each question: 491 questions map to NIST SP 800-66 sections addressing the HIPAA implementation specifications, 290 map to a specific NIST SP 800-53 control, and 28 are not mapped. While an excellent resource, NIST cautions users that "the HSR Toolkit is not intended to make any statement of an organization's compliance with the requirements of the HIPAA Security Rule."

And in 2014, HHS published the Security Risk Assessment (SRA) tool to help small and medium-sized businesses go through the risk analysis process. The tool does a much better job than the original OCR Audit Protocol in helping organizations address salient elements of the HIPAA Security Rule's standards and implementation specifications; however, questions are specific to the Rule's requirements and subsequently has some of the same limitations as the NIST HSR Toolkit. HHS also has similar disclaimers, stating:

- Use of this tool is neither required by nor guarantees compliance with federal, state or local laws.
- The information presented may not be applicable or appropriate for all healthcare providers and organizations.
- The tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks.

Organizations may also leverage the second OCR Audit Protocol published in 2016 to determine high interest areas they should ensure are addressed in their security program, and which should be assessed accordingly. However, organizations must understand that, like all audits, the Protocol is narrowly focused and may not address all the security control requirements that would be implemented by the organization to support its obligations under the HIPAA Security Rule. The audit procedures also focus heavily on policy

and process requirements but, unlike the original, provide guidance on specific activities that help address the intent of a particular standard or specification. However, neither the tools or the audit protocols provide a mechanism to evaluate and score the relevant maturity of the control, compute risk estimates or support risk reporting. This is left for the organization to determine.

Organizations should note that, while the NIST HSR Toolkit, HHS SRA Tool OCR Audit Protocol and DHS/OCR SRA tool will support HIPAA-specific assessments, they do not necessarily support a more general assessment that includes other legislative, regulatory, industry or best practice requirements that should be addressed by an organization's information protection program, including the provision of third-party assurances about its program to relevant internal and external stakeholders.

### Summary

NIST publishes a comprehensive set of controls designed for use by federal agencies, an extensive library of guidance documents for the NIST RMF, and special interest documents on specific information security topics and control areas. NIST also publishes an excellent resource on the implementation of NIST SP 800-53 security controls to satisfy HIPAA requirements. However, private-sector organizations are not subject to all the same legislative and regulatory requirements as a federal healthcare organization (e.g., the Federal Information Security Management Act), nor do they have the same skilled personnel and resources available to support their information security program. It can be difficult for many organizations to adapt the NIST RMF to their specific needs, i.e., to determine what controls are "reasonable and appropriate" for a non-federal organization. In particular, NIST healthcare guidance is focused on compliance with the HIPAA Security Rule and does not specifically address the selection and implementation of controls necessary to satisfy other legislative, regulatory, industry and best practice requirements.

HITRUST was formed to address the growing need and broad desire within the industry for a common framework—a set of common standards and supporting methodologies—that would provide a minimum baseline set of security requirements, tailorable to a specific size and type of organization, which would improve trust as well as mitigate potential liability from breaches of sensitive information. HITRUST believes that improvements in the state of information security and privacy are critical to the broad adoption, utilization and confidence in health information systems, information technologies and electronic exchanges of information. The HITRUST RMF provides a consistent approach to certification, risk acceptance and shared trust through the HITRUST CSF, CSF Assurance Program, and supporting methodologies and tools such as the HITRUST CSF Assessment Methodology and MyCSF.

## HITRUST RMF

### Step 1 - Identify Risks and Define Protection Requirements

The HITRUST CSF provides a fundamental and holistic change in the way industry manages information security and privacy-related risk by rationalizing relevant regulations and standards into a single overarching framework designed for industry and tailorable to an organization.

Figure 5 is intended to show how various frameworks and standards are mutually reinforcing, can be tailored to an organization's needs, and intelligently applied in the intended environment to help ensure organizations meet business goals while achieving regulatory compliance. It shows that overarching

governance frameworks such as COBIT can be integrated with risk management frameworks like the NIST RMF and ISO/IEC 27000-series publications, as well as other frameworks like ITIL for service delivery and ISO 9000 for capability or process maturity. This concept applies to many other standards that an enterprise may wish to adopt. The key is to adopt specific frameworks and standards that meet one's needs, tailor them appropriately and implement them smartly.

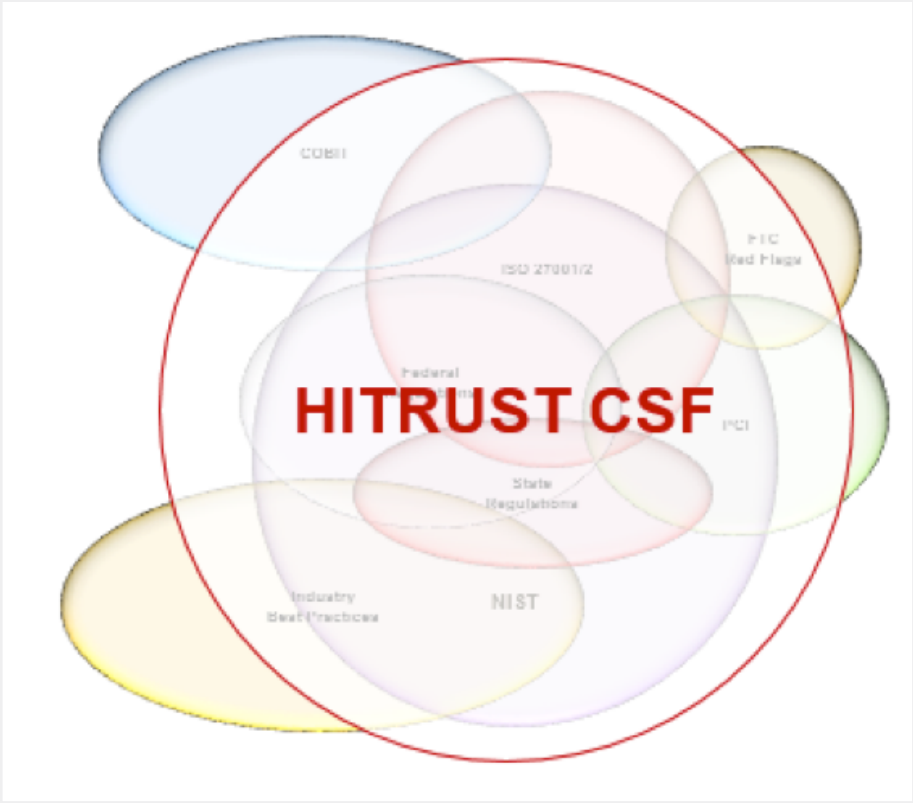



Figure 5

HITRUST structured the CSF on the ISO/IEC 27001 control framework and baselined the initial control requirements from NIST SP 800-53 as well as security- and privacy-relevant requirements from legislative, regulatory, industry and best practice guidance such as ISO/IEC 27002, HIPAA, HITECH, CMS, FTC Red Flags, PCI-DSS, ISO 27799 and COBIT. State requirements specific to information security are also integrated into the framework. This allows organizations to leverage a single industry control framework to meet its business objectives and satisfy multiple regulatory and other compliance requirements.

The HITRUST CSF is freely available to qualified organizations through the HITRUST website or by paid subscription to MyCSF for an interactive version tailorable to the subscribing organization.

### Step 2 - Specify Controls

Like NIST, HITRUST built the CSF to accommodate multiple control baselines. However, unlike NIST, HITRUST assigns controls using three risk factors: organizational (e.g., holds fewer than 60 million total records), system requirements (e.g., the system stores ePHI, is accessible from the Internet, and process-

es fewer than 6,750 transactions per day), and regulatory requirements (e.g., subject to FTC Red Flags Rule and PCI-DSS compliance). The result is a semi-custom, industry-specific information security control baseline, i.e. a set of controls that is partially tailored to an organization's clinical, business and compliance requirements, as shown below.


Figure 6

The capability to tailor controls to a specific organization's needs is available in MyCSF. Training on the CSF and the MyCSF assessment support tool is provided to anyone seeking the HITRUST Certified CSF Practitioner (CCSFP) credential.

### Step 3 - Implement and Manage Controls

HITRUST trains third-party consulting and assessment firms in the CSF and CSF Assurance Program methodologies and tools so that they may offer CSF implementation support to healthcare provider organizations that lack the capability to implement and assess information security and privacy controls, as recommended by HHS.

HITRUST also recommends the development of an information security and privacy risk management architecture in which strategic planning and information security architecture, policies and standards form the foundation for specific customer-facing information security and privacy services, which should be documented in security and privacy service catalogues consistent with recommendations in the Information Technology Infrastructure Library (ITIL). Examples of these customer-facing services include security operations, incident management and investigations, business continuity and disaster recovery, identity

and access management, and education, training and awareness. CSF controls and available resources can then be mapped to each service. The result is the ability to develop operational and capital project plans for defined security services based on deficiencies for specific control requirements identified via risk assessment as well as continuous monitoring activities such as vulnerability assessment, penetration testing, control maturity assessments and incident root cause analysis.

### Step 4 - Assess and Report

The HITRUST CSF Assurance Program provides simplified and consistent compliance assessment and reporting against the CSF and the authoritative sources it incorporates. This risk-based approach, which is governed and managed by HITRUST, is designed for the unique regulatory requirements and business needs that provide organizations with an effective, standardized and streamlined assessment process to manage compliance. This solution offers a more effective process than that used by other assessment approaches and toolkits, which support only limited requirements and checkbox approaches to assessment and reporting.

An integral component of the CSF Assurance Program is the HITRUST risk assessment methodology, which is built around the concept of residual risk, i.e., the risk that is left after the controls, which are intended to mitigate risk to a level deemed acceptable by the organization, have been fully implemented. Thus, excessive residual risk occurs when one or more controls are not fully implemented, and it is this risk the organization must strive to minimize in its day-to-day operations.

Since excessive residual risk may be estimated by the risk of a control failure, we must estimate the likelihood the control will fail as well as the impact to the organization when a failure occurs. Some purists might argue that only quantitative assessments provide value; however, in reality, decisions are often made with incomplete information. The reasons are many and varied. For example, there may be a limited amount of time in which to make a decision, or the information simply is not available. In many cases, expert judgment is applied such as when auditors scope work or make judgments about the effectiveness of financial controls. (Decision making under conditions of uncertainty is a central focus of the body of knowledge known as ‘decision theory.’)

The level of precision one needs to make a decision may also depend on the type of problem or question being addressed. For example, triage in an emergency room following a natural disaster requires a general level of information. Is the patient breathing or bleeding? Is the injury life threatening? Medical diagnoses, on the other hand, generally require a much more granular level of information to determine if the patient is suffering from one particular disease or another with similar symptoms. However, none of the decisions described are made without some sort of framework or methodology to support the decision-making process.

HITRUST leverages the NIST PRISMA methodology, which incorporates the concept of capability maturity to determine likelihood of a control failure but expresses the levels in a way that, while roughly equivalent with their Capability Maturity Model-Integrated (CMMI) counterparts, is much more intuitive for the evaluation of information security, as opposed to the traditional language used around process maturity. HITRUST also leverages the PRISMA quasi-quantitative scoring model to facilitate the assessment process and provide a standardized estimate of the maturity (effectiveness) of a control’s implementation.

The other part of the risk equation—the impact of a specific control failure—is often harder to assess than the efficacy of the control implementation, especially in the context of the entire control environment. One way to make this more tractable is to map control-level impacts from, and through, established information security

control frameworks to provide a non-contextual estimate of the relative impact of one control failure with respect to another. HITRUST leveraged work done by the DoD to assign non-contextual impact values to individual controls contained in DoD Instruction 8500.2. By mapping through the NIST 800-53 controls to the ISO 27001 information security control clauses, estimates of the relative impact for the failure of each control were obtained. This provides a common point of reference for organizations to use in a contextual analysis, e.g., one that might be performed on a smaller sub-set of controls found deficient in an audit, which is arguably more tractable than trying to determine the impact of all the controls implemented in the environment at the same time. HITRUST believes this approach is justified as it was used extensively by the DoD in its information system security certification and accreditation methodology, when developing a residual risk analysis after a security test and evaluation.

Once estimates are obtained for impact and likelihood, the computation of estimated residual risk is relatively straightforward. However, rather than represent risk in terms of "heat maps," it is possible to present risk to executive management in a more intuitive way. By making adjustments to the PRISMA scoring model and normalizing the risk computations on a scale of zero to 100, excessive residual risk may be represented as academic-style grades. In this model, anything below 60 would be a failing grade (an 'F') and present a severe risk. Similarly, scores from 60 to 70 would represent a high risk (a 'D'), from 70 to 80 a medium risk (a 'C'), from 80 to 90 a low risk (a 'B'), and from 90 to 100 as a minimal risk (an 'A'). (In this model, a score of 75 would most likely indicate the organization had policies and procedures in place and the control was fully implemented.) HITRUST essentially interprets a 'C" as the minimum acceptable 'passing grade' for the purposed of certification. Better grades, i.e., better assurances a control is effective and will continue to be effective, are provided through continuous monitoring of the control, i.e., keeping track of how well the control is performing and addressing any deficiencies as they arise.

Although not a true quantitative estimate of the risk, the scores provide sufficient information in a very intuitive way for organizations to make decisions under normal conditions of uncertainty about the relative control-related risks these scores represent.

A graphical representation of the control objectives and the control categories they support (such as the one that follows in figure 7) can be provided for specific systems and/or business units within an organization. vIn the case of a healthcare entity, this could be an electronic health record system, organizations such as single hospitals within a health system, or common departments within health systems such as emergency rooms or pharmacies. These scores can also be used for internal and industry-level benchmarking.

HITRUST CSF assessments are now supported by a fully integrated, optimized, and user-friendly tool which marries the content and methodologies of the CSF and CSF Assurance Program with the technology and capabilities of a governance, risk and compliance (GRC) tool. MyCSF provides healthcare organizations of all types and sizes with a secure, Web-based solution for accessing the CSF, performing assessments, managing remediation activities, and reporting and tracking compliance. MyCSF is also managed and supported by HITRUST, providing organizations with up-to-date content, accurate and consistent scoring, reports validated by HITRUST and benchmarking data available nowhere else within the industry, thus going far beyond what a traditional GRC tool provides.

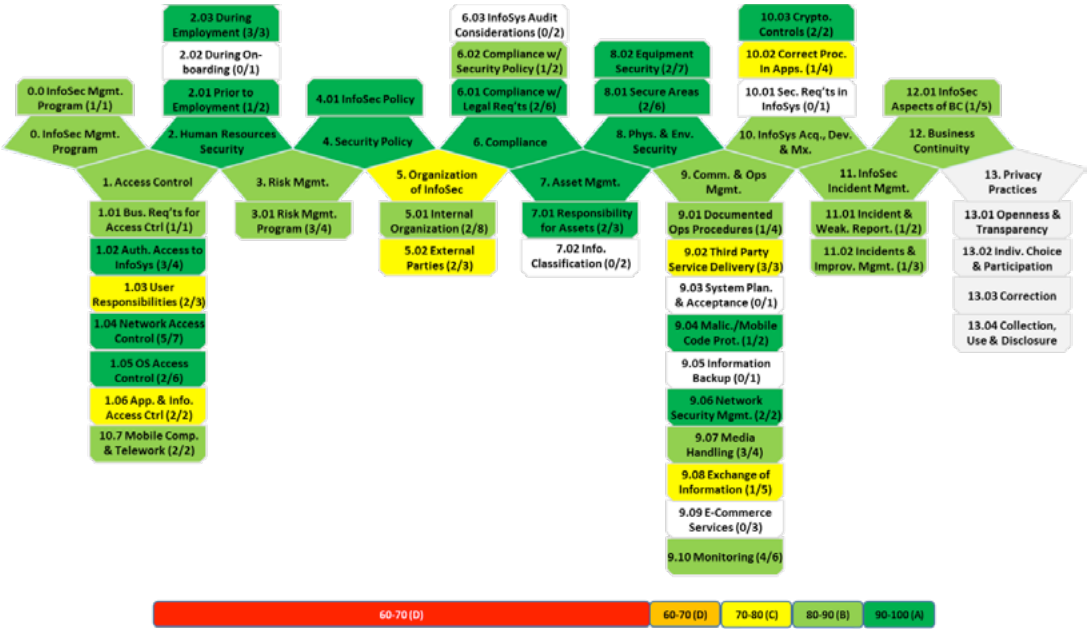



**Figure 7**

The CSF Assurance Program enables trust in health information protection through an efficient and manageable approach by identifying incremental steps for an organization to take on the path to becoming HITRUST CSF Validated or CSF Certified.

The comprehensiveness of the security requirements specified for an assessed entity is based on the multiple levels within the HITRUST CSF, which are determined by its risk factors. The level of assurance for the overall assessment of the entity is based on multiple tiers or levels of assessment, from Readiness Assessment questionnaires to on-site analysis/testing performed by an independent External Assessor. The results of the assessment are documented in a standard report with a compliance scorecard and remediation activities tracked in a corrective action plan (CAP). Once vetted by HITRUST and performed for all levels of assurance, the assessed entity can use the assessment results to report to external parties in lieu of existing security requirements and processes, saving time and minimizing costs.

The following diagram outlines the relationship between the comprehensiveness of an assessment and its level of assurance provided by the assessment for organizations of varying complexity based on the risk of the third-party relationship as determined by the relying organization:
A HITRUST CSF assessment allows an organization to communicate to relying entities its compliance with the CSF and, optionally, with other requirements such as HIPAA. HITRUST reviews the assessment results and CAPs to provide added assurance to those external entities relying on the assessed entity's results. And the HITRUST CSF Assurance Program effectively establishes trust in information protection through an achievable assessment and reporting path for organizations of all sizes, complexities and risks.

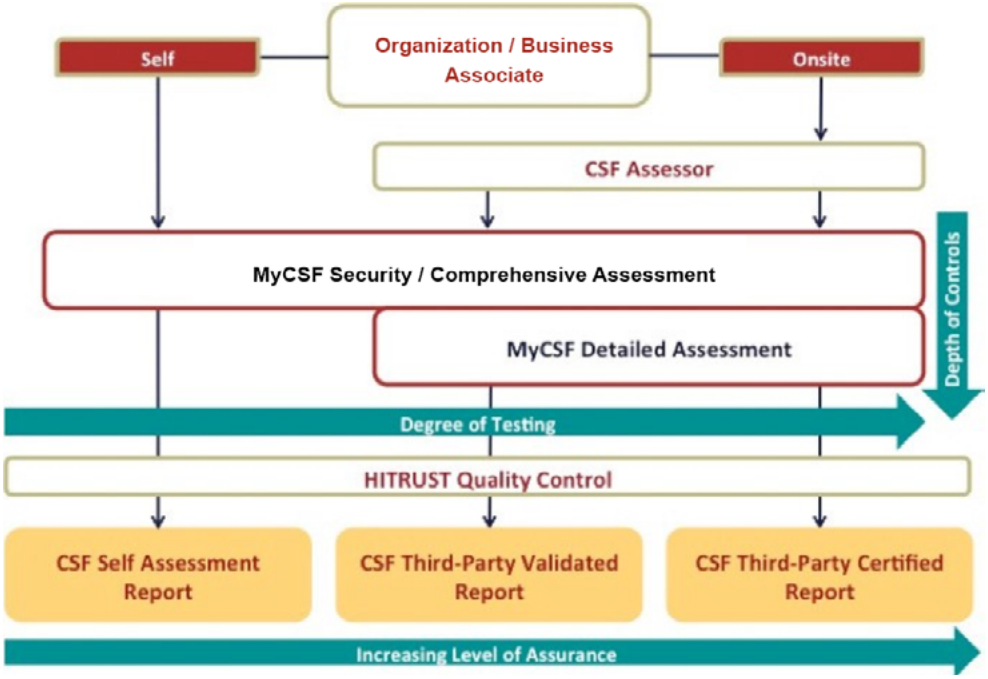



**Figure 8**

## Summary

HITRUST integrated multiple international, federal, industry frameworks and best practice standards and frameworks, adapted them to the healthcare environment, and provided an industry standard of due diligence and due care that can be tailored to an individual organization based upon its specific business requirements. The HITRUST CSF and CSF Assurance Program provide organizations with a single approach to assessment and reporting against these multiple requirements, and both are updated at least annually to account for changes in legislation, regulation, standards, guidance and best practices, such as with the release of the NIST SP 800-53 revision 4, the NIST Cybersecurity Framework. Further, all changes to the HITRUST CSF are provided to the industry for review and comment to ensure an open and transparent framework that is freely available to qualified organizations that wish to use it.

## Conclusion

The only thing constant about information security and privacy in is change. New regulations, standards, guidance and tools continue to complicate the landscape, and organizations are left to determine how best to achieve compliance and provide an 'adequate' level of protection.

Healthcare organizations often do not have the skilled personnel or resources to develop a custom set of 'reasonable and appropriate' safeguards and choose to adopt and adapt external information security control and risk management frameworks. But even this can be difficult for many organizations to do. So, rather than independently performing the work of integrating multiple international, federal and industry frameworks and best practice standards and then adapting them to their specific organization, HITRUST was formed to perform this work on behalf of the industry and establish a standard of due diligence and due care that can be tailored to an individual organization based upon their specific business requirements—the HITRUST CSF.

The HITRUST CSF Assurance Program also provides organizations a single approach to assessment and reporting against these multiple requirements, and both the CSF and CSF Assurance Program are updated at least annually to account for changes in legislation, regulation, standards, guidance and best practices,

such as with the 2014 release of the NIST Cybersecurity Framework. Further, all changes to the CSF are provided to the industry for review and comment, ensuring transparency and openness. And HITRUST provides the CSF free to qualified healthcare organizations that wish to implement the framework.

Given that the CSF is an integrated, harmonized, healthcare centric, transparent, prescriptive, tailorable, scalable and certifiable framework that provides a common mechanism for the sharing of risk information, why hasn't it been adopted by 100 percent of healthcare organizations? Unfortunately, many organizations have not yet come-to-terms with the level of due diligence and due care required to safeguard ePHI and meet regulatory compliance requirements.

For example, the NIST HSR toolkit appeals to some organizations because it provides a "check-the-box" approach to addressing specific safeguards; however, they often fail to dig deeper into the references to determine what is actually "in-the-box" they are checking. They may stop with the results of this control gap analysis and fail to fully evaluate the likelihood and impact components necessary to complete the risk analysis. Other organizations may go even further and rely on the OCR Audit Protocol to satisfy their HIPAA risk analysis requirements without realizing the protocol is incomplete; it doesn't address every implementation specification in the Security Rule and does not integrate well with the NIST HSR Toolkit or the NIST RMF. The focus is on "passing" an audit rather than on the spirit and intent of their compliance requirements. The HITRUST CSF on the other hand, is tightly integrated with the CSF Assurance Program and MyCSF.

Fortunately, most of the industry understands the need to provide 'reasonable and appropriate' safeguards and satisfy their regulatory obligation to provide 'adequate' protection, which is why the HITRUST CSF is demonstrably the de facto standard in the healthcare industry. The 2018 Healthcare Information and Management Systems Society (HIMSS) Cybersecurity Survey indicates the HITRUST CSF is the leading information security control framework in healthcare, and the *NIST Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)* recognizes the HITRUST CSF as an industry-led security standard that addresses multiple areas of concern with the use of IoT devices. The Government Accountability Office (GAO) *Report to Congressional Committees on Critical Infrastructure Protection* also cites the HITRUST CSF as a means of demonstrating compliance with the NIST Cybersecurity Framework in the HPH sector, as demonstrated in the *Healthcare Sector Cybersecurity Implementation Guide*—a document produced under the auspices of the Critical Infrastructure Protection Advisory Council (CIPAC).

For those that have not yet fully adopted the HITRUST CSF, many are left with the task of choosing, adapting and implementing an existing information security control framework. Even those that have decided to fully adopt the CSF can sometimes struggle with its implementation. This is why HITRUST continues to develop and publish guidance and tools like the CSF assessment methodology and MyCSF as part of an overall risk management framework to help organizations implement and manage 'reasonable and appropriate' safeguards that demonstrate the level of due care and due diligence required to ensure 'adequate' protection of the sensitive information with which they are entrusted.

So, when HITRUST is asked how new regulations, standards, guidance and tools affect the value of the CSF and CSF-related tools, the answer is simple. The CSF, CSF Assurance Program and related methodologies and tools that make up the HITRUST RMF are needed more now than ever before.

# About HITRUST

Founded in 2007, HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from both the public and private sectors, HITRUST develops, maintains and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and assurance methodologies; and initiatives advancing cyber sharing, analysis and resilience.

HITRUST actively participates in many efforts in government advocacy, community building and cybersecurity education.

HITRUST is led by a seasoned management team and governed by a Board of Directors made up of leaders from across the healthcare industry and its supporters. These leaders represent the governance of the organization, but other founders also comprise the leadership to ensure the framework meets the short- and long-term needs of the entire industry.

For more information, visit www.HITRUSTalliance.net.

# MyCSF

MyCSF makes it easier and more cost-effective for an organization to manage information risk and meet international, federal and state regulations concerning privacy and security. The MyCSF tool provides global organizations of all sizes with a purposefully designed, and engineered SaaS solution for performing risk assessments, corrective action plan management, enhanced benchmarking and dashboards, and integration with major GRC platforms and the HITRUST Assessment XChange®. MyCSF is a solution that will support an organization's evolving assessment needs that align with managing risk in the changing cyber threat, information risk and global regulatory landscape.
For more information, visit www.hitrustalliance.net/MyCSF.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net