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

May 2014
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 Common Security Framework (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 did so 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 best 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 best practices that fully support the type of robust and comprehensive information protection program required under the HIPAA Security Rule. We also look 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 Statement on Standards for Attestation Engagements (SSAE) 16 Service Organization Control (SOC) 2 reports.

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

Introduction ................................................................. 1
Table of Contents .......................................................... 3
Frequently Asked Questions ................................................ 4

The HITRUST CSF ......................................................... 4
  Q. Why does healthcare need a security framework? ................. 4
  Q. What were the industry’s goals for the CSF? ....................... 5
  Q. How is the CSF structured? ......................................... 5
  Q. Is the CSF an industry standard for healthcare? .................. 6
  Q. Is the CSF a compliance-based or risk-based framework? ....... 7
  Q. Does the CSF take a “one size fits all” approach to information security? ......................................................... 7
  Q. Is the scope of the CSF too large for most healthcare organizations? ................................................................. 7
  Q. How does the CSF keep up with the rapidly changing cybersecurity landscape? ......................................................... 8

The CSF Assurance Program and Certification .......................... 9
  Q. Do HITRUST certification programs provide safe harbor in the event of a breach? .................................................. 9
  Q. Does the use of alternate controls diminish the value of HITRUST Certification? .................................................. 9
  Q. Does HITRUST rely too heavily on the Assessor’s opinion of control effectiveness? ................................................ 10
  Q. What methods are used to evaluate the effectiveness of CSF controls? ................................................................. 10
  Q. Does CSF Assurance take a compliance-based approach to information protection? ................................................ 10
  Q. Does CSF Assurance take a compliance approach and weight all controls equally? .................................................. 11
  Q. Can assessors use sampling to improve the efficiency of the assessment? ................................................................. 11
  Q. Is the HITRUST CSF Assurance Program a one-size-fits-all approach? ................................................................. 12
  Q. Are HITRUST assessments only useful for formal certification against the CSF? .................................................. 12
  Q. Does the CSF Assurance Program support an “assess once, report many” approach? .................................................. 12

The HITRUST RMF .......................................................... 13
  Q. Can risk be calculated based on a control’s maturity level? ................................................................. 13
  Q. Do non-contextual impact ratings for controls provide any real value? ............................................................... 14
  Q. How does the RMF fit into the NIST Framework for Critical Infrastructure Cybersecurity? ........................................ 14
Frequently Asked Questions

The HITRUST CSF

Q. 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 for 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 level 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 performed. (Not surprisingly, OCR’s focus for the second round of audits is risk analysis and risk management).
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).

Q. 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

Q. 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 was then structured along the lines of ISO 27001 with the 12 control clauses (or domains) and one additional control domain addressing the implementation of an Information Security Management Program, similar to that of the Information Security Management System of ISO 27001:2005.

- Control Objective – states the desired result or purpose of what is to be achieved
- Control Specification(s) – The policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management or legal nature to meet the Control Objective
- Implementation Requirement(s) – 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: 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; and any additional, but related, functionality to level 2 control and/or increase in the strength of a Level 2 control
- Control Audit Procedure – The activities to carry out the formal examination of the organization’s implementation of the Control Requirements. This is achieved through the examination of documentation, interviewing of organizational personnel and testing of the technical implementation
- Standard Mapping – The cross-reference between each Implementation Requirement level and the requirements and controls of other common standards and regulations

Q. 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.
Q. 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.

Q. 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 best 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.

Q. 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.
Q. How does the CSF keep up with the rapidly changing cybersecurity landscape?

HITRUST has established a cyber threat working group to collaborate with the HITRUST Cybersecurity Threat Intelligence and Incident Coordination Center (C3) to develop a threat catalog tied to the HITRUST CSF controls. By identifying the controls intended to address a particular threat, organizations can more easily consume threat intelligence and proactively address active and emerging threats. HITRUST will issue additional guidance to organizations regarding the CSF controls or any additional requirements when needed, as well as use the information to modify or update the CSF control requirements to address these threats.
The CSF Assurance Program and Certification

Q. 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 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.

The State of Texas also provides for the consideration of past compliance as a mitigating factor in the event of a data breach through the Texas 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.

Q. 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.

**Q. 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 CSF is not used. Before an assessor can become a HITRUST-certified CSF Assessor organization, it undergoes a vetting process for their assessment methods, and the experience and qualifications of their 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.

**Q. 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, then 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.

**Q. 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 shown on the following page:

- 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

Q. Does CSF Assurance take a compliance approach and 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 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, best 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 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—hence the introduction of impact codes—and their relationship with each other—hence 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.
Q. 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, for example by external auditors. HITRUST also provides guidance to CSF Assessor organizations on the use of sampling in the HITRUST CSF Assessment Methodology guide, and of course anyone can refer to multiple texts on the subject.

Q. 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. And the CSF Assurance Program is no different. The only impact tailoring may have is the ability to receive a certified assessment report as controls must meet certain implementation requirements (scores) for required controls. A 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 CSF Assurance Program subsequently provides a common, consistent and repeatable means of assessing organizations and sharing assurances with internal and external stakeholders, including regulators.

Q. 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 best 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.

Q. Does the 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 3rd 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 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.
The HITRUST RMF

Q. 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 Department of Defense control framework, estimates of the information’s confidentiality and criticality requirements can result in up to nine specific control baselines. The 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.

**Q. 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. The assets in question are information or systems of a specific type, i.e., ePHI and other information with similar confidentiality and criticality requirements. As a result, 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 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 an example of how an organization can help prioritize corrective actions for control deficiencies using these impact 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.

**Q. How does the RMF fit into the NIST Framework for Critical Infrastructure Cybersecurity?**
The HITRUST RMF, which consists of the CSF, CSF Assurance Program and supporting tools, methods and services, is actually a model implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity 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 Intelligence and Incident Coordination Center (C3) 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.

The HITRUST C3 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 providing monthly threat briefings and C3 alerts. In addition, HITRUST and HSS evaluates the industry's preparedness and HITRUST C3 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.