HITRUST
Health Information Trust Alliance

February 9, 2016

Via Cyberframework@nist.gov

Ms. Diane Honeycutt
Secretary
Computer Security Division
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Subject: Views on the Framework for Improving Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

On behalf of Health Information Trust Alliance (HITRUST), we appreciate the opportunity to provide comments to the National Institute of Standards and Technology's (NIST) request for information on the "Framework for Improving Critical Infrastructure Cybersecurity" ("NIST CsF").

HITRUST Background

HITRUST believes that information security should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. Although compliance with HIPAA was already required, the Security Rule's lack of prescriptiveness led to varying interpretations and implementations in controls and non-standard reporting to external parties, such as customers or business partners. In turn, organizations could not gain the confidence necessary to share information with each other without spending the time and resources to conduct proprietary, independent reviews of security.

An important element of HITRUST is that the requirements were not new, they were existing requirements molded into a common framework that applies and scales to all organizations in healthcare. Organizations in healthcare already had a multitude of security requirements and standards. By offering a framework that makes compliance with those requirements and standards easier and offering a way to assess and report that compliance in fewer steps with fewer resource expenditures, HITRUST has been able to grow the CSF and CSF Assurance Program—the principle components of the HITRUST Risk Management Framework (RMF)—into the most widely adopted security framework and certification program in healthcare. Without this level of standardization brought by HITRUST, organizations would not have a clear, common set of expectations for security, which in turn leads to increased costs and risk.

The HITRUST RMF provides the healthcare industry with a model implementation of the NIST CsF, and the HITRUST CSF provides a comprehensive, prescriptive yet flexible information security control framework that also helps healthcare organizations address the requirement for risk analysis by leveraging the risk analyses used to develop its supporting authoritative sources. And the CSF Assurance Program complements the CSF by providing a robust mechanism for sharing information security assurances with internal and external stakeholders in a consistent and repeatable way.

Collaboration with Government Agencies

Subsequently, HITRUST applauds the work NIST has done with its Cybersecurity Framework. The NIST CsF has increased "C-Suite" interest in information protection and has become a major driver in the private sector for implementing more robust cybersecurity programs specifically intended to address an ever-changing threat environment.

We support the healthcare industry working with the federal government and lawmakers to secure healthcare organizations' data assets, systems and medical devices, given that existing public-private efforts in these areas—including threat intelligence collaborations—are taken into account. These partnerships will work only if regulations and requirements are streamlined, and work to mitigate the risks and liabilities of those collaborating for the protection of industry data.

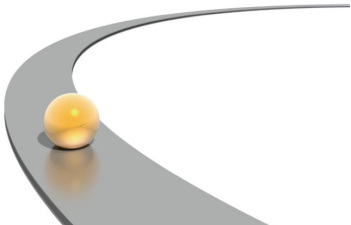
HITRUST has been working to engage in a meaningful dialogue with regulators for the better part of a decade to identify ways to incentivize entities to proactively implement comprehensive and effective information protection programs and standards. Our shared goal is to encourage strong information protection programs, while reducing the cost and complexities faced when complying with federal information protection regulations and associated audits.

Our Response

Although we address each of the 25 questions in the request for information (RFI), we would like to provide a summary of our responses in each of the four question categories.

Use of the Framework

HITRUST provides a Risk Management Framework (RMF) that helps healthcare organizations implement a robust and comprehensive information protection program that is fully consistent with the NIST CsF, including its recommendations for establishing or improving a cybersecurity program. A complete discussion of the relationship between the HITRUST RMF and NIST Framework Core, Implementation Tiers, Profiles and implementation and improvement guidance—all of which HITRUST has found to be very useful—can be found in the proposed *Healthcare Sector Cybersecurity Framework Implementation Guide*, which was recently submitted to the Joint Healthcare and Public Health (HPH) Cybersecurity Working Group (WG) for review.



The federal government should also require that any future regulations, standards and guidance be fully consistent with the NIT CsF, and that agencies review and, if needed, update any existing guidance for consistency. Incentives for voluntary private-sector use of the NIST CsF should be also be considered. HITRUST also supports healthcare organizations with multiple cybersecurity initiatives in partnership with federal agencies, including a federally-recognized Information Sharing and Analysis Organization (ISAO) that provides cyber threat intelligence sharing through Cyber Threat Exchange (CTX) and local, regional and national-level incident response exercises in concert with state and federal agencies through CyberRX.

Possible Framework Updates

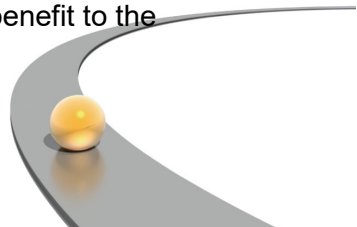
All guidance for information protection, including the NIST CsF, can become stale over time. Subsequently, HITRUST recommends NIST or other governing entities regularly review the Framework's content and update the Framework as needed to ensure it continues to remain relevant to the cyber threat environment. Specific areas that should be considered for improving the NIST CsF include the addition of HITRUST CSF mappings to the Framework Core's informative references and adding a section that specifically addresses how the NIST CsF can be leveraged by smaller, less mature organizations consistent with the recommendations outlined in NISTIR 7621, *Small Business Information Security: The Fundamentals*.

HITRUST also makes specific recommendations for most of the nine (9) areas identified by NIST in its Framework-related "Roadmap," such as providing a specific requirement and associated guidance for the use of strong authentication; mapping NIST controls to the recommendations for small business information security contained in NISTIR 7621; promoting private sector certification programs for the provision of third party assurances (e.g., SECURETexas); clarifying the similarities and differences between the NIST CsF and traditional RMFs like the one provided by NIST; discussing how the Framework relates to the Organization for International Standards (ISO) information security management system (ISMS), the focus of ISO 27001 certification; and providing a separate Framework Core Subcategory to address privacy engineering requirements.

By keeping the requirements high-level and consistent with industry best-practices, these and other updates to the NIST CsF would have minimal impact to those currently using it. Real changes would occur in frameworks and guidance that exist at a lower level and are more specific to a particular sector or sub-sector, such as with the NIST and HITRUST RMFs.

Sharing Information on Using the Framework

HITRUST has found direct consultation on the NIST CsF has been most useful in the integration of the NIST Framework into the HITRUST RMF. We've also found the NIST CsF Industry Resources Website helpful, albeit the information referenced must be vetted and approved by NIST. However, HITRUST believes more collaborative forums that promote the free exchange of ideas and examples (e.g., use cases, case studies) would provide an additional benefit to the



private sector. NIST could also sponsor regional and/or sector-specific workshops or "user groups" to help facilitate the private sector's implementation of the NIST Framework.

Private Sector Involvement in the Future Governance of the Framework

Given the intent of the Framework is to provide guidance to critical infrastructure industries, which are predominantly owned and operated by the private sector, the private sector should be equally, if not primarily, responsible for governance and the maintenance of the Framework. The NIST CsF could be transitioned to a not-for-profit enterprise modeled after a standards organization like ISO or the American National Standards Institute (ANSI). External participation by external organizations and individuals—national or international—would be voluntary; however, a membership fee structure for organizations could be implemented to help make the organization self-sustaining. Given the high-level nature of the NIST CsF and the relative infrequency of its update (ostensibly annually), transitioning governance and maintenance to a private-sector entity would likely have minimal impact on users of the Framework.

Responses to Specific Questions

Responses from HITRUST to these questions are provided in consideration of the HITRUST Risk Management Framework (RMF)—a model implementation of the NIST CsF—as it's related to the question, and where possible, observations and feedback from the industry.

Use of the Framework

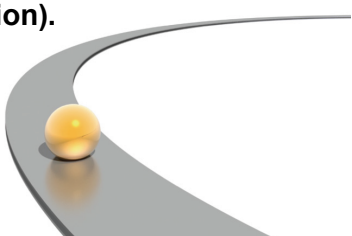
Q1. Describe your organization and its interest in the Framework.

The HITRUST RMF, which consists of the CSF, CSF Assurance Program and supporting methodologies, tools and services, provides a model implementation of the NIST CsF for the healthcare industry. Along with the Office of the Chief Privacy Officer at the Office of the National Coordination in the Department of Health and Human Services, HITRUST also co-chairs the Risk Management Sub-working Group of the Joint HPH Cybersecurity WG, which developed the draft *Healthcare Sector Cybersecurity Framework Implementation Guide* under the auspices of the Critical Infrastructure Protection Program.

Q2. Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.

HITRUST is a user of the Framework in that it integrates the NIST CsF into the HITRUST RMF, which is used by a significant number of organizations in the healthcare industry as the basis of their information protection programs.

Q3. If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).



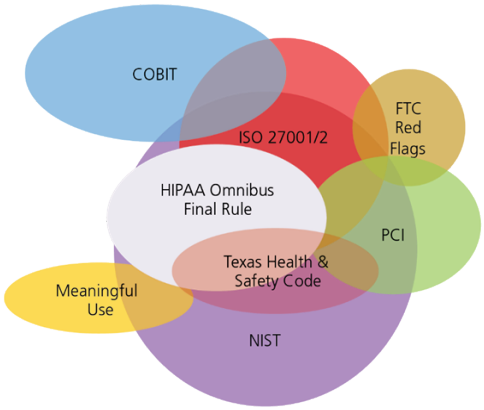
In addition to its incorporation in the HITRUST RMF for use by any and all healthcare organizations (see also our response to Q4), HITRUST uses the NIST CsF through its own internal implementation of the HITRUST RMF, including the certification of its host provider for the GRC-based MyCSF assessment support tool.

Q4. What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, [and] Privacy Methodology)?

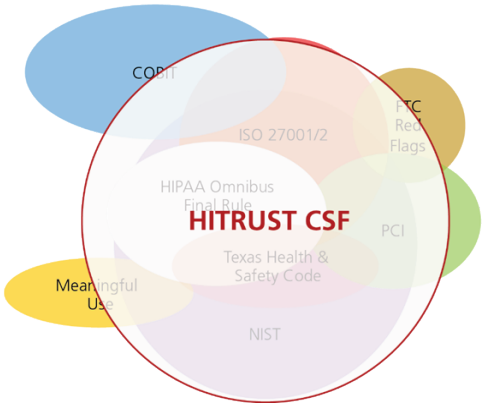
Core

The HITRUST RMF provides a risk-based control framework, the CSF, that provides an integrated, harmonized set of requirements tailored specifically for the healthcare industry by the healthcare industry, and which is updated at least annually to keep the controls current and relevant.

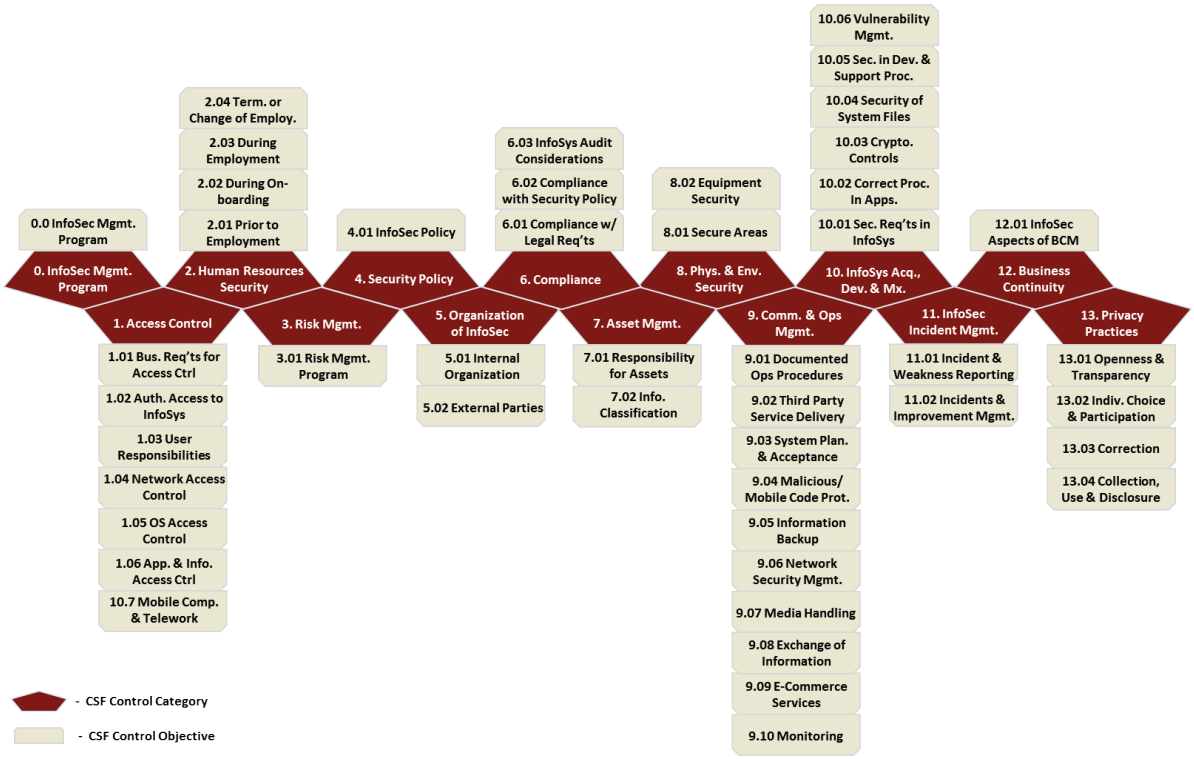
Healthcare sector organizations are subject to multiple legislative, regulatory, and other relevant requirements, including commonly accepted best practice standards. However, these "authoritative sources" often overlap in depth and breadth of their requirements as shown in the following figure, which, when integrated and harmonized, can often be mutually reinforcing when intelligently applied in the intended environment.



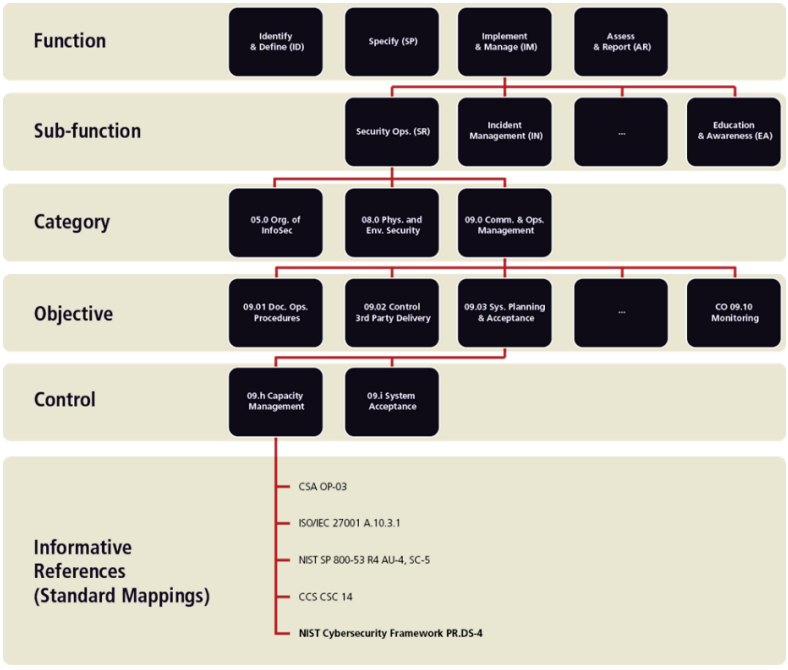
Industry working groups, supported by prominent healthcare organizations and led by HITRUST, integrated and harmonized these requirements by using ISO/IEC 27001:2005 as the basis for the CSF structure and adding in ISO/IEC 27002:2005, HIPAA, NIST SP 800-53 and other requirements. Today, the HITRUST CSF integrates, harmonizes, and tailors more than two dozen authoritative sources, including the NIST CsF. This allows Sector organizations to implement a single, comprehensive, prescriptive, healthcare-specific control framework to meet healthcare clinical and business objectives and satisfy multiple regulatory and other compliance requirements, as shown in the next figure, and ultimately meet due care and due diligence requirements for the adequate protection of health information.



Structurally, the HITRUST CSF contains 149 security and privacy controls parsed amongst 46 control objectives within 14 broad control categories (similar to the control families in NIST SP 800-53).

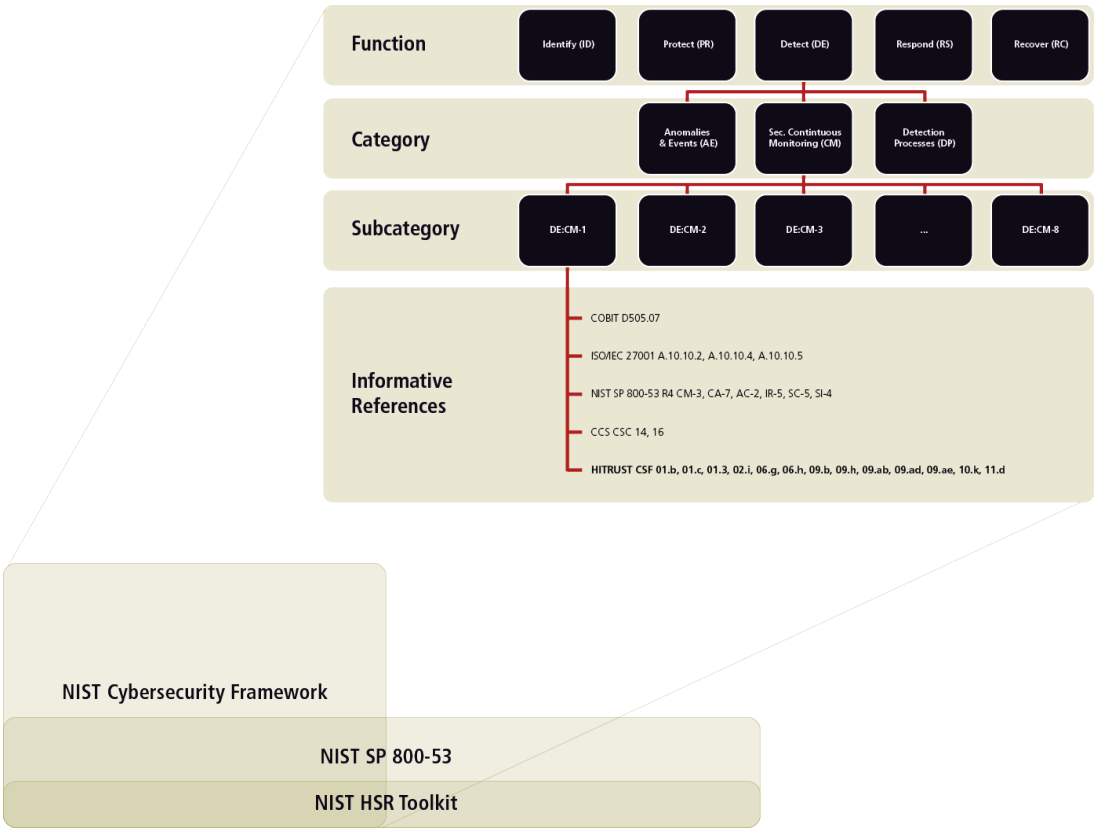


Each control has up to three implementation levels with requirements of increasing rigor and/or specificity that are broadly applicable to Healthcare Sector organizations. These levels are further supplemented by industry segments that provide specialized requirements for specific types of organizations (e.g., Health Information Exchanges, HIEs) and data (e.g., Payment Card Information, PCI). And although the HITRUST CSF is based on what may be referred to as a traditional cybersecurity risk management framework, ISO 27001, the HITRUST RMF can be represented structurally in the same manner as the NIST CsF, as seen in the figure on the following page.

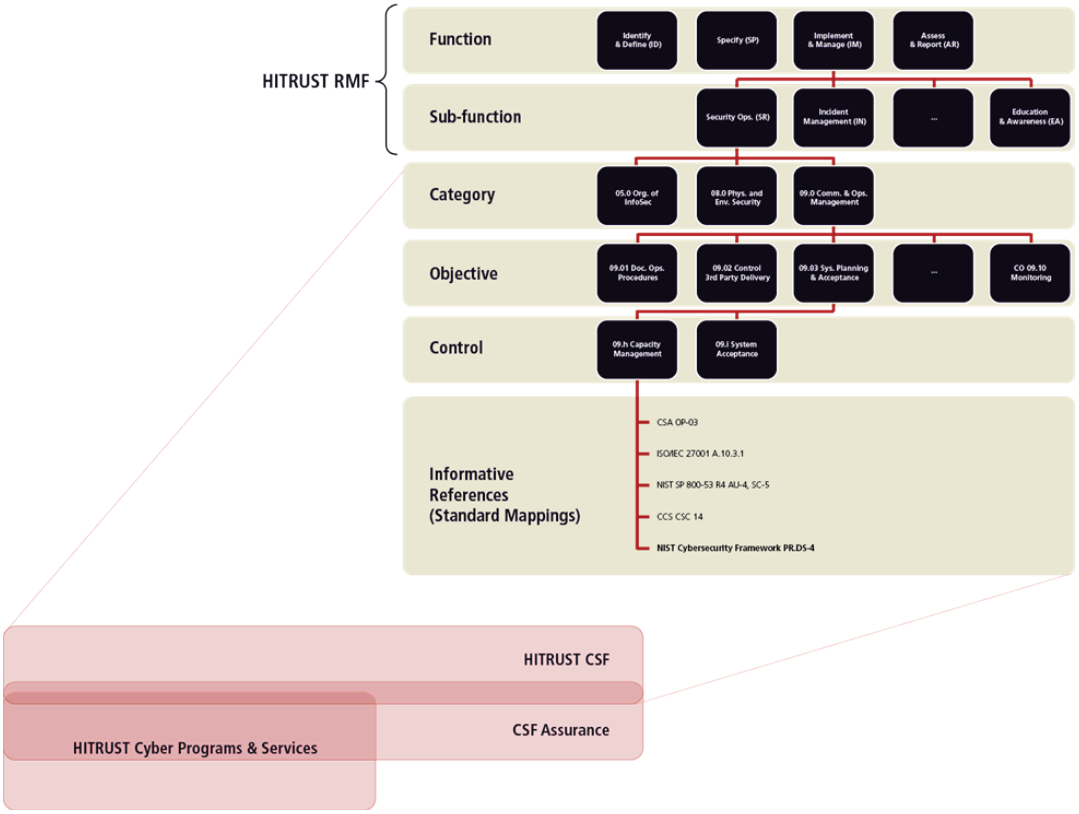


But there are a few differences between the two frameworks as depicted. One is that the functions and sub-functions listed in the figure are described in the HITRUST RMF, and the categories, objectives, controls, and standard mappings are contained in the HITRUST CSF itself. Another is that the HITRUST CSF provides a harmonized set of detailed control specifications (requirements) specific to the healthcare industry and provides standard mappings to the authoritative sources that inform those requirements, whereas the NIST CsF incorporates these as potential control requirements only by reference. A complete mapping of the HITRUST 2014 CSF v7 controls to the NIST CsF subcategories is available through the NIST CsF Industry Resources Website.

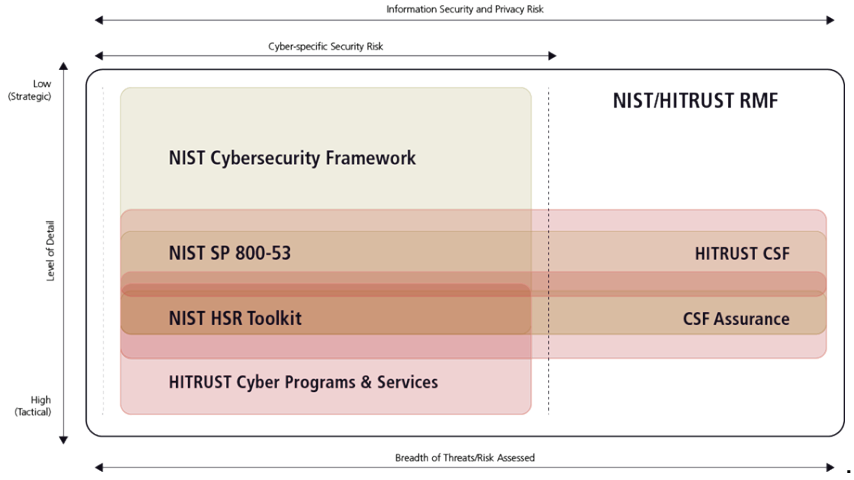
One can now represent the depth and breadth of coverage of the NIST CsF, which is arguably supported by the controls in NIST SP 800-53, and—because we're speaking to the Healthcare Sector—the NIST HIPAA Security Rule (HSR) Toolkit as shown in Figure 10. Note, one could also incorporate other tools such as the DHHS Security Risk Assessment (SRA) Toolkit at this level.



And, as with the NIST CsF, the HITRUST CSF can be similarly represented for depth and breadth of coverage. HITRUST provides industry-specific cyber intelligence and provides a mechanism for organizations to share information and collaborate on responses to specific incidents. These capabilities are included in the figure that follows, as they directly support the incident management process used by the NIST CsF to categorize cybersecurity activities (controls or safeguards) according to defined functions and sub-functions.



One can now compare the HITRUST RMF to the NIST CSF with respect to the level of detail (depth) provided, from the tactical to the strategic, and the breadth of the threats and risks addressed, as shown.



In addition, the HITRUST CSF and CSF Assurance Program fully supports a common, consistent mechanism for the communication of risk information to stakeholders, including third parties, as required by the NIST CsF. Also, continuous updating of prescriptive CSF

implementation specifications provide additional information to address "gaps" in the NIST CsF, as recommended.

Implementation Tiers

Both frameworks employ a maturity model, although the HITRUST RMF model is focused at a lower, more granular level than the model proposed by the NIST CsF. HITRUST's approach is based on a control maturity model described in NIST Interagency Report (IR) 7358, Program Review of Information Security Management Assistance (PRISMA), which provides five levels roughly similar to the Carnegie Melon Software Engineering Institute's (CM-SEI's) Capability Maturity Model Integrated (CMMI) process improvement model.

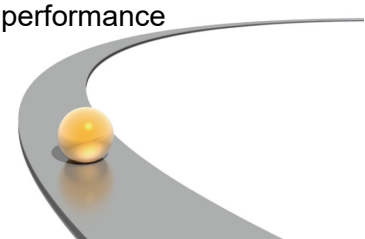
Like the PRISMA model, the HITRUST model's first three levels provide rough equivalence with traditional compliance-based assessments. First, control requirements must be clearly understood at all levels of the organization through documented policies or standards that are communicated with all stakeholders. Second, procedures must be in place to support the actual implementation of required controls. And third, the controls must be fully implemented and tested as required to ensure they operate as intended. These three levels essentially address the concept of design effectiveness. HITRUST then modified the PRISMA model to specifically incorporate the concept of "you can't manage what you don't measure." The model's last two levels address the concept of operational effectiveness.

In the initial maturity level, Policy, the assessor examines the existence of current, documented information security policies or standards in the organization's information security program to determine if they fully address the control's implementation specifications. For example, if a particular requirement statement has multiple actions associated with it, does a corporate policy or standard address all five elements, either directly in the policy or indirectly by reference to an external standard? And, does the policy apply to all organizational units and systems within scope of the assessment?

The second maturity level, Procedures, reviews the existence of documented procedures or processes developed from the policies or standards to determine if they reasonably apply to the organizational units and systems within scope of the assessment. For example, are there one or more written procedures that address the implementation of all elements in a particular requirement statement?

The third maturity level, Implemented, reviews the implementation of the policies and procedures to ensure the control's implementation specifications are applied to all organizational units and systems within scope of the assessment. For example, are all elements of a particular requirement addressed by the implementation for all corporate shared services?

The fourth maturity level, Measured, reviews the testing or measurement (metrics) of the specification's implementation to determine if they continue to remain effective. This idea of monitoring is not new, as the AICPA lists monitoring, i.e., the process of assessing performance



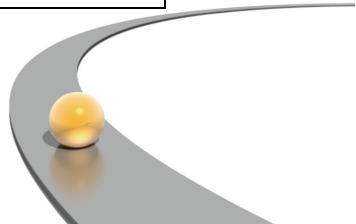
over time, as one of five interrelated components of internal control. However, the concept of continuous monitoring, upon which this level is based, is relatively new. NIST equates continuous monitoring with maintaining ongoing awareness to support organizational risk decisions.

The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions that adequately protect organization information. Thus, testing of the control to support an annual assessment or audit will likely not satisfy this requirement for many, if not most, controls. Instead, an organization must routinely measure and track this information over time. For example, an organization may use a management console to track antivirus software implementation status in near real-time and produce metrics of the percentage of end-user devices that have the latest software and signature updates.

The highest maturity level, Managed, reviews the organization’s management of its control implementations based on these metrics. For example, if common or special variations are discovered through testing or measurement of a control’s effectiveness, such as the antivirus deployment described earlier, can the organization demonstrate it has a management process for this metric and, when general or special variations occur, can it show it has performed a root cause analysis and taken corrective action based on the results?

The following table provides a bulleted list of general requirements for an organization to fully achieve each of the five HITRUST maturity levels.

Maturity Level	Points	General Requirements
Policy	25 pts	• Formal, up-to-date documented policies or standards stated as "shall" or “will” statements exist and are readily available to employees • Policies or standards establish a continuing cycle of assessing risk and implementation and uses monitoring for program effectiveness • Policies or standards are written to cover all facilities and operations and/or systems within scope of the assessment • Policies or standards are approved by key affected parties • Policies or standards delineate the information security management structure, clearly assign information security responsibilities, and lay the foundation necessary to reliably measure progress and compliance • Policies or standards identify specific penalties and disciplinary actions to be used if the policy is not followed
Procedures	25 pts	• Formal, up-to-date, documented procedures are provided to implement the security controls identified by the defined policies • Procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed

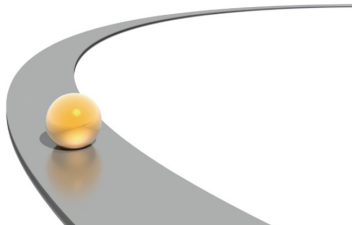


Maturity Level	Points	General Requirements
		• Procedures clearly define information security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and information technology personnel, (3) management, and (4) information security administrators • Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance • Procedures document the implementation of and the rigor in which the control is applied • Procedures are communicated to individuals who are required to follow them
Implemented	25 pts	• Information security procedures and controls are implemented in a consistent manner everywhere that the procedure applies and are reinforced through training • Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged • Initial testing is performed to ensure controls are operating as intended
Measured	15 pts	• Tests are routinely conducted to evaluate the adequacy and effectiveness of all implementations • Tests ensure that all policies, procedures, and controls are acting as intended, and that they ensure the appropriate information security level • Self-assessments, a type of test that can be performed by organization staff, by contractors, or others engaged by management, are routinely conducted to evaluate the adequacy and effectiveness of all implementations • Independent audits are an important check on organization performance, but are not to be viewed as a substitute for evaluations initiated by organizational management • Information gleaned from records of potential and actual information security incidents and from security alerts, such as those issued by software vendors, are considered measurements. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risk • Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented • The frequency and rigor with which individual controls are tested depend on the risks that will be posed if the controls are not operating effectively • Threats are continually re-evaluated • Costs and benefits of information security are measured as precisely as practicable • Status metrics for the information security program as well as individual information security investment performance measures are established

Maturity Level	Points	General Requirements
Managed	10 pts	• Effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual information security incidents or through information security alerts issued by US-CERT, vendors, and other trusted sources • Policies, procedures, implementations, and tests are continually reviewed and improvements are made • Information security is integrated into capital project/budget planning processes • An active enterprise-wide information security program achieves cost-effective information security • Security vulnerabilities are understood and managed • Controls are adapted to emerging threats and the changing information security environment • Decision-making is based on cost, risk, and mission impact • Additional or more cost-effective information security alternatives are identified as the need arises • Status metrics for the information security program as well as individual information security investment performance measures are met

The control maturity model also incorporates the following 5-point compliance scale which is used to rate each level in the model: Non-Compliant (NC), Somewhat Compliant (SC), Partially Compliant (PC), Mostly Compliant (MC) and Fully Compliant (FC).

Score	%	Description
Non-Compliant (NC)	0%	Very few, if any, of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or managed). Rough numeric equivalent of 0% (point estimate) or 0% to 12% (interval estimate).
Somewhat Compliant (SC)	25%	Some of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or managed). Rough numeric equivalent of 25% (point estimate) or 13% to 37% (interval estimate).
Partially Compliant (PC)	50%	About half of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or managed). Rough numeric equivalent of 50% (point estimate) or 38% to 62% (interval estimate).
Mostly Compliant (MC)	75%	Many, but not all, of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or managed). Rough numeric equivalent of 75% (point estimate) or 63% to 87% (interval estimate).
Fully Compliant (FC)	100%	Most, if not all, of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or



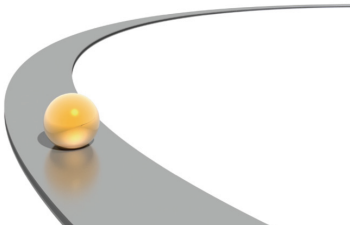
Score	%	Description
		managed). Rough numeric equivalent of 100% (point estimate) or 88% to 100% (interval estimate).

As currently used in the HITRUST CSF Assurance Program, the PRISMA-based maturity scores are converted to a 15-level maturity rating for CSF certification, as shown.

Maturity Level	1	1	1+	2	2	2+	3	3	3+	4	4	4+	5	5	5+
Cutoff Score	< 10	< 19	< 27	< 36	< 45	< 53	< 62	< 71	< 79	< 83	< 87	< 90	< 94	< 98	< 100

General definitions for each of the 15 maturity ratings are provided on the following page.

Maturity Level	Rating Description
Level 1	**Few if any** of the control specifications included in the assessment scope are defined in a policy or standard and may not be implemented as required by the HITRUST CSF.
Level 1	**Many** of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 1+	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 2	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, but **few, if any,** of the requirements are supported with organizational procedures or implemented as required by the CSF.
Level 2	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, **many** of the requirements are supported with organizational procedures, but **few, if any,** are implemented as required by the CSF.
Level 2+	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, but **few, if any,** are implemented as required by the CSF.
Level 3	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and **some** are implemented as required by the CSF.
Level 3	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and **many** are implemented as required by the CSF.
Level 3+	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, supported with organizational procedures, and implemented as required by the CSF.
Level 4	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes and implemented, and **some** of these control specifications are routinely measured to ensure they function as intended and as required by the CSF.



Maturity Level	Rating Description
Level 4	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes and implemented, and **many** of these control specifications are routinely measured to ensure they function as intended and as required by the CSF.
Level 4+	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured to ensure they function as intended and as required by the CSF.
Level 5	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and **some** are actively managed to ensure they continue to function as intended and as required by the CSF.
Level 5	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and **many** are actively managed to ensure they continue to function as intended and as required by the CSF.
Level 5+	**Most, if not all,** of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, routinely measured, and actively managed to ensure they continue to function as intended and as required by the CSF.

Although there are differences in how the NIST CsF and HITRUST RMF approach evaluation of an organization's level of maturity, their similarities allow for a direct comparison. The next table provides rough approximations as to how an organization would likely score on a HITRUST CSF assessment for a given organizational-level tier in the NIST CsF.

NIST CsF Tiers	Cybersecurity Implementation Tier Description	Approximate HITRUST Maturity Levels	Approx. HITRUST Maturity Rating
Tier 0: Partial	Organization has not yet implemented a formal, threat-aware risk management process and may implement some portions of the framework on an irregular, case-by-case basis; may not have capability to share cybersecurity information internally and might not have processes in place to participate, coordinate or collaborate with other entities.	Level 1 – Partial* Level 2 – Partial Level 3 – Partial Level 4 – Non-compliant Level 5 – Non-compliant	1 to 3-
Tier 1: Risk-Informed	Organization uses a formal, threat-aware risk management process to develop [target] profile [control requirements]; formal, approved processes and procedures are defined and implemented; adequate training & resources exist for cybersecurity; organization aware of	Level 1 – Partial Level 2 – Compliant Level 3 – Compliant Level 4 – Non-compliant Level 5 – Non-compliant	3- to 3+

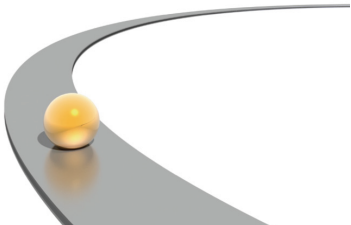
NIST CsF Tiers	Cybersecurity Implementation Tier Description	Approximate HITRUST Maturity Levels	Approx. HITRUST Maturity Rating
	role in “ecosystem” but has not formalized capabilities to interact/share info externally.		
Tier 2: Repeatable	Organization regularly updates [target] profile [control requirements] due to changing threats; risk-informed policies, processes and procedures are defined, implemented as intended, and validated; consistent methods are in place to provide updates when a risk change occurs; personnel have adequate skills & knowledge to perform tasks; organization understands dependencies/partners and can consume information from these partners.	Level 1 – Compliant Level 2 – Compliant Level 3 – Compliant Level 4 – Partial Level 5 – Partial	4- to 5-
Tier 3: Adaptive	Organization proactively updates [target] profile [control requirements] based on predictive indicators; actively adapts to changing/evolving cyber threats; risk-informed decisions are part of organizational culture; manages and actively shares information with partners to ensure accurate, current information is distributed and consumed to improve cybersecurity before an event occurs.	Level 1 – Compliant Level 2 – Compliant Level 3 – Compliant Level 4 – Compliant Level 5 – Compliant	5 to 5+

*Refers to any of three “partial” levels of compliance, from somewhat compliant (SC) to mostly compliant (MC).

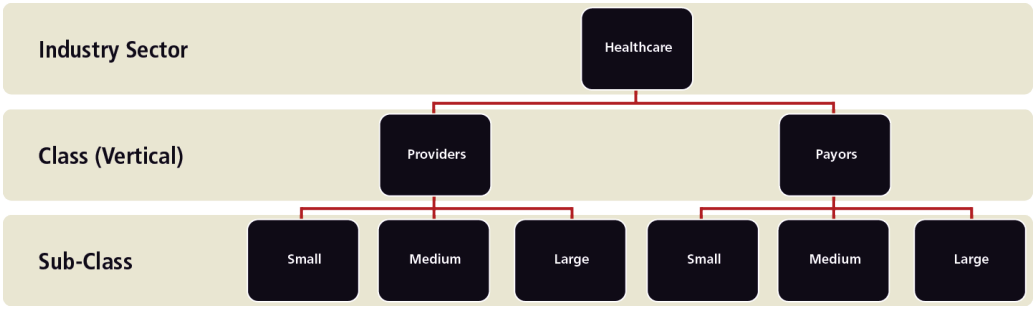
HITRUST further expands on the evaluation of maturity by proposing a multidimensional model that considers an organization’s implementation of specific classes of cyber-relevant controls, overall risk management, and its ability to consume, share, and ultimately act upon threat intelligence in a meaningful way.

Profiles

In developing the CSF, HITRUST integrated and harmonized requirements from multiple healthcare-related authoritative sources and applied the tailoring process to create an overlay, which constitutes an initial control baseline for the healthcare industry. At this point, healthcare organizations would be expected to further tailor this baseline to address their specific needs. However, HITRUST helps organizations with this tailoring process by using specific risk factors to tailor the initial comprehensive baseline and create new overlays—essentially new baselines—for specific sub-classes of organizations that are defined by those factors.



HITRUST does this by defining healthcare as the industry sector and verticals within healthcare, such as providers and payers, as classes within the sector. One may then examine what makes these classes different and tailor a baseline defined for healthcare into multiple overlays, one for each class of healthcare. However, not all organizations within a common vertical will present the same risks. For example, the risks posed by a large, geographically-diverse health system that exchanges information with multiple business partners may not present the same level of risk as a small, independent community clinic with no information exchange. Thus, healthcare organizations within a vertical or class may be further subdivided based on other criteria, such as their size, the type of architectures and/or technologies in the environment, and the type of regulatory and other requirements to which healthcare organizations may be subject. The following is a graphical depiction of what this would look like if, for example, subclasses for payers and providers were limited to small, medium, and large organizations.



The key to creating the sub-classes is to identify risk factors—essentially characteristics used in risk models as inputs to determine levels of risk in a risk assessment—that will provide a reasonable and meaningful categorization of relative risk between sub-classes, so that the resulting baselines present an appropriate number and rigor of controls to reduce the residual risk for each subcategory to a similar level. Risk models define the risk factors and the relationships among those factors. Risk factors are also used extensively in risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts. Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition.

NIST defines a predisposing condition as one that “exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operations, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, [or] other organizations.”

Examples are provided in the following table.

Predisposing Conditions		
Type	**Example**	**Effect on Risk**
Physical	Flood Plain	Increased likelihood of exposure to hurricanes or floods
Technical	Stand-alone System	Decreased likelihood of exposure to a network-based attack
Administrative	Gap in Contingency Plans	Increased likelihood of exposure to a disruption in operations

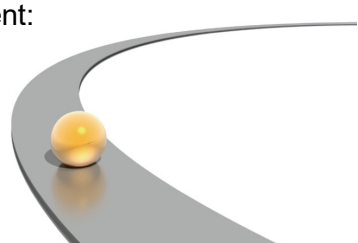
HITRUST leverages this concept of predisposing conditions along with scoping considerations (e.g., system functionality and public access in the operational environment) to define specific risk factors based on the amount and type of information processed or held by an organization, characteristics of its technology and architecture, and its legislative, regulatory, and contractual requirements, which can then be used to define industry subclasses, and create their respective overlays.

In the HITRUST CSF, these organizational, system, and regulatory factors are used to determine up to three implementation levels per control for generally applicable protection requirements and multiple industry segments for unique requirements, such as those for Health Insurance Exchanges (HIXs), to address increasing levels of inherent risk.

The three classes of risk factors and their constituent elements are as follows:

- **Organizational Factors:** The Organizational Factors are defined based on the size of the organization and complexity of the environment as follows:
  - Record Count
    - All – Total Number of Records Held
    - All – Total Number of Records Processed Annually
  - Volume of business (Used if record count cannot be determined)
    - Health Plan / Insurance – Number of Covered Lives
    - Medical Facilities / Hospital – Number of Licensed Beds
    - Pharmacy Companies – Number of Prescriptions Per Year
    - Physician Practice – Number of Visits Per Year
    - Third Party Processor – Number of Records Processed Per Year
    - Biotech Companies – Annual Spend on Research and Development
    - IT Service Provider / Vendor – Number of Employees
    - Health Information Exchange – Number of Transactions Per Year
  - Geographic scope
    - State
    - Multi-state
    - Off-shore (outside U.S.)

- **Regulatory Factors:** The regulatory factors are defined based on the compliance requirements applicable to an organization and systems in its environment:

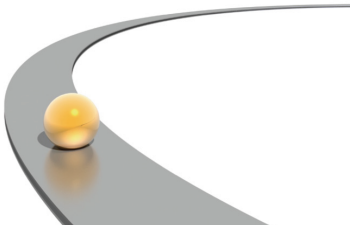


  - Subject to PCI Compliance
  - Subject to FISMA Compliance
  - Subject to FTC Red Flags Rules
  - Subject to the State of Massachusetts Data Protection Act
  - Subject to the State of Nevada Security of Personal Information Requirements
  - Subject to the State of Texas Medical Records Privacy Act
  - Subject to Joint Commission Accreditation
  - Subject to CMS Minimum Security Requirements (High-level Baseline)
  - Subject to MARS-E Requirements
  - Subject to FTI Requirements

- **System Factors:** The system factors are defined considering various system attributes that would increase the likelihood or impact of a vulnerability being exploited. These factors are to be assessed for each system or system grouping to determine the associated level of control.
  - Stores, processes, or transmits PHI
  - Accessible from the Internet
  - Accessible by a third party
  - Exchanges data with a third party/business partner
  - Publicly accessible
  - Mobile devices are used
  - Connects with or exchanges data with a Health Information Exchange (HIE)
  - Number of interfaces to other systems
  - Number of users
  - Number of transactions per day

For example, an organization might need to specify Level 2 implementation requirements for a system if it processes ePHI AND includes at least one of the other system factors associated with the control. Suppose a system is accessible from the Internet, exchanges data with a business partner, and has the Level 2 threshold number of users, but DOES NOT process ePHI. The organization would only need to address Level 1 implementation requirements for this system. However, if another system DOES process ePHI AND is accessible from the Internet, then the organization would need to address any additional requirements specified in Level 2.

If a control contains more than one category of factors, the organization must adhere to the highest level of implementation requirements driven by the factors. For example, if a health plan is at the Level 2 threshold for a control based on the total number of records held, but must also be FISMA compliant (implementing and adhering to the controls specified in NIST SP 800-53), the organization must implement the Level 3 requirements of the CSF if FISMA is a Level 3 regulatory factor for that control.



In this way, users of the CSF are able to create—in a very dynamic way—a custom baseline for their subclass of healthcare organizations based on their applicable risk factors. However, organizations are expected to then tailor these subclass-specific baselines (overlays) generated from the application of these risk factors. Fortunately, the problem-space has been reduced to something more manageable, and the process is relatively straightforward. Organizations should (1) identify and designate common controls in the baseline; (2) apply scoping considerations to the remaining baseline security controls; (3) select alternate (compensating) controls, if needed; (4) assign specific parameters if a control doesn't provide them; (5) supplement the baseline with additional control requirements, if needed; and (6) provide additional information to support implementation, if needed.

This tailoring of a minimum security baseline such as the HITRUST CSF to create an organizational overlay is consistent with HIPAA requirements for reasonable and appropriate protection, as HIPAA also states covered entities and business associates may "use any security measures that … reasonably and appropriately implement the standards and implementation specifications" by taking into consideration its size, complexity, and capabilities; its technical infrastructure, hardware and software security capabilities; the costs of security measures, and the probability and criticality of potential risks to ePHI. Note, risk analysis is one of those implementation specifications.

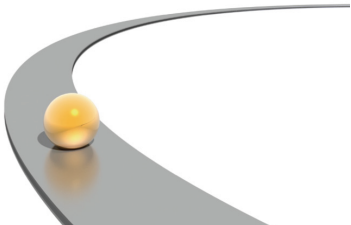
These new baselines then become the Target Profile as defined by the NIST CsF, and assessments against the Target Profile will help organizations identify their Current Profile and the gaps between the two.

Privacy Methodology

The HITRUST CSF fully integrates HIPAA Privacy Rule requirements along with additional control requirements from the privacy catalog contained in NIST SP 800-53 r4 Appendix J. The HITRUST RMF is also used by the Texas Health Services Authority to support SECURETexas, the first state-recognized covered entity security and privacy certification in the country. Subsequently, the HITRUST CsF also includes requirements from other federal and state privacy legislation, regulations and guidance (e.g., IRS Pub 1075 for federal tax information), which are specified in Title 1 Texas Administrative Code § 390.2.

Q5. What portions of the Framework are most useful?

The NIST Framework Core and Profiles are arguably its most useful elements. It ensures an organization address the breadth of the threat environment through the use of an incident management process model and conduct a gap analysis between the current and target state of its program. The implementing organization determines the target state (profile) based on a traditional risk analysis (as required under HIPAA and recommended by HHS for the healthcare industry) or by leveraging a control-based risk management framework such as NIST or



HITRUST. The informative references also provide helpful guidance on the types of controls an organization should consider when selecting controls for its target state.

Q6. What portions of the Framework are least useful?

The Framework Implementation Tier model is probably the least useful due to the lack of a mechanism to evaluate and score an organization against the model. HITRUST recognizes that NIST does not consider the Tiers to represent maturity levels and that progression to higher Tiers should only be encouraged when such a change would reduce cybersecurity risk cost-effectively. However, HITRUST provides a mechanism for evaluating an organization against the Tiers' criteria through the evaluation of information security and privacy controls against a NIST PRISMA-based maturity model (as discussed in Q4).

Q7. Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?

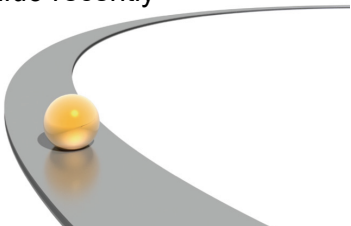
HITRUST has ensured all elements of the NIST CsF have been incorporated into the HITRUST RMF, including addressing the NIST CsF privacy recommendations through incorporation of the HIPAA Privacy Rule and the NIST SP 800-53 r4 Appendix J Privacy Catalog into the HITRUST CSF.

Q8. To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.

As the HITRUST RMF has always incorporated multiple regulatory and best practice frameworks, including NIST (e.g., the NIST SP 800-53 moderate-level control baseline and the maturity-based approach to control assessment described in NISTIR 7358, *Program Review for Information Security Management Assistance (PRISMA)*), the NIST CsF did little to help further reduce cybersecurity risk for those organizations that fully leverage the HITRUST RMF. However, what the NIST CsF did to reduce cybersecurity risk in the industry was raise awareness for organizations around the need to comprehensively address cyber risks and increase emphasis on impact-reducing practices such as security incident response and business continuity management to help improve cyber resilience.

Q9. What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?

Sector-specific agencies (SSAs) in the Federal government should be required to develop guidance, if they choose to do so, or formally recognize private-sector guidance that is consistent with the NIST CsF and any additional guidance produced by the Critical Infrastructure Protection Program (CIPP), e.g., the various sector-wide implementation guides. One example is the *Healthcare Sector Cybersecurity Framework Implementation Guide* recently



submitted to the Joint HPH Cybersecurity WG. Such recognition should include specific incentives for the use of such guidance by implementing organizations, such as mandatory caps on fines and penalties in the event of a breach, if the implementation of such guidance is done in good faith.

Possible Framework Updates

Q10. Should the Framework be updated? Why or why not?

All frameworks become "stale" over time and should be periodically re-evaluated and updated to ensure it continues to be relevant to a changing threat environment and provide for the adequate protection of sensitive information.

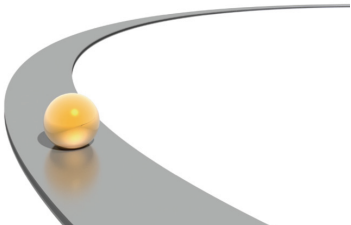
Q11. What portions of the Framework (if any) should be changed or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.

Since the Framework intentionally exists at a relatively high-level to provide applicability across national boundaries and industry sectors, it should be updated to emphasize that it cannot be the only framework or approach used by an organization to implement its information protection program. Although examples of the additional specificity required to address a sub-category in the NIST CsF are provided in the informative references, and risk assessment is a critical step in the implementation process, many organizations still do not fully understand the need to enumerate threats and vulnerabilities, identify and rank risks, and develop a comprehensive set of risk responses—including the complete specification of information security and privacy controls to mitigate excessive residual risk. Additional information on control tailoring and the production of organizational overlays, such as those described in the NIST RMF and produced in the HITRUST CSF, should also be included.

The Framework should also be updated to reflect those threats it does not address along with the control references to NIST, HITRUST and other frameworks that are intended to address those threats. Otherwise an organization may not implement a comprehensive information protection program that addresses threats from other sources besides malicious human threat actors, e.g., natural threats and non-malicious threat actors such as the well-meaning but misguided employee.

Q12. Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?

The HITRUST CSF is the most widely used control framework in the healthcare industry, and the HITRUST RMF is one of the most comprehensive and mature sector-wide implementations of the NIST CsF in any critical infrastructure industry. Therefore, the NIST CsF-to-HITRUST



CSF mappings contained in the *Healthcare Sector Cybersecurity Framework Implementation Guide* should be incorporated into the NIST CsF document's references.

NIST may also wish to formally incorporate privacy into the Framework Core beyond its reference in NIST Subcategory ID-GV-3. A separate subcategory for privacy that specifically addresses privacy engineering, mapped to appropriate NIST, CSF and other privacy controls, could help ensure privacy concerns are better integrated into an organization's information protection program. It may also be useful to provide an additional table that maps Framework Core Subcategories to supporting NIST, ISO, and other documentation (down to the chapter and appendix-level if needed) to refer users of the Framework to more descriptive guidance (in in addition to the control-level mappings currently provided in Table 2: Framework Core).

And finally, NIST should consider expanding on the ability of organizations of all sizes and maturities to implement the Framework. HITRUST recommends adding a section to the Framework document that specifically addresses how small, less mature organizations can implement the framework consistent with the recommendations outlined in NISTIR 7621, *Small Business Information Security: The Fundamentals*. A mapping of NIST controls to the recommendations contained in NISTIR 7621 might also prove helpful.

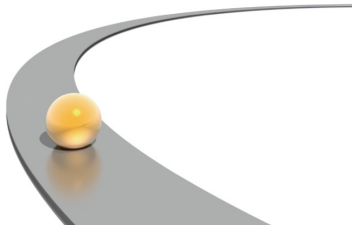
Q13. Are there approaches undertaken by organizations—including those documented in sector-wide implementation guides—that could help other sectors or organizations if they were incorporated into the Framework?

The HITRUST RMF forms the basis of the draft *Healthcare Sector Cybersecurity Implementation Guide* and modifies the NIST CsF guidance for establishing or improving a cybersecurity program to fully leverage the use of a control-based RMF such as those provided by NIST and HITRUST. It does so by categorizing the organization's information systems and identifying a tailorable control baseline for its Target Profile. By conducting a controls assessment against the Target Profile, the organization is able to determine its Current Profile and perform the gap analysis needed to develop appropriate risk responses, including the remediation of control deficiencies to help minimize any excessive residual risk.

Q14. Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?

In general, recommend adding content to the Framework document that addresses these additional areas as follows:

Area 4.1 Authentication: Specifically address strong authentication in a Framework Core subcategory and provide guidance on the use of strong and risk-based authentication in the document; consider adding specific sections to provide guidance around each of the Framework Core categories similar to the approach used in NISTIR 7621, *Small Business Information Security: The Fundamentals*.



Area 4.2 Automated Indicator Sharing: No recommendation at this time.

Area 4.3 Conformity Assessment: Work with private-sector certification bodies like HITRUST that implement the NIST CsF and actively promote such programs in the Framework as a means of providing assurances to internal and external stakeholders, including regulators. One example of such a program is SECURETexas.

Area 4.4 Cybersecurity Workforce: No recommendation at this time.

Area 4.5 Data Analytics: Add a subcategory under Framework Core Category PR.DS to specifically address the additional risks and required protections for "big data," and then map additional standards and other resources to the subcategory as informative references.

Area 4.6 Federal Agency Cybersecurity Alignment: Add a section in the NIST CsF document that compares, contrasts and ultimately integrates the NIST RMF—and by extension other control-based frameworks such as HITRUST and PCI—into the Framework.

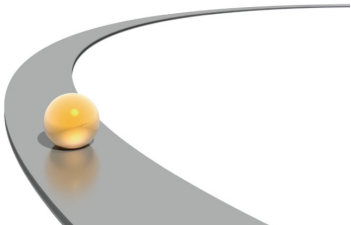
Area 4.7 International Aspects, Impacts, and Alignment: Add a section in the NIST CsF document that compares, contrasts and ultimately integrates the ISO/IEC 27001:2013 information security management system requirements into the Framework.

Area 4.8 Supply Chain Risk Management: Include a separate Framework Core subcategory under Category ID.RM that specifically addresses supply chain risk management, and then map relevant standards to the subcategory as informative references (per the NIST CsF Roadmap).

Area 4.9 Technical Privacy Standards: Reference our response to Q.12, incorporate a new privacy-specific Framework Core Subcategory to require the integration of privacy requirements into an organization's information protection (cybersecurity) program through privacy engineering and provide specific privacy-related informative references from NIST SP 800-53 r4 Appendix J, HITRUST CSF and other authoritative sources.

Q15. What is the best way to update the Framework while minimizing disruption for those currently using the Framework?

The NIST CsF is written at a high level and should not require revisions that would adversely impact an organization using it. But any changes that are made should be consistent with the current approach to the Framework Core, Tiers and Profiles. HITRUST believes real change should occur at the Sector-level and below, as this is where the specifics around how an organization would implement the NIST CsF would be written.



Sharing Information on Using the Network

Q16. Has information that has been shared by NIST or others affected your use [of] the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?

Direct consultation with NIST has been the most helpful. Joint presentations with NIST on the Framework, which have included sector-level implementation guidance like that provided by HITRUST, have also proven helpful to organizations integrating the NIST CsF into their information protection programs.

Q17. What, if anything, is inhibiting the sharing of best practices?

There is currently no forum for the free exchange of ideas. While valuable, the NIST CsF Industry Resources Website has limited content, and the addition of such content is strictly controlled by NIST. Case studies or similar accounts of an organization's experience implementing the NIST CsF could help other organization's leverage lessons learned by early adopters of the Framework.

Q18. What steps could the U.S. government take to increase sharing of best practices?

Recommend NIST consider a more collaborative online forum for the exchange of information and potentially sponsor regional and/or sector-specific workshops on implementing the Framework at the organizational-level, from small local businesses to very large multi-national corporations.

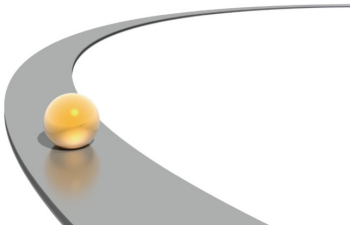
Q19. What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?

Recommend NIST consider a more collaborative online forum for the exchange of information and potentially sponsor regional and/or sector-specific workshops or "user groups" on implementing the Framework at the organizational-level, from small local businesses to very large multi-national corporations.

Private Sector Involvement in the Future Governance of the Framework

Q20. What should be the private sector's involvement be in the future governance of the Framework?

Given the intent is to provide guidance to critical infrastructure industries, which are predominantly owned and operated by the private sector, the private sector should be equally, if not primarily, responsible for governance and the maintenance of the Framework. NIST should continue to serve in an oversight/advisory role.



Q21. Should NIST consider transitioning some or even all of the Framework's coordination to another organization?

NIST should consider transitioning the entire Framework to the private sector or, at the very least, a public/private partnership organization.

Q22. If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, [and/or] methodologies)?

All elements of the Framework could be transitioned.

Q23. If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining

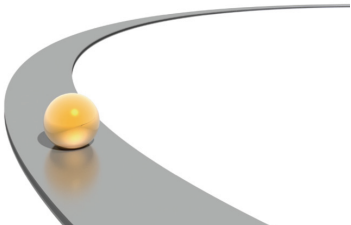
The Framework could be transitioned to a not-for-profit, U.S.-based organization with multinational private-sector representation. Participation could also be voluntary, both at an individual or organizational-level. However, nominal membership fees could be charged for both types of members, with the fees for organizations structured on a tiered model, e.g., by annual revenue. Such fees could be used to make the not-for-profit self-sustaining. The not-for-profit would only be required to hold the intellectual property and provide administrative support, similar to that provided by ISO or ANSI. (In fact, ANSI itself may be a good candidate.)

Q24. How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?

As the Framework is relatively static and—given its relatively high-level—must be supplemented by additional frameworks, standards, and/or guidance, transitioning ownership from NIST to another entity would likely have minimal impact on its use.

Q25. What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?

A new organization could be chartered to specifically address the need to “work closely and effectively with domestic and international organizations and governments.” However, factors to consider for the selection of an existing organization to take on the role of transition partner would necessarily include a demonstrated history of working at all levels of the public and private sector, both nationally and internationally. ANSI would be an example of one such organization.



HITRUST
Health Information Trust Alliance

In Closing

The quality of the work NIST has done in developing and communicating the *Framework for Improving Critical Infrastructure Cybersecurity* has been outstanding. The Framework is consistent with previous federal guidance and industry best practices, and it provides specific, implementable guidance for private sector organizations along with significant latitude in how critical infrastructure industries and organizations implement their information protection programs.

HITRUST would like to thank NIST for all its support for the private sector, including the work on the NIST Framework as well as other programs and initiatives. We've had the opportunity to work with multiple federal agencies on the problems faced by the HPH sector regarding cyber threats, and we look forward to establishing an even closer working relationship with these agencies, including NIST, in the future.

We stand ready to support NIST with its cybersecurity and information protection initiatives, not just with the NIST Framework, and are available to answer any questions you might have about our response to the RFI. Our point of contact is Dr. Bryan Cline, who may be reached by phone at (469) 269-1118 or via email at bryan.cline@hitrustalliance.net.

Very truly yours,

Daniel Nutkis
Chief Executive Officer