Healthcare Sector Cybersecurity Framework Implementation Guide

May 2016



Cautionary Note

This publication is not intended to replace or subsume other cybersecurity-related activities, programs, processes, or approaches that Healthcare and Public Health (HPH) Sector Organizations have implemented or intend to implement, including any cybersecurity activities associated with legislation, regulations, policies, programmatic initiatives, or mission and business requirements. Additionally, this publication uses the words “adopt,” “use,” and “implement” interchangeably. These words are not intended to imply compliance or mandatory requirements.

This publication and the information contained incorporates certain intellectual property of HITRUST Alliance Inc. (“HITRUST”), specifically relating to the CSF, CSF Assurance and HITRUST RMF. HITRUST claims all rights to this specific intellectual property. HITRUST assumes no responsibility for any errors or omissions and makes no, and expressly disclaims any, representations or warranties, express or implied, regarding this guidance, including, without limitation, the correctness, accuracy, completeness, timeliness, and reliability of the text or links to other resources. Copyrighted information is provided on an “as is” basis and offered for fair use subject to the limitations of specific licenses (e.g., the HITRUST CSF) and/or applicable copyright laws for such fair use. Under no circumstances shall the HITRUST Alliance, its affiliates, or any of its respective partners, officers, directors, employees, agents or representatives be liable for any damages, whether direct, indirect, special or consequential damages for lost revenues, lost profits, or otherwise, arising from or in connection with the materials contained within and referenced by this guide.

This document was developed in part based on feedback provided by public and private sector organizations under the Critical Infrastructure Partnership Advisory Council framework. The U.S. Government has made no representation with respect to the sufficiency of this document in complying with any Federal requirement, nor does the U.S. Government endorse the use of this document over the use of other frameworks, tools, or standards. This document is also considered a “living” document and subject to frequent updates, as needed, to best serve the healthcare industry.

Acknowledgements

The National Infrastructure Protection Plan (NIPP), developed under Presidential Policy Directive 21 (PPD-21), calls for public and private sector collaboration to improve the security and resilience of the nation's critical infrastructure in 16 critical infrastructure sectors. Under the NIPP, the U.S. Department of Health and Human Services (HHS) is responsible for coordinating critical infrastructure security and resilience activities for the Healthcare and Public Health (HPH) Sector. Under the NIPP's Critical Infrastructure Partnership Advisory Council (CIPAC), a structure administered by the Department of Homeland Security (DHS) to allow for interaction on critical infrastructure security and resilience matters among public and private sector partners, HHS leads a Government Coordinating Council (GCC) of Federal, State, local, Tribal, and Territorial representatives that partners with a self-governed Sector Coordinating Council (SCC) of private sector healthcare organizations. Together, the public and private sector partners combine to form the HPH Sector Critical Infrastructure Partnership.[1] The Partnership has established several joint work groups (WGs) and one such WG is the Joint HPH Cybersecurity WG.

In 2014, the National Institute of Standards and Technology (NIST) released the Framework for Improving Critical Infrastructure Cybersecurity ("Cybersecurity Framework") in response to a requirement of Executive Order (EO) 13636, Improving Critical Infrastructure Cybersecurity. EO 13636 also called on Sector-specific Agencies like HHS to "coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments." The Joint HPH Cybersecurity WG subsequently launched a Risk Management (RM) Sub-working Group (SG) in 2015 to build upon the work of existing organizations within the HPH Sector to advance the implementation of the Cybersecurity Framework in the Sector and provide a forum for discussion of cybersecurity issues related to risk management among a wide variety of HPH Sector stakeholders. This publication was developed in consultation with this SG.

RM SG members who assisted with the review of this guide include:

Phil Alexander, UMC Health System
Denise Anderson, NH-ISAC
Damon Becknel, Horizon BCBS
Cathy Beech, Children's Hospital of Philadelphia
Brenda Callaway, HCSC
Dr. Bryan Cline, HITRUST *(Co-chair)*
Leo Dittemore, Healthcare Partners
Dr. Cris Ewell, University of Washington
Andrew Hicks, Coalfire
Daryl Hykel, Health Management Systems, Inc.
Raj Mehta, Deloitte
Daniel Nutkis, HITRUST *(Private Sector Oversight)*
Michael Parisi, PwC
Michael Pinch, Univ. of Rochester Medical Ctr.
Terry Rice, Merck & Co., Inc.
Anahi Santiago, Christiana Care Health System
Dr. Suzanne Schwartz, FDA/CDRH/EMCM
Nick Sloan, Baylor Scott & White Health
Malikah Smith, HHS/ONC/OICPO *(Co-chair)*
Brandon Theis, Texas A&M Health Science Ctr.
Howard Tsai, DHS/NPPD
Michael Von Hoven, Humana
Jeffrey Webb, Express Scripts
Dr. Laura Wolf, HHS/ASPR *(Gov't Sector Oversight*

[1] DHS & DHHS (2010). Healthcare and Public Health Sector-specific Plan: An Annex to the National Infrastructure Plan. Washington, DC: Authors. Retrieved from http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf.

Version History

Version Number	Date Reviewed	Reviewed By	Brief Description
1.0	31 Dec 2015	Risk Mgmt. Sub-Working Group	Final document consolidating content from multiple documents/resources to support intent of broader implementation guidance for the healthcare sector and incorporating comments from the Risk Mgmt. Sub-working Group, the Public, and a final review by DHS. Contains placeholders for additional content being developed by the Risk Mgmt. Sub-Working Group for the next version of the Guide.
1.0	22 Jan 2016	HHS/OS/ASPR/OEM	Contains changes to the cautionary notes and acknowledgements, as well as minor changes to pp. 11-14 for clarity. Also corrects errors in Tables 15 and 21.
1.0	22 Feb 2016	Joint HPH Cybersecurity WG	Removes DRAFT from the document; updates the date from January to February 2016; adds placeholder appendices for proposed content on Cloud security, medical device security, and industry resource mappings; and makes minor grammatical corrections.
1.1	15 May 2016	Risk Mgmt. Sub-Working Group	Incorporates OCR's NIST CsF-to-HIPAA crosswalk, updates CNSSI No. 4009 definitions to reflect its 2015 release; and makes other minor corrections.

Table of Contents

List of Tables

List of Figures

Introduction

The United States has seen a marked increase in the use of electronic information and a resulting increase in the level of exposure to cyber-attacks, which target an organization's use of cyberspace for the purpose of stealing information or disrupting, disabling, or destroying related information resources. As a result of these ever increasing cyber threats, President Barack Obama directed the National Institute of Standards and Technology (NIST) to work with the private sector to develop the Framework for Improving Critical Infrastructure Cybersecurity,[2] also known as the Cybersecurity Framework (CsF). The NIST CsF provides an overarching incident management-based model that industries, industry sectors, or organizations can leverage to identify opportunities for improving their management of cybersecurity risk.

The Health Information Trust Alliance (HITRUST)[3] Risk Management Framework (RMF)[4]—consisting of the CSF,[5] CSF Assurance Program,[6] and supporting methods, tools and services—is a model implementation[7] of the NIST CsF. Consistent with the NIST framework, the HITRUST CSF provides a comprehensive, prescriptive, yet flexible, information security control framework that leverages the risk analyses used to develop its supporting authoritative sources. The CSF Assurance Program complements the CSF by providing the mechanism for sharing information security assurances with internal and external stakeholders in a consistent and repeatable way.

This document seeks to help Healthcare Sector organizations understand and use the HITRUST RMF to achieve the goals of the NIST CsF. To help further this aim, the document presents background information on the NIST and HITRUST frameworks, including potential benefits to Healthcare Sector organizations, explains the relationship between the two frameworks and how the HITRUST RMF provides a model implementation of the NIST CsF for the Healthcare Sector, presents a mapping of HITRUST CSF controls to the NIST CsF subcategories, and provides additional implementation guidance.

Executive Order 13636 and the NIST CsF

In its December 2011 report, "Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use"[8], the GAO found similarities in cybersecurity guidance and practices across multiple sectors, even though much of this guidance is tailored to business needs or to address unique risks and operations, and recommended promoting existing guidance to assist individual entities within a sector to identify "the guidance that is most applicable and effective in improving their security posture."[9] But even before the

---

[2] NIST (2014). Framework for Improving Critical Infrastructure Cybersecurity, Version 1. Wash., DC: Author. Retrieved from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.
[3] https://hitrustalliance.net/
[4] Cline, B. (2013a). Risk Management Frameworks: How HITRUST provides an efficient and effective approach to the selection, implementation, assessment and reporting of information security and privacy controls to manage risk in a healthcare environment. Frisco, TX: HITRUST. Retrieved from https://hitrustalliance.net/content/uploads/2015/03/HITRUST-RMF-Whitepaper-2015.pdf
[5] https://hitrustalliance.net/hitrust-csf/
[6] https://hitrustalliance.net/csf-assurance/
[7] Cline, B. (2014a). Healthcare's Model Approach to Critical Infrastructure Cybersecurity: How the Industry is Leading the Way with its Information Security Risk Management Framework. Frisco, TX: HITRUST. Retrieved from https://hitrustalliance.net/content/uploads/2015/09/ImplementingNISTCybersecurityWhitepaper.pdf.
[8] GAO (2011). Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use, Wash., DC: Author. Retrieved from http://www.gao.gov/products/GAO-12-92
[9] Ibid., p. i

GAO released its report, HITRUST worked with prominent healthcare organizations to create a cyber threat intelligence and incident coordination capability for the Sector. Officially launched in April of 2012, HITRUST's cyber threat intelligence and incident coordination products and services provide meaningful 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.

Less than a year later, President Obama issued Executive Order 13636 (EO),[10] "Improving Critical Infrastructure[11] Cybersecurity" on February 12, 2013, which called for the development of a voluntary Cybersecurity Framework to provide a "prioritized, flexible, repeatable, performance-based, and cost-effective approach" for the management of cybersecurity risk. As a result, HITRUST reviewed several cybersecurity-related best practice frameworks, including the SANS 20 Critical Controls for Cybersecurity[12] and, in June 2013—identified 59 CSF controls[13] determined to be most relevant to cybersecurity, which helps provide assurances as to how well one is addressing cyber-specific threats.

After three cybersecurity framework workshops, NIST published its August 28, 2013, discussion draft of the Preliminary Cybersecurity Framework intended to help improve critical infrastructure cybersecurity in advance of its Fourth Cybersecurity Framework workshop in September and made the draft available to the general public for review. NIST released a "final" public draft of the Preliminary Cybersecurity Framework in October of 2013, and the final version was released in February of 2014,[14] which HITRUST formally integrated into the CSF and CSF Assurance Program in April of 2014 with version 6.1.

EO 13636 also directed development of a program to serve as a central repository for government and private sector tools and resources. This Critical Infrastructure Cyber Community (C^3) Voluntary Program provides critical infrastructure sectors, academia, state, local, tribal, and territorial governments with businesses tools and resources to use the NIST CsF and enhance their cyber risk management practices.

Potential Benefits of Healthcare's Implementation of the NIST CsF

Based on a collection of cybersecurity standards and industry best practices, the NIST CsF broadly applies across all organizations, regardless of size, industry, or cybersecurity sophistication. Whether an organization has a mature risk management program and processes, is developing a program or processes, or has no program or processes, the Framework can help guide an organization in improving cybersecurity and thereby improve the security and resilience of critical infrastructure.

---

[10] Exec. Order No. 13636, 3 C.F.R. 11739-11744 (2013). Retrieved from http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

[11] Critical infrastructure is defined in the EO as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

[12] Council on CyberSecurity (2014). The Critical Security Controls for Effective Cyber Defense, Version 5.1. Retrieved from http://www.counciloncybersecurity.org/critical-controls/

[13] Cline, B. (2013b). Using the HITRUST CSF to Assess Cybersecurity Preparedness, Frisco, TX: HITRUST. Retrieved from http://hitrustalliance.net/content/uploads/2014/05/HITRUST-Cybersecurity-Preparedness.pdf

[14] NIST (2014). NIST Releases Cybersecurity Framework Version 1.0. Retrieved from http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

Specifically, the NIST CsF:

- Provides guidance on risk management principles and best practices,
- Provides common language to address and manage cybersecurity risk
- Outlines a structure for organizations to understand and apply cybersecurity risk management, and
- Identifies effective standards, guidelines, and practices to manage cybersecurity risk in a cost-effective manner based on business needs.

Beyond the stated goals and benefits of the NIST CsF, there are additional potential benefits to organizations that implement NIST CsF "compliant" information protection programs, such as those based on the HITRUST RMF.

The Federal Government will seek to recognize organizations that use NIST CsF — The Department of Homeland Security (DHS) seeks to recognize those organizations that use the NIST CsF and leverage the C^3 Voluntary Program, regardless of size and maturity level.[15] The C3 Voluntary Program's Partner Program will be a formal recognition of an organization's efforts to use the tools and resources made available through the Voluntary Program to enhance their use of the NIST CsF. The HITRUST RMF is fully consistent with the recommendations of the NIST CsF, and it will likely be recognized by the Federal Government under the Partner Program. Organizations that receive HITRUST CSF or SECURETexas certification would subsequently benefit from this recognition.

Compliance with the Health Insurance Portability and Accountability Act (HIPAA) and Other Regulatory Requirements – Organizations that correctly implement a NIST CsF-based information protection program can demonstrate a minimal, recognizable level of due care and due diligence for the protection of protected health information (PHI). The HITRUST CSF provides prescriptive requirements that may assist organizations in responding to the standards and implementation specifications of the HIPAA Security Rule, including the requirement for a comprehensive risk analysis.

Organizations leveraging the NIST CsF may see limitations in breach liability — Organizations may be less liable in the event a cyber-incident occurs if they have a proven track record of implementing and evaluating their cyber risk management procedures.[16] These areas include reduced tort liability, limited indemnity, higher burdens of proof, or the creation of a federal legal privilege that preempts State disclosure requirements. The HITRUST CSF and CSF Assurance Program are used to support SECURETexas—the first state-recognized security and privacy certification program for covered entities in the country—and certification may provide evidence of compliance with federal and state requirements, including HIPAA. State regulators and courts are further required by law to consider SECURETexas certification as a mitigating factor when assessing fines and other penalties due to a breach of covered information. This model may eventually be adopted by other states.

Reductions in cybersecurity insurance premiums as a potential incentive for using the framework — Organizations should consider the impact on their insurance premiums if they do or do not follow sound cybersecurity practices.[17] Furthermore, as cybersecurity continues to grow on the national and international security agenda, insurance underwriters are strongly

[15] Department of Energy, DOE (N.D). Energy Sector Cybersecurity Framework Implementation Guidance, Version 4 (DRAFT), Wash., D.C.: Author, p. 4
[16] Ibid.
[17] Ibid., p. 3

considering evaluating their client's premiums based on standards, procedures, and other measures consistent with the NIST CsF. The goal would be to build underwriting practices that promote the use of cyber risk-reducing measures and risk-based pricing and foster a competitive cyber insurance market. As of this writing, HITRUST is collaborating with a major insurance broker to pilot use of the HITRUST CSF and CSF Assurance Program to provide more accurate and consistent assessments of risk in the underwriting process.

Federal Agencies will incentivize use of the CsF and perhaps make C³ Voluntary Program participation a condition or criterion for federal grants — Organizations that follow the NIST CsF, or show proof of attempt to follow the NIST CsF more closely, are more likely to receive grants from various federal grant programs.[18] Agencies suggest incentivizing the use of the NIST CsF and participation in the C³ Voluntary Program by making them a condition of, or as one, of the weighted criteria for federal critical infrastructure grants. In addition, agencies generally require some level of compliance with NIST security guidance on many, if not most, federal contracts. The HITRUST CSF incorporates NIST SP 800-53 and Centers for Medicaid and Medicare Services (CMS) Information Security (IS) Acceptable Risk Safeguards (ARS) control baselines. NIST CsF adoption/compliance is a natural extension of existing requirements.

The Federal Government can provide prioritized technical assistance for organizations that seek to leverage the CsF — The Federal Government provides several hands-on tools that will help organizations assess their current-state of cybersecurity practices and identify areas to grow their cybersecurity resilience. HPH Sector organizations are encouraged to visit the US-CERT Critical Infrastructure Community (C3) Voluntary Program webpage at https://www.us-cert.gov/ccubedvp for additional information related to both facilitated and self-service risk assessment resources. Based off this assessment, the Federal government helps prioritize next steps for organizations, depending on their level of cybersecurity maturity. For example, the government offers preparedness support, assessments, training of employees, and advice on best practices. Under this incentive, the primary criteria for assistance would be criticality, security, and resilience gaps. Owners and operators in need of incident response support will never be denied assistance based on cybersecurity maturity and/or level of prior engagement with the use of the NIST CsF.

In general, conducting national/sector-level cybersecurity activities in parallel with organizational level activities based on the NIST CsF enhances the resiliency of the Healthcare Sector, the Nation, and individual organizations. Use by many organizations across the Healthcare Sector can help identify those cross-cutting risks that cannot be managed by one organization. Sector efforts can manage these systemic risks that cut across many organizations and also lead to research and development efforts to create new security solutions, policy or legal solutions, and national-level programs.

For example, leading organizations within the healthcare industry formed from an alliance to address the growing need and broad desire within the industry for a set of common standards and supporting methodologies that would provide a minimum baseline set of security requirements, tailorable to a specific size and type of organization, which would improve trust as well as mitigate potential liability from breaches of sensitive information. The result was the creation of the HITRUST CSF and CSF Assurance Program, which became the core of the HITRUST RMF.

[18] Ibid., p.4

Another, more recent example includes the collaboration between the Department of Health and Human Services (DHHS), DHS, HITRUST and its Alliance participants in the HITRUST Information Sharing and Analysis Organization (ISAO) has resulted in a better understanding of threats, vulnerabilities, and consequences and how to manage them through the sharing of indicators and practices and the coordination of policies, response, and recovery activities such as the HITRUST Cyber Threat Xchange (CTX) and CyberRX incident management exercise program at local, regional and national levels.

Key Elements of a Cybersecurity Program

There are three key elements that must be addressed to ensure an organization implements a robust and comprehensive cybersecurity program: threat modeling, threat intelligence[19] and collaboration. Threat modeling may be accomplished either through a traditional risk analysis or the selection of a control baseline from an appropriate security framework. A good framework helps an organization:

- Ensure people, process and technology elements completely and comprehensively address information and cybersecurity risks consistent with their business objectives, including legislative, regulatory and best practice requirements
- Identify risks from the use of information by the organization's business units and facilitate the avoidance, transfer, reduction or acceptance of risk
- Support policy definition, enforcement, measurement, monitoring and reporting for each component of the security program and ensure these components are adequately addressed

Threat intelligence is essential for an organization to understand and proactively address active and emerging cyber threats, and collaboration with other public and private sector entities allows an organization to address cyber threats more efficiently and effectively than it otherwise could.

The NIST CsF provides the structure needed to ensure these three key elements are addressed by industry sectors and organizations while providing the flexibility needed to implement the framework smartly. Organizations have unique cybersecurity risks, including different threats, vulnerabilities, and tolerances, all of which affect benefits from investing in cybersecurity risk management, and they must apply the principles, best practices, standards, and guidelines provided in the NIST CsF to their specific context and implement practices based on their own needs.

The Healthcare Sector embraces the flexibility the NIST CsF offers but recognizes organizations' potential need for more guidance on how to specifically apply the framework to their particular context. In addition, the Healthcare Sector recognizes the potential of the NIST CsF to benefit cybersecurity risk management efforts across all critical infrastructure industry sectors.

[19] Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets … used to inform decisions regarding a response to that menace or hazard. (https://www.gartner.com/doc/2487216/definition-threat-intelligence)

Purpose of the Cybersecurity Implementation Guidance

To help organizations understand and use the HITRUST RMF to implement the NIST CsF in the Healthcare Sector, HITRUST developed this document in consultation with the Sector Coordinating Council (SCC) and Department of Homeland Security (DHS) Sector Outreach and Programs Division (SOPD) (as the SSA), along with input from sector members and the DHS Critical Infrastructure Cyber Community (C^3) Voluntary Program.

This document is intended to help Sector organizations understand and use the HITRUST RMF as the sector's implementation of the NIST CsF and support implementation of a sound cybersecurity program that addresses the five core function areas of the NIST CsF to ensure alignment with national standards, help organizations assess and improve their level of cyber resiliency, and provide suggestions on how to link cybersecurity with their overall information security and privacy risk management activities to the Healthcare Sector.

The guidance will also help an organization's leadership to:

- Understand NIST CsF and HITRUST RMF terminology, concepts, and benefits
- Assess their current and targeted cybersecurity posture
- Identify gaps in their current programs and workforce
- Identify current practices that exceed NIST CsF requirements

Health Sector Cybersecurity Framework Implementation

While the generic cybersecurity framework implementation approach outlined in Appendix C – NIST CsF Basics—and used by other critical infrastructure sectors such as the Department of Energy—works well for organizations that design or specify their own controls, it does not work *as well* (i.e., most efficiently) for those organizations that leverage a framework-based risk analysis to select and modify a control baseline (or overlay). Fortunately, this generic implementation approach can be modified to accommodate a control framework-based approach in the same way the basic risk analysis process advocated by DHHS can be modified (see Approach to Risk Analysis and Risk Management in Appendix D – Healthcare's Implementation of the NIST CsF).

The primary reason for the modification is that, for those organizations that leverage the HITRUST RMF, Target Profiles are easily obtained once organizations are able to scope their organization and systems, tailor the HITRUST CsF controls based on their organizational, system and regulatory risk factors, and then further tailor the overlay to address any unique threats. There is no need to develop a Current Profile beforehand. *Placement of the Current and Target Profiles can subsequently be reversed*, although some basic information about the state of the organization's cybersecurity program will necessarily be ascertained before the Target Profile is complete.

Implementation Process

Healthcare Sector organizations leveraging the HITRUST RMF should use the following seven-step process for implementation.[20]

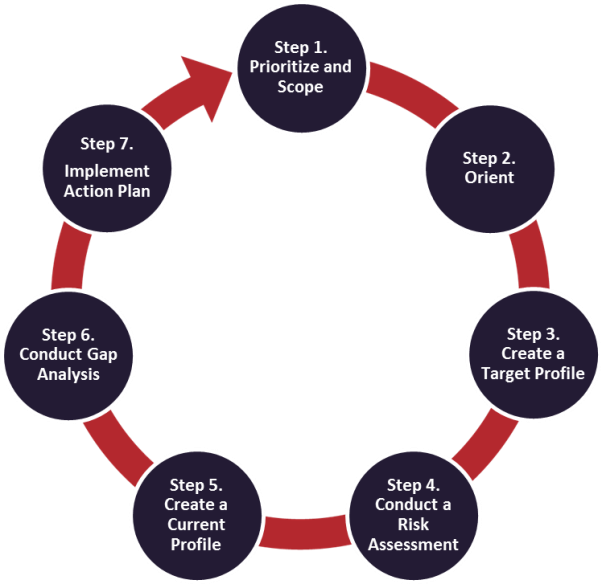
- Step 1: Prioritize and scope organizational components for framework adoption
- Step 2: Identify systems and existing risk management approaches within the scope
- Step 3: Create a desired risk management profile based on the organization's risk factors (Target Profile)
- Step 4: Conduct a risk assessment
- Step 5: Create a current risk management profile based on assessment results (Current Profile)
- Step 6: Develop a prioritized action plan of controls and mitigations (Action Plan)
- Step 7: Implement the Action Plan

The revised process is depicted in Figure 1.

As with the generic process, implementation should include a plan to communicate progress to appropriate stakeholders, such as senior management, as part of its risk management program. In addition, each step of the process should provide feedback and validation to previous steps.

[20] NIST (2014), pp. 13-15

Figure 1. Healthcare Implementation Process



Each step is now discussed in more detail, first introduced by a table describing the step's inputs, activities, and outputs followed by additional explanation.[21] A table of the inputs, activities, and outputs for all seven steps is also included in Appendix F – NIST CsF and HIPAA Security Rule Mapping.

Step 1: Prioritize and Scope

Table 1. Step 1: Prioritize and Scope Inputs, Activities, and Outputs

Step 1: Prioritize and Scope		
Inputs	Activities	Outputs
1. Risk management strategy 2. Organizational objectives and priorities 3. Asset inventory 4. HITRUST RMF	1. Organization determines where it wants to apply the HITRUST RMF to evaluate and potentially guide the improvement of the organization's capabilities 2. Threat analysis 3. Business impact analysis 4. System categorization (based on sensitivity & criticality)	1. Usage scope 2. Unique threats

The risk management process should begin with a strategy addressing how to frame, assess, respond to, and monitor risk. For healthcare organizations, leveraging the HITRUST RMF is a central component of that strategy as it forms the basis of their HIPAA-required risk analysis,

[21] The tables describing the activities in the 7-step implementation process are derived from DOE (2015).

informs the organization on the minimum level of due care and due diligence required to meet its multiple compliance obligations, provides for the adequate protection of PHI and other sensitive information, and provides a comprehensive and rigorous methodology for control assessment, scoring, and reporting. The organization's risk strategy is also used to inform investment and operational decisions for improving or otherwise remediating gaps in their cybersecurity and information protection program.

In this step, the organization decides how and where it wants to apply the HITRUST RMF (its usage scope)—whether in a subset of its operations, in multiple subsets of its operations, or for the entire organization. This decision should be based on risk management considerations, organizational and critical infrastructure objectives and priorities,[22] availability of resources, and other internal and external factors. Current threat and vulnerability information from HITRUST or other nationally recognized ISAO may also help inform scoping decisions.

An organization that is using the HITRUST RMF for the first time might want to apply it to a small subset of operations to gain familiarity and experience with it. After this activity, the organization can consider applying the RMF to a broader subset of operations or to additional parts of the organization as appropriate.

Note, this step includes the following elements of the DHS risk analysis process as modified to accommodate use of a control framework:

- Conduct a complete inventory of where electronic PHI (ePHI) lives (if not already performed)
- Perform a Business Impact Analysis (BIA) on all systems with ePHI (criticality)
- Categorize & evaluate these systems based on sensitivity and criticality

Step 2: Orient

Table 2. Step 2: Orient Inputs, Activities, and Outputs

Step 2: Orient		
Inputs	Activities	Outputs
1. Usage scope 2. Risk management strategy 3. HITRUST RMF	1. Organization identifies in-scope systems and assets (e.g., people, information, technology and facilities) and the appropriate regulatory and other authoritative sources (e.g., cybersecurity and risk management standards, tools, methods and guidelines)	1. In-scope systems and assets 2. In-scope requirements (e.g., organizational, system, regulatory)

The organization identifies the systems, assets, compliance and best practice requirements, and any additional cybersecurity and risk management approaches that are in scope. This includes standards and practices the organization already uses, and could include additional standards

[22] DHS and DHHS (2010). Healthcare and Public Health Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan. Wash., DC: Author. Retrieved from http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf

and practices that the organization believes would help achieve its critical infrastructure and business objectives for cybersecurity risk management. The organization's risk management program may already have identified and documented much of this information, or the program can help identify individual outputs. A good general rule is to initially focus on critical systems and assets and then expand the focus to less critical systems and assets as resources permit.

Note that this step includes the following element of the DHS risk analysis process as modified to accommodate use of a control framework: *Conduct a complete inventory of where ePHI lives.* (Note a HIPAA-compliant risk analysis generally considers all systems, devices, locations, etc., where ePHI "lives" to be in scope.)

Step 3: Create a Target Profile

Table 3. Step 3: Target Profile Inputs, Activities, and Outputs

Step 3: Create a Target Profile		
Inputs	Activities	Outputs
1. Organizational objectives 2. Risk management strategy 3. Detailed usage scope 4. Unique threats 5. HITRUST RMF	1. Organization selects a HITRUST CSF control overlay and tailors the overlay based on unique threats identified in the prioritization and scoping phase 2. Organization determines level of maturity desired in the selected controls	1. Target Profile (Tailored HITRUST CSF control overlay) 2. Target Tier

The organization applies its specific risk factors as determined during the first two steps to create an overlay of the CSF for its particular subclass of healthcare entity and then tailors the overlay to account for any unique threats (as compared to other, similar organizations in its subclass). The Target Profile should include these practices as well.

However, information protection cannot be a "one size fits all" approach. For example, organizations, more often as not, have different information systems (or different implementations of similar systems), different business and compliance requirements, different cultures, and different risk appetites. Even the HITRUST CSF cannot account for all these differences through the tailoring of controls based on specific organizational, system, and regulatory risk factors.

So for whatever reason an organization cannot implement a required control, one or more compensating controls should be selected to address the risks posed by the threats the originally specified control was meant to address. But while compensating controls are well-known and extensively employed by such compliance frameworks such as the Payment Card Industry Digital Security Standard (PCI-DSS), the term compensating control has often been used to describe everything from a legitimate work-around to a mere shortcut to compliance that fails to address the intended risk.

As a result, organizations should be able to demonstrate the validity of a compensating control by way of a legitimate risk analysis that shows the control has the same level of rigor and addresses a similar type and level of risk as the original. Additionally, the compensating control must be something other than what may be required by other, existing controls. For more

information on how compensating controls can be used to support HITRUST CSF validated or certified assessments and reporting, refer to the HITRUST Risk Analysis Guide.[23]

The organization should also determine the evaluation approach it will use to identify its current cybersecurity and risk management posture. Organizations can use any of a number of evaluation methods to identify their current cybersecurity posture and create a Current Profile. These include self-evaluations, where an organization may leverage its own resources and expertise; facilitated approaches, where the evaluation is assisted by a third party; or completely independent evaluations, such as those used to support a HITRUST validated or certified report or American Institute of Certified Public Accountants (AICPA) Service Organization Control (SOC 2) for HITRUST report.[24]

The organization should also determine its goals for the Target Tier from the NIST CsF and identify the equivalent levels of control maturity required to achieve those goals. For example, an organization may be satisfied with a Tier 1, Risk-Informed level of organizational maturity, which would translate to an overall 3- to 3+ maturity rating. However, an organization with less risk tolerance may select a Tier 3, Repeatable level and subsequently strive for an overall control maturity rating of 4- to 5-. Refer to Table 13 and Table 14 in Appendix D – Healthcare's Implementation of the NIST CsF for more information on the HITRUST maturity ratings and how they map to the NIST CsF Implementation Tiers.

Note, this step includes the following elements of the DHS risk analysis process as modified to accommodate use of a control framework:

- Select an appropriate framework baseline set of controls
- Apply an overlay based on a targeted assessment of threats unique to the organization

Step 4: Conduct a Risk Assessment

Table 4. Step 4: Risk Assessment Inputs, Activities, and Outputs

Step 4: Conduct a Risk Assessment		
Inputs	Activities	Outputs
1. Detailed usage scope 2. Risk management strategy 3. Target Profile 4. HITRUST RMF	1. Perform a risk assessment for in-scope systems and organizational elements	1. Risk assessment reports

Evaluation of the maturity of the organization's control implementation—often colloquially referred to as a risk assessment (even though NIST considers the terms synonymous)—is performed in this step. Organizations perform cybersecurity risk assessments to identify and evaluate cybersecurity risks and determine which are outside of current tolerances. The outputs of cybersecurity risk assessment activities assist the organization in developing its Current Profile and Implementation Tier based on control maturity, which occurs in Step 5. For organizations

[23] Cline, B. (2014b). Risk Analysis Guide for HITRUST Organizations and Assessors: A Guide for Self- and Third-party Assessors on the Application of HITRUST's Approach to Risk Analysis, Frisco, TX: HITRUST, pp. 34-40. Retrieved from https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf

[24] https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/pages/soc2additionalsubjectmatter.aspx

that have a risk management program in place, this activity will be part of regular business practice, and necessary records and information to make this determination may already exist. For example, many organizations perform regular evaluations of their programs through internal audits or other activities, which may describe the controls as implemented within the defined scope of the risk assessment.

Note, this step includes the following elements of the DHS risk analysis process as modified to accommodate the use of a control framework:

- Evaluate residual risk
  - Likelihood based on an assessment of control maturity
  - Impact based on relative (non-contextual) ratings

Step 5: Create a Current Profile

Table 5. Step 5: Current Profile Inputs, Activities, and Outputs

Step 5: Create a Current Profile		
Inputs	Activities	Outputs
1. Risk assessment reports 2. HITRUST RMF	1. Organization identifies its current cybersecurity and risk management state	1. Current Profile (Implementation status of selected controls) 2. Current Tier (Implementation maturity of selected controls, mapped to NIST CsF Implementation Tier model)

A Current Profile is created from the evaluation of the organization's cybersecurity and risk management practices against the Target Profile created in Step 4. The organization may represent the results using the HITRUST CSF control structure, or if a report is generated using HITRUST's online assessment support tool,[25] the results can be presented as a scorecard for the HITRUST assessment domains and/or the NIST CsF subcategories. To manually generate a scorecard for a NIST CsF Target Profile, refer to Appendix E – NIST CsF and HITRUST CSF Mapping. In fact, scorecards against any of the CSF's authoritative sources, including the NIST CsF, may be manually generated using the mappings contained in the HITRUST CSF cross-reference document.[26] The maturity scores generated during the assessment will also inform the current Implementation Tier as described earlier in this document.

Note, this step includes the following elements of the DHS risk analysis process as modified to accommodate use of a control framework:

- Evaluate residual risk
  - Likelihood based on an assessment of control maturity
  - Impact based on relative (non-contextual) ratings

[25] Frederick, M. (2015). HITRUST vs. GRC Tools: Understanding the Differences and Total Cost of Ownership. Frisco, TX: HITRUST. Retrieved from https://hitrustalliance.net/mycsf/
[26] Available in the CSF download package through the CSF license agreement landing page: https://hitrustalliance.net/csf-license-agreement/.

Step 6: Perform Gap Analysis

Table 6. Step 6: Gap Analysis Inputs, Activities, and Outputs

Step 6: Perform Gap Analysis		
Inputs	Activities	Outputs
1. Current Profile 2. Target Profile 3. Organizational objectives 4. Impact to critical infrastructure 5. Gaps and potential consequences 6. Organizational constraints 7. Risk management strategy 8. Risk assessment/analysis reports 9. HITRUST RMF	1. Analyze gaps between Current and Target Profiles in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention 4. Identify actions to address gaps 5. Perform cost-benefit analysis (CBA) or similar analysis on actions 6. Prioritize actions (CBA or similar analysis) and consequences 7. Plan to implement prioritized actions	1. Prioritized gaps and potential consequences 2. Prioritized implementation plan

The organization evaluates its Current Profile and Implementation Tier against its Target Profile and Target Implementation Tier and identifies any gaps. When mapping back to the NIST CsF, a gap exists when there is a desired Category or Subcategory outcome in the Target Profile or program characteristic in the Target Implementation Tier that is not currently achieved by the organization's existing cybersecurity and risk management approach, and when current practices do not achieve the outcome to the degree of satisfaction required by the organization's risk management strategy. When using the HITRUST CSF controls as the evaluation and reporting mechanism, gaps are identified by a level of control maturity that does not meet or exceed the levels specified by the Target Implementation Tier. (A control maturity score of zero is a valid measure of a control that is not implemented as required by the Target Profile.)

After controls are specified by an organization to ensure risk is controlled to a level formally deemed acceptable by executive leadership, the most common way of dealing with deficiencies observed with the implementation and management of those controls is to remediate them. This reduces risk to an acceptable level, a process referred to as mitigation.

HITRUST requires assessed entities requesting a validated or certified report to prepare Corrective Action Plans (CAPs) for identified deficiencies. Self- or third-party assessors, as applicable, must describe the specific measures intended to remediate (correct) deficiencies identified during an assessment for validation or certification. HITRUST understands that most organizations have more vulnerabilities than they have resources to address, so organizations should prioritize corrective actions based on the sensitivity and criticality of the information systems or assets affected, the direct effect the vulnerability has on the overall security posture of the information systems or assets, and the requirements for CSF certification. Note, third party assessors must review the CAP to evaluate the effectiveness of the remediation strategy,

provide recommendations or feedback as needed, and document any findings for submission to HITRUST if the organization wishes to receive a HITRUST validated or certified report.

Non-contextual Impact and Relative Risk

Although HITRUST organizations and CSF Assessors typically have no problem with identifying the corrective actions needed to address specific deficiencies, some have difficulty rating the risks associated with these deficiencies and subsequently prioritizing the work. To help with CAP prioritization, HITRUST provides non-contextual impact ratings for each CSF control, which allows the computation of relative risk for each deficiency identified in an assessment. The ratings are non-contextual in that they assume the probable impact should the control fail—assuming all other controls are in place.

Impact is described using five rating levels: Very Low (1), Low (2), Moderate (3), High (4) and Very High (5). For the purpose of computing risk, ratings may be assigned specific values such as those prescribed by NIST: Very Low (1) = 0, Low (2) = 2, Moderate (3) = 5, High (4) = 8, and Very High (5) = 10.[27] HITRUST uses a similar approach and computes impact (I) as a function of the impact rating (IR):

$$\text{Impact} = I = (IR - 1) \times (25),$$

which equates to Very Low (1) = 0, Low (2) = 25, Moderate (3) = 50, High (4) = 75, and Very High (5) = 100. When converted to a 10-point scale and rounded up, the values are identical to the NIST model.

Table 7 provides the HITRUST impact ratings for all 135 CSF controls directly related to cybersecurity.

Table 7. Impact Ratings (Non-contextual)

Ctrl	IR	Ctrl	IR	Ctrl	IR	Ctrl	IR	Ctrl	IR	Ctrl	IR	Ctrl	IR	Ctrl	IR	Ctrl	IR
0.a	3	01.o	3	02.e	5	05.e	3	06.i	4	08.i	4	09.k	3	09.z	5	10.i	4
01.a	5	01.p	3	02.f	5	05.f	4	06.j	3	08.j	4	09.l	3	09.aa	3	10.j	4
01.b	5	01.q	5	02.g	5	05.g	4	07.a	4	08.k	5	09.m	4	09.ab	3	10.k	4
01.c	5	01.r	4	02.h	5	05.h	5	07.b	3	08.l	5	09.n	4	09.ac	3	10.l	3
01.d	5	01.s	4	02.i	5	05.i	4	07.c	5	08.m	5	09.o	3	09.ad	3	10.m	3
01.e	5	01.t	3	03.a	3	05.j	5	07.d	4	09.a	5	09.p	5	09.ae	3	11.a	3
01.f	5	01.u	3	03.b	3	05.k	5	07.e	5	09.b	4	09.q	4	09.af	3	11.b	4
01.g	4	01.v	3	03.c	3	06.a	4	08.a	5	09.c	5	09.r	4	10.a	4	11.c	3
01.h	3	01.w	3	03.d	3	06.b	4	08.b	5	09.d	4	09.s	5	10.b	4	11.d	3
01.i	4	01.x	5	04.a	3	06.c	3	08.c	5	09.e	4	09.t	3	10.c	4	11.e	3
01.j	5	01.y	5	04.b	3	06.d	3	08.d	4	09.f	4	09.u	3	10.d	3	12.a	3
01.k	4	02.a	4	05.a	4	06.e	5	08.e	5	09.g	4	09.v	4	10.e	4	12.b	3
01.l	4	02.b	5	05.b	5	06.f	4	08.f	4	09.h	3	09.w	4	10.f	3	12.c	3
01.m	3	02.c	5	05.c	3	06.g	4	08.g	4	09.i	4	09.x	4	10.g	3	12.d	3
01.n	4	02.d	4	05.d	3	06.h	4	08.h	3	09.j	4	09.y	4	10.h	4	12.e	3

[27] NIST (2012), Guide for Conducting Risk Assessments, NIST SP 800-30 r1, Wash., DC: Author, p. H-3. Downloaded from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

The numbers are intended to provide a starting point for assignment of relative risk to CAPs based on relative maturity of the controls as determined by a HITRUST CSF assessment. For internal remediation planning purposes, organizations may adjust the impact ratings based on the status of other controls in the environment or the sensitivity and/or criticality of the information assets in scope. However, these non-contextual impact ratings may not be adjusted for validation and certification reporting to ensure consistency across the industry.

Note, the formula for computing risk using the HITRUST CSF control maturity score may be written as:

$$R = L \times I = [(100 - MS) / 100] \times [(IR - 1) \times 25],$$

where, R = risk, L = likelihood, I = impact, MS = HITRUST CSF control maturity score, and IR = impact rating.

For example, suppose an organization obtains a maturity score of 75 for CSF control 01.a. Since this is a very high impact control, the risk would be computed as [(100 - 75) / 100] x [(5 - 1) x 25) = .25 x 100 = 25, which is a moderate risk.

HITRUST recognizes two types of risk scales, a traditional bell-shaped model and a left-skewed bell-shaped "academic" model. Although the traditional model is best used for communicating risk to external stakeholders, the academic model provides a very intuitive approach to understanding risk when presented as risk grades, reminiscent of the model used by the federal government to report security compliance for federal agencies.

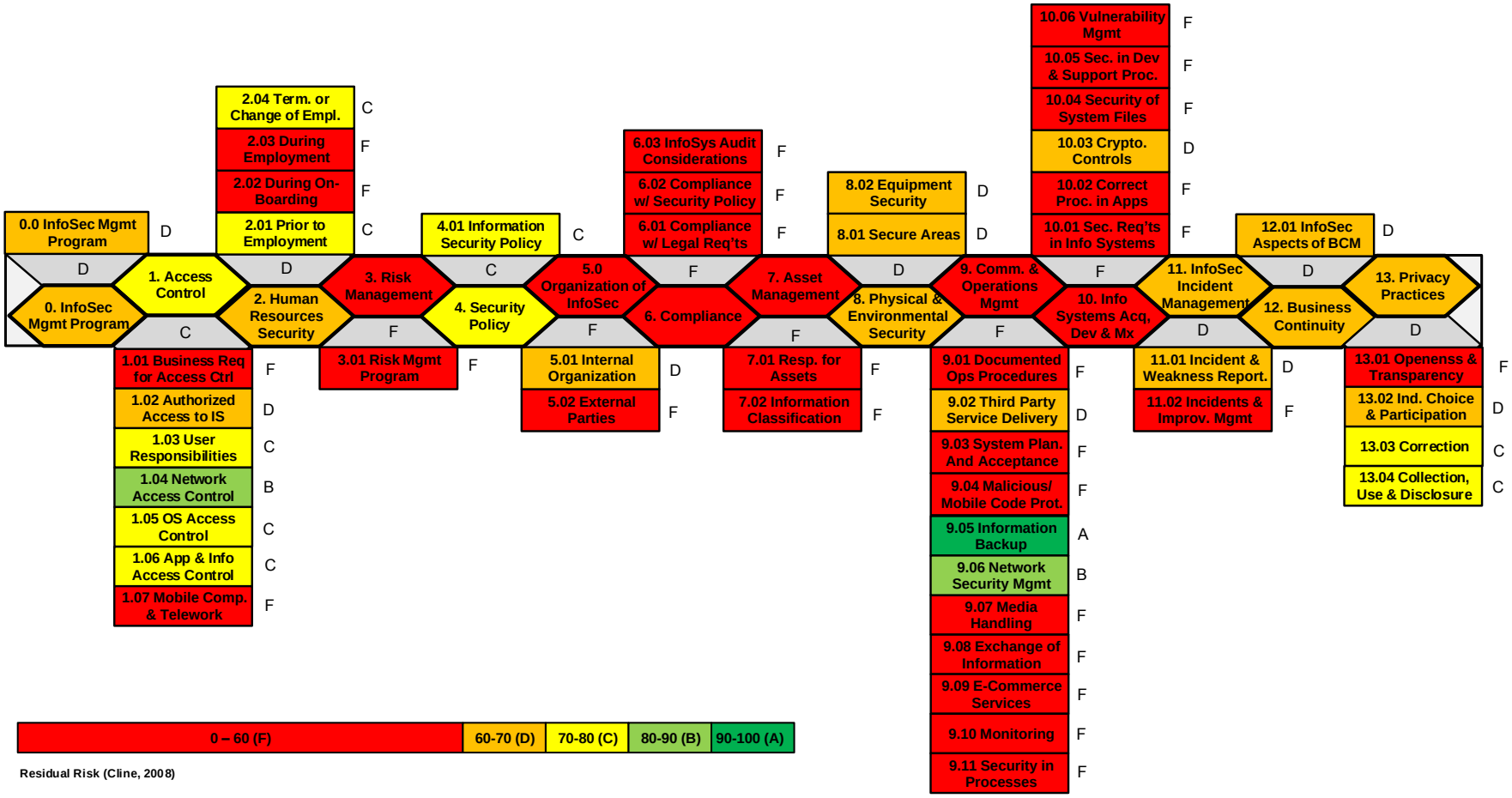
The following table provides the intervals for both models:

Table 8. Risk Scales

Risk Level	Range (Traditional Model)	Range (Academic Model)
Very High (Severe)	96-100	41-100
High	80-95	31-40
Moderate	21-79	21-30
Low	5-20	11-20
Very Low (Minimal)	0-4	0-10

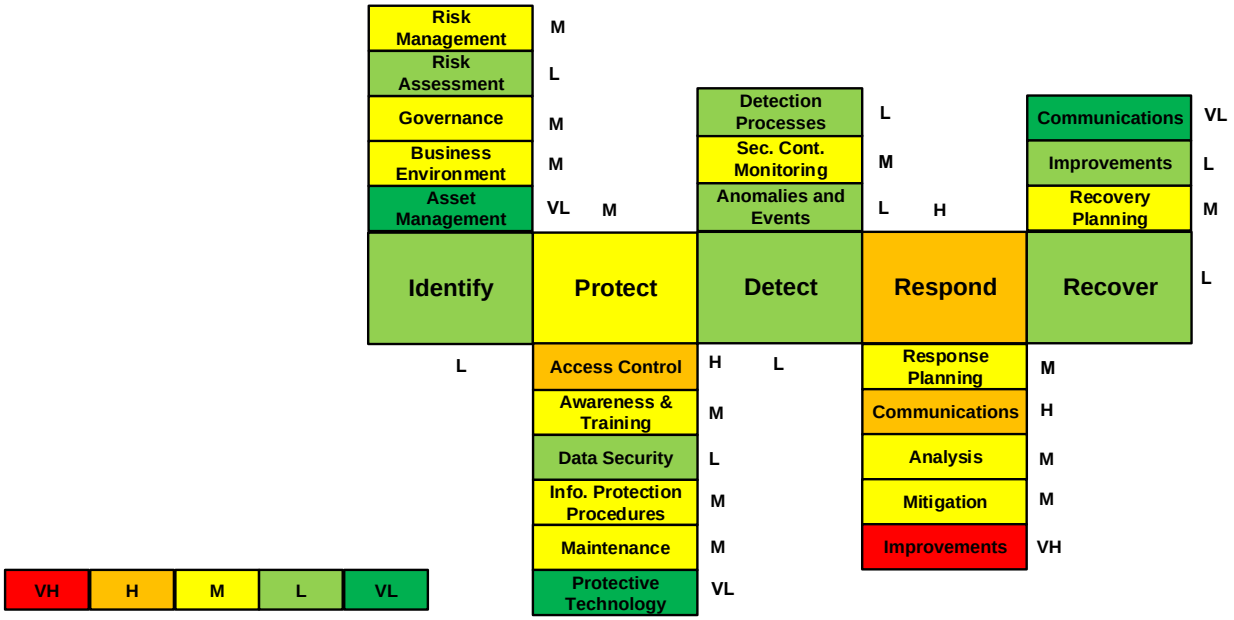
There are many ways in which the resulting information can be presented. One way is to show relative residual risk at the control objective level of the HITRUST CSF using an academic scoring model. An example of such a "scorecard" that can be manually generated using standard office productivity software is presented in Figure 2 on the following page.

Figure 2. Example HITRUST CSF Residual Risk Scorecard (Academic Model)



A similar, manually constructed view based on the NIST CSF functions and categories using a traditional scoring model is provided in Figure 3. Example NIST CsF Residual Risk Scorecard (Traditional Model).

Figure 3. Example NIST CsF Residual Risk Scorecard (Traditional Model)



Prioritization

HITRUST also provides implementation dependencies amongst CSF controls based on priority codes for federal controls[28] contained in NIST SP 800-53 r4. The priority codes indicate relative order of priority (sequencing) for implementation, which helps provide a more structured, phased approach by ensuring controls upon which other controls depend are implemented first.

Priority code sequencing, consistent with NIST SP 800-53 r4, is as follows:

- P1 – First (Control contains significant number of foundational requirements)
- P2 – Next (Control contains requirements that depend on the successful implementation of one or more foundational control requirements)
- P3 – Last (Control contains requirements that generally depend on the successful implementation of one or more priority 2 requirements)

The following table provides the HITRUST priority codes for all 135 CSF controls directly related to cybersecurity:

Table 9. Priority Codes

Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code
0.a	P1	01.o	P1	02.e	P1	05.e	P2	06.i	P1	08.i	P1	09.k	P1	09.z	P2	10.i	P2
01.a	P1	01.p	P2	02.f	P3	05.f	P3	06.j	P1	08.j	P1	09.l	P1	09.aa	P1	10.j	P2
01.b	P1	01.q	P1	02.g	P2	05.g	P3	07.a	P1	08.k	P1	09.m	P1	09.ab	P2	10.k	P1
01.c	P1	01.r	P1	02.h	P2	05.h	P3	07.b	P1	08.l	P1	09.n	P1	09.ac	P1	10.l	P2
01.d	P1	01.s	P1	02.i	P2	05.i	P1	07.c	P1	08.m	P1	09.o	P1	09.ad	P1	10.m	P1
01.e	P1	01.t	P3	03.a	P1	05.j	P1	07.d	P1	09.a	P1	09.p	P1	09.ae	P2	11.a	P1
01.f	P1	01.u	P2	03.b	P1	05.k	P1	07.e	P1	09.b	P1	09.q	P1	09.af	P1	11.b	P1
01.g	P2	01.v	P1	03.c	P1	06.a	P1	08.a	P1	09.c	P1	09.r	P2	10.a	P1	11.c	P1
01.h	P1	01.w	P1	03.d	P1	06.b	P1	08.b	P1	09.d	P1	09.s	P1	10.b	P1	11.d	P1
01.i	P1	01.x	P1	04.a	P1	06.c	P2	08.c	P1	09.e	P1	09.t	P2	10.c	P1	11.e	P1
01.j	P1	01.y	P1	04.b	P1	06.d	P2	08.d	P1	09.f	P1	09.u	P1	10.d	P1	12.a	P1
01.k	P1	02.a	P1	05.a	P1	06.e	P1	08.e	P1	09.g	P2	09.v	P1	10.e	P2	12.b	P1
01.l	P1	02.b	P1	05.b	P1	06.f	P1	08.f	P1	09.h	P1	09.w	P1	10.f	P1	12.c	P2
01.m	P1	02.c	P1	05.c	P1	06.g	P3	08.g	P2	09.i	P3	09.x	P1	10.g	P1	12.d	P1
01.n	P1	02.d	P1	05.d	P3	06.h	P3	08.h	P1	09.j	P1	09.y	P2	10.h	P1	12.e	P3

Whether or not these priority codes will be useful to an organization will depend on the specific deficiencies requiring CAPs. Self- and third-party assessors must also fully understand the requirements in order to understand their dependencies.

An organization should understand that CAP prioritization will depend on other factors unique to the organization, which cannot be addressed by an RMF like HITRUST or NIST. Examples

[28] NIST (2013). Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 80-53 r4, Wash., DC: Author, pp. D-1 – D-8. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

include available operational and capital budget, budget planning processes, architecture and infrastructure constraints, and even organizational culture and politics.

For the purposes of certification, HITRUST generally requires CAPs for all CSF requirements that score a 3 or below and for any requirement that is not fully implemented (i.e., not fully compliant for maturity level 3, Implemented).

To illustrate how risk and priority codes can be applied to CAP prioritization, consider a scenario in which an organization has an immature business continuity program and received the following HITRUST maturity scores for controls 12.a thru 12.e.

- 12.a, Including Info. Security in the Business Continuity Mgmt. Process: 50
- 12.b, Business Continuity and Risk Assessment: 75
- 12.c, Developing and Implementing Continuity Plans Including Info. Security: 50
- 12.d, Business Continuity Planning Framework: 50
- 12.e, Testing, Maintaining, Reassessing Business Continuity Plans: 38

CAPs would likely be required to address deficiencies with one or more requirement statements for controls 12.a, 12.c, 12.d and 12.e; however, for the sake of simplicity, assume one requirement specification for each control.

Risk and priority information for these four controls are provided in the next table.

Table 10. CAP Prioritization Example

CSF Control	Maturity Score (MS)	Impact Rating (IR)	Raw Risk Score (R)	Priority Code	Assigned Priority
12.a	50	3	25	P1	2
12.c	50	3	25	P2	3
12.d	38	3	31	P1	1
12.e	50	3	25	P3	4

The highest risk gap has a priority code of 1, so this CAP is assigned the highest priority. The three remaining controls have similar excessive residual risk, and so they may be ordered according to their priority codes: 12.a (P1), 12.c (P2) and 12.e (P3).

For more information on alternate risk treatments (i.e., transference, avoidance, and acceptance), refer to the HITRUST Risk Analysis Guide.[29]

Note, this step includes the following elements of the DHS risk analysis process as modified to accommodate use of a control framework:

- Rank risks and determine risk treatments
- Make contextual adjustments to likelihood & impact, if needed, as part of the corrective action planning process

[29] Cline, B. (2014b), App. A

Step 7: Implement Action Plan

Table 11. Step 7: Implement Action Plan Inputs, Activities, and Outputs

Step 7: Implement Action Plan		
Inputs	Activities	Outputs
1. Prioritized implementation plan 2. HITRUST RMF	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks using metrics or other suitable performance indicators	1. Project tracking data 2. New security measures implemented

The organization executes the CAP and tracks its progress over time, ensuring that gaps are closed and risks are monitored. CAPs can be used as the overarching document to track all capital (project) and operational work performed by the organization to address gaps in its Target Profile.

A complete CAP should include, at a minimum, a control gap identifier, description of the control gap, CSF control mapping, point of contact, resources required (dollars, time, and/or personnel), scheduled completion date, corrective actions, how the weakness was identified (assessment, CSF Assessor, date), date identified, and current status.

Note, this step includes the following element of the DHS risk analysis process as modified to accommodate use of a control framework: Implement corrective actions and monitor the threat environment.

Process Summary

This implementation approach can help organizations leverage the HITRUST RMF to establish a strong cybersecurity program or validate the effectiveness of an existing program. It enables organizations to map their existing program to the NIST CsF, identify improvements, and communicate results. It can incorporate and align with processes and tools the organization is already using or plans to use.

The process is intended to be continuous, repeated according to organization-defined criteria (such as a specific period of time or a specific type of event) to address the evolving risk environment. Implementation of this process should include a plan to communicate progress to appropriate stakeholders, such as senior management, as part of its overall risk management program. In addition, each step of the process should provide feedback and validation to previous steps. Validation and feedback provide a mechanism for process improvement and can increase the overall effectiveness and efficiency of the process. Comprehensive and well-structured feedback and communication plans are a critical part of any cybersecurity risk management approach.

Additional Resources to Support Framework Use Goals

The use of the HITRUST RMF along with other tools and approaches discussed above is an important step Healthcare Sector organizations can take to align their cybersecurity programs with existing sector-level goals and guidelines. The approaches below can also be used to increase knowledge and enhance cybersecurity practices.

- **Council on CyberSecurity (CsC) Critical Security Controls for Effective Cyber Defense:**[30] The Critical Controls for Effective Cyber Defense (the Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive attacks. They were developed and are maintained by a consortium of hundreds of security experts from across the public and private sectors. An underlying theme of the Controls is support for large-scale, standards-based security automation for the management of cyber defenses.
- **DHS Cyber Resilience Review (CRR):**[31] The CRR is a no-cost, voluntary, non-technical assessment to evaluate an organization's operational resilience and cybersecurity practices. The CRR may be conducted as a self-assessment or as an on-site assessment facilitated by DHS cybersecurity professionals. The CRR assesses enterprise programs and practices across a range of ten domains including risk management, incident management, service continuity, and others. The assessment is designed to measure existing organizational resilience and provide a gap analysis for improvement based on recognized best practices.
- **HHS Security Risk Assessment (SRA) Tool:**[32] ONC, in collaboration with the HHS Office for Civil Rights (OCR) and the HHS Office of the General Counsel (OGC), developed a downloadable tool to help guide organizations through the HIPAA risk assessment/analysis process. The SRA Tool presents a question about your organization's activities for each HIPAA standard and implementation specification, and then identifies what is needed to take corrective action for that particular item. Resources for each question help assessors understand the context of the question, consider the potential impacts to PHI if the requirement is not met, and provide the actual safeguard language of the HIPAA Security Rule. DISCLAIMER: The SRA Tool is provided for informational purposes only. Use of this tool is neither required by, nor guarantees, compliance with federal, state, or local laws. Please note that the information presented may not be applicable or appropriate for all healthcare providers and organizations. The Security Risk Assessment Tool is not intended to be an exhaustive or definitive source on safeguarding health information from privacy and security risks.
- **ISO 27799:**[33] ISO 27799:2008 specifies a set of detailed controls for managing health information security and provides health information security best practice guidelines. By implementing this International Standard, healthcare organizations and other custodians of health information will be able to ensure a minimum requisite level of security that is appropriate to their organization's circumstances and maintain the confidentiality, integrity, and availability of personal health information.
- **NIST HSR Toolkit:**[34] The NIST HIPAA Security Toolkit Application is intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment.

---

[30] http://www.counciloncybersecurity.org/critical-controls/
[31] https://www.us-cert.gov/ccubedvp/self-service-crr
[32] http://www.healthit.gov/providers-professionals/security-risk-assessment-tool
[33] http://www.iso.org/iso/catalogue_detail?csnumber=41298
[34] http://scap.nist.gov/hipaa/

Target users include, but are not limited to, HIPAA covered entities, business associates, and other organizations such as those providing HIPAA Security Rule implementation, assessment, and compliance services. Target user organizations can range in size from large nationwide health plans with vast information technology (IT) resources to small healthcare providers with limited access to IT expertise.

- **NIST SP 800-66:**[35] Federal guidance intended to help educate readers about information security terms used in the HIPAA Security Rule and improve understanding of the meaning of the security standards set out in the Security Rule; direct readers to helpful information in other NIST publications on individual topics addressed by the HIPAA Security Rule; and aid readers in understanding the security concepts discussed in the HIPAA Security Rule. DISCLAIMER: This publication does not supplement, replace, or supersede the HIPAA Security Rule itself.

[35] http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf

Informing Existing Sector Efforts

This Framework Guidance was developed to be intrinsically backwards compatible, meaning it can be used to enhance the success of existing sector-specific programs and inform sector-level goals and guidelines. The approaches below can be used to increase knowledge and enhance cybersecurity practices; the Framework can make them more effective.

- **Critical Infrastructure Cyber Community (C³) Voluntary Program:**[36] The C³ Voluntary Program is a public-private partnership aligning business enterprises and Federal, State, Local, Tribal, and Territorial (SLTT) governments to existing resources that will assist their efforts to use the Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management. Currently, there are many programs and resources available to critical infrastructure sectors and organizations that are looking to improve their cyber risk resilience. These resources are provided by many DHS and government-wide agencies and offices. The C³ Voluntary Program provides the central place to access that information. The C³ Voluntary Program is the coordination point within the Federal government to leverage and enhance existing capabilities and resources to promote use of the Framework. While the Framework is based on existing guidelines and standards, organizations may still need assistance in understanding its purpose, and how the Framework may apply to them. The C³ Voluntary Program will provide assistance to organizations of all types interested in using the Framework.
- **HPH Sector-Specific Plan:**[37] The HPH Sector-Specific Plan (SSP) is designed to guide the sector's efforts to improve security and resilience, and describes how the Chemical Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21 (PPD-21). The SSP reflects the overall strategic direction for the Chemical Sector and represents the progress made in addressing the sector's evolving risk, operating, and policy environments. As an annex to the National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013), this SSP tailors the NIPP's strategic guidance to the unique operating conditions and risk landscape of the HPH Sector.

[36] https://www.us-cert.gov/ccubedvp
[37] https://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf

Conclusion

This document serves as a foundation for how Healthcare Sector organizations, both nascent and mature, can leverage a series of resources to increase their use of the NIST CsF via the HITRUST RMF and, at minimum, increase their overall cybersecurity awareness. Specifically, the information provided in this document can help an organization assess their current cybersecurity practices, or lack thereof, provide tools to help identify gaps, and enable owners and operators to determine their cybersecurity goals. The NIST CsF in its entirety, released on February 12, 2014 can be accessed from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. The C^3 Voluntary Program, a compilation of various resources organized by the five core functions of the Framework, can be accessed from https://www.us-cert.gov/ccubedvp. For any questions related to this guidance, please e-mail Info@HITRUSTalliance.net. For any questions related to the NIST CsF or C^3 Voluntary Program, please e-mail CCubedVP@hq.dhs.gov.

Appendix A – Reference List

Bowen, P. and Kissel, R. (2007). Program Review for Information Security Management Assistance (PRISMA), NISTIR 7358, Wash., DC: NIST. Downloaded from http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf.

Cline, B. (2013a). Risk Management Frameworks: How HITRUST provides an efficient and effective approach to the selection, implementation, assessment and reporting of information security and privacy controls to manage risk in a healthcare environment. Frisco, TX: HITRUST. Downloaded from https://hitrustalliance.net/content/uploads/2015/03/HITRUST-RMF-Whitepaper-2015.pdf

Cline, B. (2013b). Using the HITRUST CSF to Assess Cybersecurity Preparedness, Frisco, TX: HITRUST. Downloaded from http://hitrustalliance.net/content/uploads/2014/05/HITRUST-Cybersecurity-Preparedness.pdf

Cline, B. (2014a). Healthcare's Model Approach to Critical Infrastructure Cybersecurity: How the Industry is Leading the Way with its Information Security Risk Management Framework. Frisco, TX: HITRUST. Downloaded from https://hitrustalliance.net/documents/csf_rmf_related/ImplementingNISTCybersecurityWhitepaper.pdf.

Cline, B. (2014b). Risk Analysis Guide for HITRUST Organizations and Assessors: A Guide for Self- and Third-party Assessors on the Application of HITRUST's Approach to Risk Analysis, Frisco, TX: HITRUST, pp. 9-12. Downloaded from https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf.

Cline, B. (2014c). Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection: Why risk analysis is crucial to HIPAA compliance and an overall information protection program, Frisco, TX: HITRUST. Downloaded from https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf.

Cline, B. (2014d). Using the HITRUST CSF to Assess Cybersecurity Preparedness. Frisco, TX: HITRUST. Downloaded from https://hitrustalliance.net/content/uploads/2014/06/HiTrustCSFCybersecurityTable.pdf.

Cline, B. (2015). HITRUST CSF Risk Factors: How HITRUST Uses and Updates Risk Factors to Help Healthcare Organizations Dynamically Tailor CSF Control and Create a Targeted, Common Baseline to Meet Their Information Protection Needs. Frisco, TX: HITRUST.

CM-SEI (2010). CMMI for Services (CMMI-SVC), V1.3, TR CMU/SEI-2010-TR-034, Hanscom AFB, MA: ESC (DoD), p. 23. Downloaded from http://www.sei.cmu.edu/reports/10tr034.pdf.

Council on CyberSecurity (2014). The Critical Security Controls for Effective Cyber Defense, Version 5.1. Downloaded from http://www.counciloncybersecurity.org/critical-controls/.

Department of Energy [DOE] (N.D). Energy Sector Cybersecurity Framework Implementation Guidance, Version 4 (DRAFT), Wash., D.C.: Author.

Department of Health and Human Services, HHS (2010). Guidance on Risk Analysis Requirements under the HIPAA Security Rule, Wash., DC: Author, p. 1. Downloaded from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

Department of Homeland Security [DHS] and DHHS (2010). Healthcare and Public Health Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan. Wash., DC: Author. Downloaded from http://www.dhs.gov/xlibrary/assets/nipp-ssp-healthcare-and-public-health-2010.pdf.

Exec. Order No. 13636, 3 C.F.R. 11739-11744 (2013). Downloaded from http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

Frederick, M. (2015). HITRUST vs. GRC Tools: Understanding the Differences and Total Cost of Ownership. Frisco, TX: HITRUST. Downloaded from https://hitrustalliance.net/mycsf/.

Government Accountability Organization [GAO] (2011). Critical Infrastructure Protection: Cybersecurity Guidance is Available, but More Can Be Done to Promote Its Use, Wash., DC: Author. Downloaded from http://www.gao.gov/products/GAO-12-92

Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification, 45 CFR Pts 160, 162, and 164 (2006, as amended). Downloaded from http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

National Institute of Standards and Technology [NIST] (2009). Recommended Security Controls for Federal Information Systems and Organizations, NIST SP 800-53 r3, Wash., DC: Author.

NIST (2012). Guide for Conducting Risk Assessments, NIST SP 800-30 r1, Wash., DC: Author, p. 23. Downloaded from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

NIST (2013). Security and Privacy Controls for Federal Information Systems and Organizations, NIST SP 80-53 r4, Wash., DC: Author. Downloaded from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

NIST (2014). Framework for Improving Critical Infrastructure Cybersecurity, Version 1. Wash., DC: Author. Downloaded from http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

NIST (2014). NIST Releases Cybersecurity Framework Version 1.0. Downloaded from http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm

Scholl, M., Stine, K., Hash, J., et al. (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, NIST SP 800-66 r1, Wash., DC: NIST. Downloaded from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.

Appendix B – Glossary of Terms

Term	Definition
Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information.
Adversary [DHS Risk Lexicon]	Individual, group, organization or government that conducts or has the intent to conduct detrimental activities.
Alternate Control [HITRUST]	See Compensating Control.
Analysis Approach [NIST SP 800-53 r4]	The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated.
Assessment	See Security Control Assessment or Risk Assessment.
Attack [CNSSI No. 4009]	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself.
Availability [44.U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Compensating Security Control [CNSSI No. 4009, adapted]	A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. Synonymous with Alternate Control [HITRUST].
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Criticality [NIST SP 800-60]	A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. Note criticality is often determined by the impact to the organization due to a loss of integrity or availability.
Cyber Attack [NISTIR 7298 r2]	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Term	Definition
Cyber Incident [CNSSI No. 4009]	Actions through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See incident.
Cybersecurity [CNSSI No. 4009]	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.
Cyberspace [CNSSI No. 4009]	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.
Defense-in-Breadth [CNSSI No. 4009]	A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).
Defense-in-Depth [CNSSI No. 4009]	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Impact Level [CNSSI No. 4009]	The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.
Impact Value [CNSSI No. 1253]	The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high.
Incident [CNSSI No. 4009]	An occurrence that results in actual or potential jeopardy to the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Information Security Risk [NIST SP 800-53 r4]	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems. See Risk.

Term	Definition
Information System-Related Security Risk [CNSSI No. 4009, adapted]	Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, and other organizations. A subset of Information Security Risk. See Risk.
Integrity (44 U.S.C., Sec. 3542)	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Likelihood of Occurrence [CNSSI No. 4009, adapted]	A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.
Overlay [NIST SP 800-53 r4]	A specialized set of controls tailored for specific types of missions/business functions, technologies, or environments of operation.
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. Synonymous with Corrective Action Plan.
Quantitative Assessment [DHS Risk Lexicon]	A set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.
Qualitative Assessment [DHS Risk Lexicon]	A set of methods, principles, or rules for assessing risk based on non-numerical categories or levels.
Repeatability [NIST SP 800-53 r4]	The ability to repeat an assessment in the future, in a manner that is consistent with, and hence comparable to, prior assessments.
Reproducibility [NIST SP 800-53 r4]	The ability of different experts to produce the same results from the same data.
Residual Risk [CNSSI No. 4009]	Portion of risk remaining after security measures have been applied.
Risk Analysis [NISTIR 7298 r2]	The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Term	Definition
Risk Assessment [CNSSI No. 4009]	The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Factor [NIST SP 800-53 r4]	A characteristic in a risk model as an input to determining the level of risk in a risk assessment.
Risk Management [CNSSI No. 4009, adapted]	The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.
Risk Management Framework [HITRUST]	A common taxonomy and standard set of processes, procedures, activities, and tools that support the identification, assessment, response, control and reporting of risk
Risk Mitigation [CNSSI No. 4009]	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. [A subset of Risk Response.]
Risk Model [NIST SP 800-53 r4]	A key component of a risk assessment methodology—in addition to the assessment approach and analysis approach—that defines key terms and assessable risk factors.
Risk Monitoring [NIST SP 800-39]	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.
Risk Response [NIST SP 800-39, adapted]	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, or other organizations. See Course of Action. Synonymous with Risk Treatment.
Root Cause Analysis [NIST SP 800-53 r4]	A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.
Scaling [HITRUST]	The act of applying specific considerations related to the size and financial/resource capabilities/constraints of an organization on the applicability and implementation of individual security and privacy controls in the control baseline. A subset of Scoping.

Term	Definition
Scoping [NIST SP 800-53, adapted]	The act of applying specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security and privacy controls in the control baseline.
Security Controls [CNSSI No. 4009, adapted]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an organization and/or information system(s) to protect information confidentiality, integrity, and availability.
Security Control Assessment [NIST SP 800-39; CNSSI No. 4009, adapted]	The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security Control Baseline [CNSSI No. 1253, adapted]	A set of information security controls that has been established through information security strategic planning activities intended to be the initial security control set selected for a specific organization and/or system(s).
Semi-Quantitative Assessment [DHS Risk Lexicon]	Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. Synonymous with Quasi-Quantitative Assessment.
Tailored Security Control Baseline [NIST SP 800-39]	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See Tailoring.
Tailoring [NIST SP 800-53; CNSSI No. 4009]	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.
Threat [CNSSI No. 4009, adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.
Threat Assessment [CNSSI No. 4009]	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Term	Definition
Threat Event [NIST SP 800-53 r4]	An event or situation that has the potential for causing undesirable consequences or impact.
Threat Scenario [NIST SP 800-53 r4]	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.
Threat Source [CNSSI No. 4009]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.
Vulnerability [CNSSI No. 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.
Vulnerability Assessment [CNSSI No. 4009]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Appendix C –NIST CsF Basics

NIST CsF Structure and Terminology

For an industry, sector or organization to implement the NIST CsF one must understand that it relies on existing standards, guidance, and best practices to achieve specific outcomes meant to help organizations manage their cybersecurity risk.[38] The NIST CsF provides a common language and mechanism to:

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

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

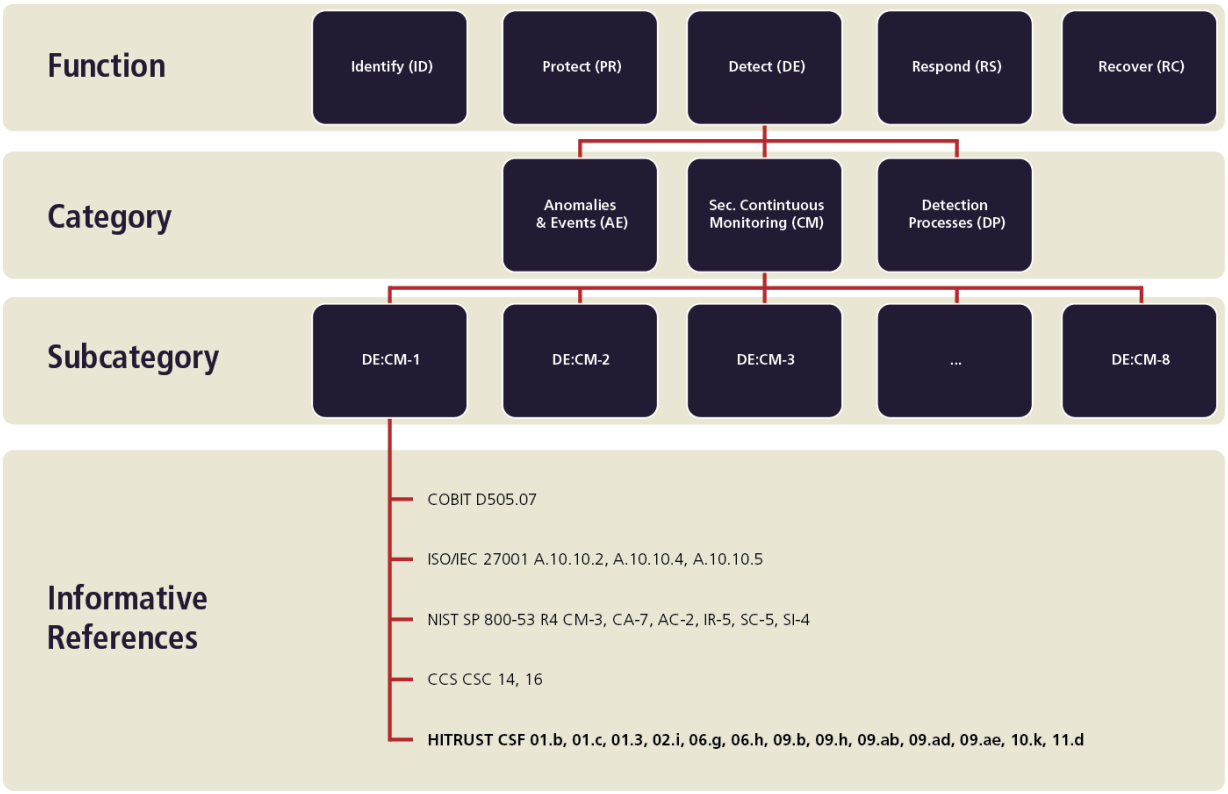
The NIST CsF consists of three main components: the Framework Core, Framework Implementation Tiers, and the Framework Profile.[39] Each component is designed to strengthen the connection between business drivers and cybersecurity activities. The Core, Tiers, and Profiles represent the key structure of the Framework, which this document frequently references.

Core

The NIST CsF Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors.[40] The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level.

[38] NIST (2014), p. 4
[39] Ibid., pp. 4-5
[40] Ibid.

Figure 4. Framework Core Structure



The four Core elements are:[41]

1. **Functions:** Functions provide five focus areas that can shape cybersecurity activities at a strategic level for an organization's cybersecurity management. The Functions aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. Although the NIST CsF leverages the risk management framework outlined in NIST's Special Publication 800-series documents, it is different in several respects. The key difference here is that the NIST CsF functions categorize cybersecurity requirements using what is essentially an incident management process. The five functions are:[42]

    - **Identify** - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function lay the foundation for effective Framework use.
    - **Protect** - Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function limits potential cybersecurity events.
    - **Detect** - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event, enabling the timely discovery of cybersecurity incidents.

[41] Ibid., pp. 4-5.
[42] Ibid., pp. 8-9.

- **Respond** - Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event.
- **Recover** - Develop and implement appropriate activities for resilience planning and restore any capabilities or services impaired by the cybersecurity event.

When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

2. **Categories:** The Framework decomposes functions into categories, which are cybersecurity outcomes that closely relate to programmatic needs and specific activities. Categories add an additional layer of specificity within the Core Functions. In the Identify Function for instance, categories include Governance, Business Environment, and Asset Management.
3. **Subcategories:** Subcategories further break down a particular category into specific outcomes of a technical or management activity. Subcategories also provide a set of results that help support achievement of each category's outcomes. Examples of Subcategories include "External information systems are catalogued," "Data-at-rest is protected," and "Notifications from detection systems are investigated."
4. **Informative References:** References are specific sections of standards, guidelines, and practices common among critical infrastructure sectors such as NIST and the Council on CyberSecurity (CCS) Critical Security Controls (CSC) for Cyber Defense, as shown for subcategory DE.CM-1 in Figure 4. Note the figure also reflects HITRUST CSF controls in the last line for illustration.

Implementation Tiers

Implementation tiers provide context on how an organization views cybersecurity risk and the processes in place to manage that risk.[43] Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers characterize an organization's practices over a range, from Partial (Tier 1) to Adaptive (Tier 4). These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.

Profiles

NIST CsF Profiles represent outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories.[44] A profile can be characterized as the alignment of standards, guidelines, and practices to the NIST CsF Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" Profile (the "to be" state). To develop a Profile, an organization can review all of the Categories and Subcategories and, based on business drivers and a risk assessment, determine which are most important; they can add Categories and Subcategories as needed to address the organization's risks. The Current Profile can then be used to support prioritization and measurement of progress toward the Target Profile, while factoring in other business needs including cost-

[43] Ibid., pp. 11-12
[44] Ibid., p. 12

effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

Refer to the *Framework for Improving Critical Infrastructure Cybersecurity* for more information on the NIST CsF.

Generic Implementation

Within the Healthcare Sector, various organizations already have risk management programs of some type with varying levels of maturity. In many cases, organizations' risk assessment activities already align with the NIST CsF, and implementation is largely a matter of translating elements of current activities and programs to the NIST CsF Core and Implementation Tiers.

NIST recommends using a seven-step process for implementation.[45]

- Step 1: Prioritize and scope organizational components for framework adoption
- Step 2: Identify systems and existing risk management approaches within the scope
- Step 3: Create a current risk management profile (Current Profile)
- Step 4: Conduct a risk assessment
- Step 5: Create a desired risk management profile based on assessment results (Target Profile)
- Step 6: Develop a prioritized action plan of controls and mitigations (Action Plan)
- Step 7: Implement the Action Plan

The diagram below shows these steps and the key activities completed within each step. The approach can and should be an iterative process, repeated to address the evolving risk environment.

Figure 5. Generic Implementation Process

In addition to these steps, implementation should include a plan to communicate progress to appropriate stakeholders, such as senior management, as part of the organization's risk

[45] NIST (2014), pp. 13-15

management program. Each step of the process should provide feedback and validation to previous steps, which can facilitate process improvement and increase the overall effectiveness and efficiency of the process. Comprehensive and well-structured feedback and communication plans are a critical part of any cybersecurity risk management approach.

The following provides additional context, explanation, and guidance from the NIST CsF document for each step.[46]

Step 1: Prioritize and Scope

The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance.

Step 2: Orient

The organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then identifies threats to, and vulnerabilities of, those systems and assets.

Step 3: Create a Current Profile

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved.

Step 4: Conduct a Risk Assessment

The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations seek to incorporate emerging risks along with threat and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities.

Step 5: Create a Target Profile

The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile.

Step 6: Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps. Next it creates a prioritized action plan to address those gaps that draws upon mission drivers, a cost/benefit analysis, and understanding of risk to achieve the outcomes in the Target Profile. The organization then determines resources necessary to address the gaps. Using Profiles in

[46] Ibid.

this manner enables the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan

The organization determines which actions to take in regards to any existing gaps identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices work best for their needs, including those requirements that are sector or organization-specific.

An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the Current Profile, subsequently comparing the Current Profile to the Target Profile. Organizations may also utilize this process to align their cybersecurity program with their desired Framework Implementation Tier.

Appendix D – Healthcare's Implementation of the NIST CsF

Compliance Drivers

Regulatory compliance is arguably one of the most significant drivers for cybersecurity and information protection in the Healthcare Sector. And amongst all the regulations applicable to the Sector, the Health Insurance Portability and Accountability Act (HIPAA)[47] is the biggest driver of all.

Unfortunately, "HIPAA compliance" and "HIPAA compliant" have probably been some of the most overused yet least understood terms in the healthcare industry. This is because the HIPAA Security Rule provides numerous standards and implementation specifications for administrative, technical and physical safeguards that, despite what the terms imply, lack the prescription necessary for actual implementation by a healthcare organization. However, this approach was necessary as no two healthcare organizations are exactly alike, which means no single set of information protection requirements could possibly apply across the entire industry. In other words, one size truly does not fit all.

To ensure the implementation of a comprehensive set of 'reasonable and appropriate' safeguards to provide for the 'adequate' protection of health information by a particular covered entity or business associate, DHHS requires organizations subject to the HIPAA Security Rule to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information [(ePHI) created, received, maintained or transmitted to][48] … protect against any reasonably anticipated threats or hazards to the security or integrity of such information."[49]

Unfortunately, many of these covered entities and business associates do not conduct a valid risk analysis but instead rely on implementing safeguards that simply address the Security Rule's remaining standards and implementation specifications, which has resulted in wildly varying information protection programs amongst these organizations, including those of similar size and scope, due to the relatively high level or "objective" nature of the requirements.

The problem organizations encounter by not performing a valid risk analysis can best be demonstrated by looking at how NIST SP 800-66 r1[50] maps the HIPAA Security Rule requirements against NIST's comprehensive control framework,[51] which is necessarily based on such a risk analysis for information with common information protection needs. Of all controls listed, regardless of selection for a particular NIST control baseline, only about half of them are mapped to the HIPAA Security Rule.[52] In addition, there are 55 specific NIST SP 800-53 r4 controls[53]—also common to r3—that are referenced by the NIST CsF but do not map to the

---

[47] HIPAA Administrative Simplification, 45 CFR Pts 160, 162, and 164 (2006, as amended).
[48] Ibid., § 164.308(a)(1)
[49] Ibid., § 164.306(a)(2)
[50] Scholl, M., Stine, K., Hash, J., et al. (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, NIST SP 800-66 r1, Wash., DC: NIST. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf.
[51] NIST (2009). Recommended Security Controls for Federal Information Systems and Organizations, NIST SP 800-53 r3, Wash., DC: Author.
[52] Cline, B. (2014c). Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection: Why risk analysis is crucial to HIPAA compliance and an overall information protection program, Frisco, TX: HITRUST, pp. 5-6. Retrieved from http://hitrustalliance.net/content/uploads/2015/09/RiskVsComplianceWhitepaper.pdf.
[53] NIST (2013), App. F.

HIPAA standards and implementation specifications in NIST SP 800-66 r1. This means that such an approach to compliance with the HIPAA Security Rule would result in a failure to address all the threats a federal healthcare organization might reasonably anticipate.

The same is true for non-federal organizations. The HITRUST CSF harmonizes multiple, relevant information security and privacy regulations, frameworks, and best-practice standards relevant to healthcare, including the controls contained in NIST SP 800-53 r4. But despite the additional healthcare-relevant content, only 98 of 135 or 73% of HITRUST CSF security controls map directly to the HIPAA Security Rule.[54] This is because the HITRUST CSF, like NIST, addresses a more complete range of threats to healthcare information.

This position also appears to be supported by DHHS, which states in their HIPAA risk analysis guidance that "Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule."[55]

Approach to Risk Analysis and Risk Management

Regardless of the risk management model used, risk analysis is generally the first step in the risk management process. According to NIST,[56] risk assessment (synonymous with analysis[57]) consists of five steps:

- Identify threat sources and events
- Identify vulnerabilities and predisposing conditions
- Determine likelihood of occurrence
- Determine magnitude of impact
- Determine risk

The NIST model is also consistent with DHHS' risk analysis guidance, which requires organizations to (iteratively):

- Scope the assessment to include all ePHI
- Identify & document all assets with ePHI
- Identify & document all reasonably anticipated threats to ePHI
- Assess all current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of a threat occurrence
- Determine the level of risk
- Document assigned risk levels and corrective actions[58]

However, many organizations fall short in conducting their risk analysis for many reasons, not the least of which is a general lack of executive sponsorship and priority within the organization.

---

[54] Exceptions include but are not limited to 01.w, Sensitive System Isolation; 05.f, Contact with Authorities; 05.j, Addressing Security When Dealing with Customers; 08.m, Removal of Property; 09.y, On-line Transactions; 09.ac, Protection of Log Information; 09.af, Clock Synchronization; 10.b, Input Data Validation; 10.e, Output Data Validation; 10.h, Control of Operational Software, and 10.k, Change Control Procedures. Reference mappings available from http://hitrustalliance.net/content/uploads/2014/05/CSF-HIPAA-Matrix-v3-CSF-HIPAA-Primary_Secondary.pdf.

[55] DHHS (2010). Guidance on Risk Analysis Requirements under the HIPAA Security Rule, Wash., DC: Author, p. 1. Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

[56] NIST (2012), p. 23.

[57] Ibid., p. B-9.

[58] DHHS (2010), pp. 5-7

Some of the reasons specifically related to the risk analysis model include, but are not limited to, the following:

- Incomplete asset inventory
- Failure to categorize assets properly
- Limited or no understanding of asset value
- Failure to enumerate/address all reasonably anticipated threats
- Unable to determine likelihood of a threat occurrence or impact
- Control effectiveness interpreted as risk
- No documentation of risk treatments, especially of risk acceptance
- Failure to address corrective actions for all risks requiring mitigation

Of these, the threat and impact analyses are perhaps the most difficult. From a quantitative viewpoint, the process of determining the likelihood of a threat occurrence is virtually impossible for many—if not most—Healthcare Sector organizations, and not always due to a lack of expertise. Unless actuarial-type information is available, the likelihood a threat-source will successfully exploit one or more vulnerabilities cannot be calculated with any level of precision. In the case of a human threat actor, likelihood is also dependent on the motivation of the threat source and the difficulty or cost associated with exploiting one or more vulnerabilities to achieve the actor's objectives.

An alternative to this traditional approach to risk analysis is to rely on a comprehensive control framework, which is already built upon a broad analysis of threats faced by similar types of organizations with information requiring similar levels of protection using similar information technologies. This is the approach employed by the U.S. intelligence community (IC), Department of Defense (DoD) and civilian agencies of the federal government with their respective information security control and risk management frameworks (currently being integrated under a Joint Task Force Initiative). To understand how this works, one must understand how risk analysis supports the overall risk management process. Although several models exist, the activities can be distilled into a basic four-step model.

Step 1—Identify Risks and Define Protection Requirements: The objective of this step is to determine the risks to information and information assets that are specific to the organization. Risks can be identified through the analysis of regulations and legislative requirements, breach data for similar organizations in the industry, as well as an analysis of current architectures, technologies, market trends, and related threats. The end result of this analysis should be a prioritized list of high-risk areas and an overall control strategy to minimize the risk to the organization from the use of PHI and other sensitive or business critical information in terms of overall impact to the organization. The HITRUST RMF, through the CSF, rationalizes relevant regulations and standards into a single overarching control framework to help healthcare organizations meet healthcare clinical and business objectives and satisfy multiple regulatory and other compliance requirements.

Step 2—Specify Controls: The next step after the risk analysis is to determine a set of reasonable and appropriate safeguards an organization should implement in order to adequately manage information security risk. The end result should be a clear, consistent, and detailed/prescriptive set of control recommendations that are customized for the healthcare organization. A control-based risk management framework will provide a comprehensive control catalog as well as specific criteria for the selection of a baseline set of controls, which is performed in this step. HITRUST built the CSF to accommodate multiple control baselines, and controls are assigned to specific baselines using three risk factors:

- Organizational type and size (e.g., a physician practice with fewer than 60,000 visits per year)
- System requirements (e.g., the system stores ePHI, is accessible from the Internet, and processes fewer than 6,750 transactions per day)
- Regulatory requirements (e.g., subject to Federal Trade Commission (FTC) Red Flags Rule and PCI-DSS compliance). The result is a healthcare industry-specific baseline, which can be further tailored to an organization's specific clinical, business and compliance requirements

Step 3—Implement and Manage Controls: Controls are implemented through an organization's normal operational and capital budget and work processes with board-level and senior executive oversight using existing governance structures and processes. A risk management framework will provide guidance and tools for the implementation of the framework, including the controls specified in Step 2. HITRUST trains third-party consulting and assessment firms in the CSF and CSF Assurance Program methodologies and tools so that they may offer CSF implementation support, as recommended by OCR, to healthcare provider organizations that lack the capability to implement and assess information security and privacy controls.

Step 4—Assess and Report: The objective of this last step is to assess the efficacy of implemented controls and the general management of information security against the organization's baseline. The end result of these assessment and reporting activities is a risk model that assesses internal controls, and the controls of business associates, based on the risk factors identified in Step 2. It should also provide common, easy-to-use tools that address requirements and risk without being burdensome, support third-party review and validation, and provide common reports on risk and compliance.

This process is then repeated by evaluating the effectiveness of existing safeguards and any new threats that may have materialized, which then results in the selection of new safeguards and/or the improvement of existing ones.

For the purpose of this guidance, however, one only need focus on the first two steps. As with any process model, the output of one step is the input of the second. Subsequently, one can see that the whole point of conducting a risk analysis is to determine a specific set of reasonable and appropriate controls that will provide adequate information protection, as HIPAA requires. By applying a baseline set of controls from a comprehensive control framework developed from an analysis of common threats to specific types of information using common technologies by similar organizations, one can be assured the organization is providing a known, minimally acceptable (i.e., adequate) level of protection for this information.

It's important to note, however, that organizations are also expected to identify any unique threats it may face and address them accordingly. Fortunately, the selection of a control baseline reduces the problem space for the risk analysis required to create an organizationally-unique overlay for the baseline as discussed in NIST SP 800-53 r4,[59] and subsequently makes the risk analysis more tractable. Successive iterations of the risk analysis, when required, are then limited to changes in the organization and the threat environment, as with the traditional approach. One can then focus on managing excessive residual risk—the risk that remains after all efforts have been made to mitigate, eliminate, or transfer risks to their organization—by ensuring the selected safeguards are fully implemented and operating effectively.

[59] NIST (2013), pp. 40-41

The risk analysis guidance from HHS can then be modified to support the use of a comprehensive control framework built upon an analysis of common threats to common classes of information and technologies, as follows:

- Conduct a complete inventory of where ePHI lives
- Perform a BIA on all systems with ePHI (criticality)
- Categorize & evaluate these systems based on sensitivity & 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 & impact, if needed, as part of the corrective action planning process
- Implement corrective actions and monitor the threat environment

Considering the sensibility of this approach, one might ask why the use of a control baseline from a comprehensive control framework was not addressed in the original HIPAA Security Rule. The answer is quite simple: no healthcare-specific framework existed at the time, and DHHS does not endorse any one framework or approach over another, including NIST. However, they do recognize the value added by such use.

While OCR does not endorse any particular credentialing or accreditation program, we certainly encourage covered entities and business associates to build strong compliance programs internally. Many of these credentialing/accreditation programs can help them do so…. OCR considers mitigation and aggravating factors when determining the amount of a civil monetary penalty, and these include the entity's history of prior compliance. An entity with a strong compliance program in place, with the help of a credentialing/ accreditation program or on its own, would have that taken into account when determining past compliance. "[60]

According to NIST, the implementation of risk management programs also offers organizations the ability to quantify and communicate changes to their cybersecurity programs.[61] The NIST CsF uses risk management processes to allow organizations to inform and prioritize these change decisions and supports recurring risk assessments and validation of business requirements that help define their Target Profiles.

[60] http://omnibus.healthcareinfosecurity.com/how-texas-boosting-hipaa-compliance-a-6800
[61] NIST (2014), p. 5

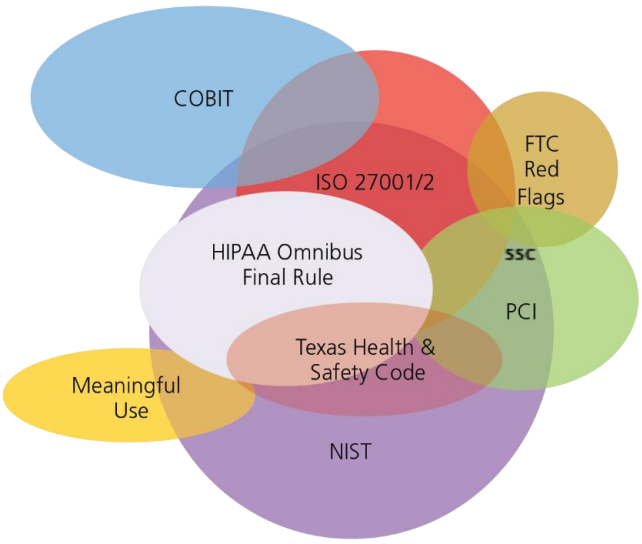
Relationship to NIST CsF

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 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 Figure 6, which, when integrated and harmonized, can often be mutually reinforcing when intelligently applied in the intended environment.

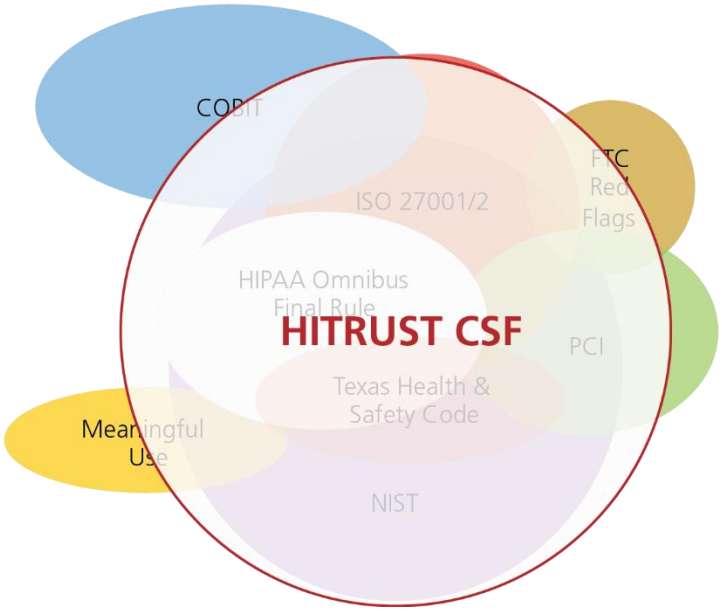
Figure 6. Overlap of Multiple Legislative, Regulatory and Other Requirements



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 Figure 7, and ultimately meet due care and due diligence requirements for the adequate protection of health information.[62]

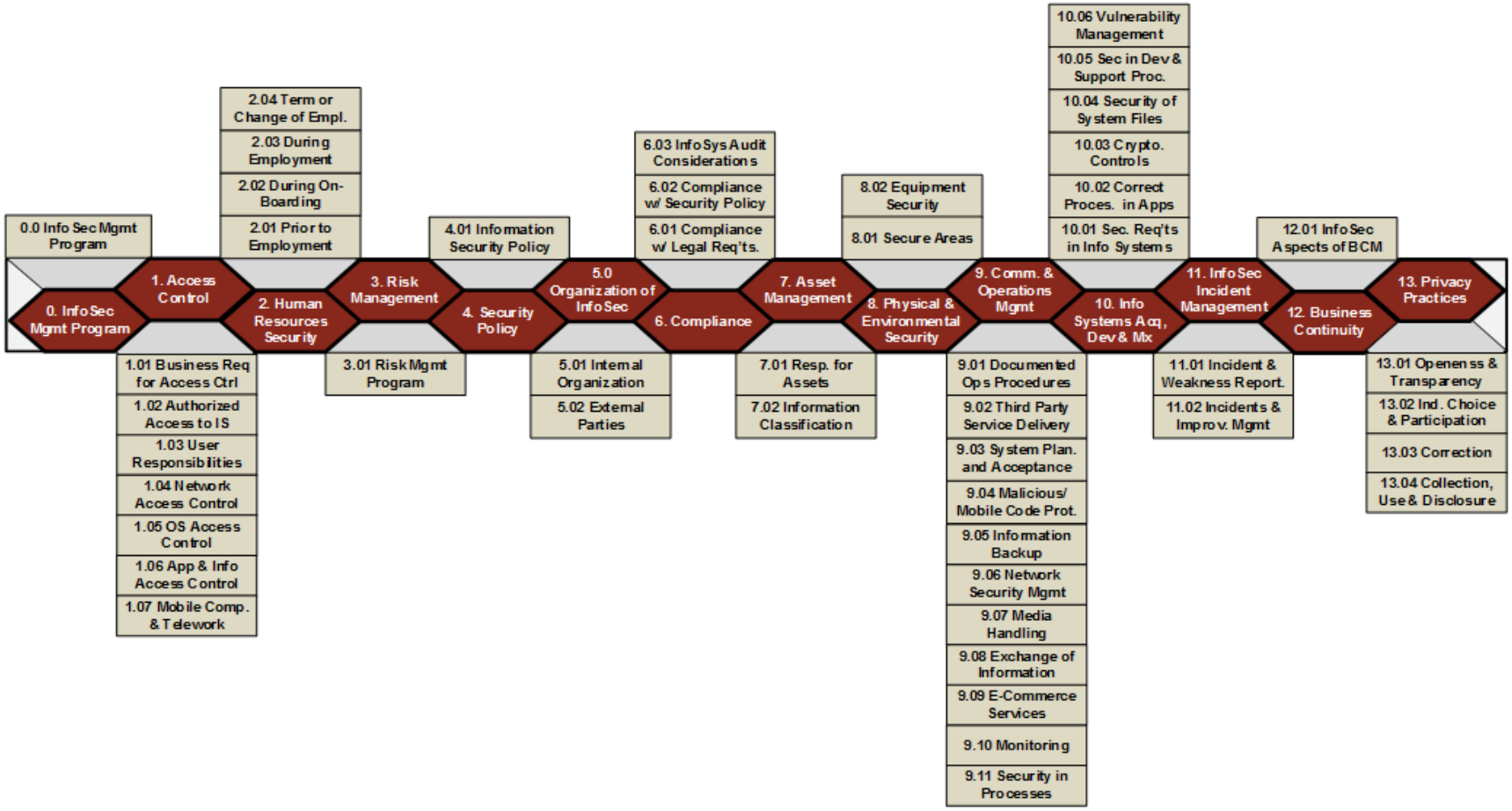
[62] While the focus of the healthcare industry is on protected health information (PHI), this guidance applies to the protection of any confidential or otherwise sensitive information and care-delivering technologies (e.g., biomed) as part of an organization's overall cybersecurity and information protection program.

Figure 7. Healthcare's Cybersecurity and Information Protection Framework



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), as shown in Figure 8. HITRUST CSF Structure, on the following page.

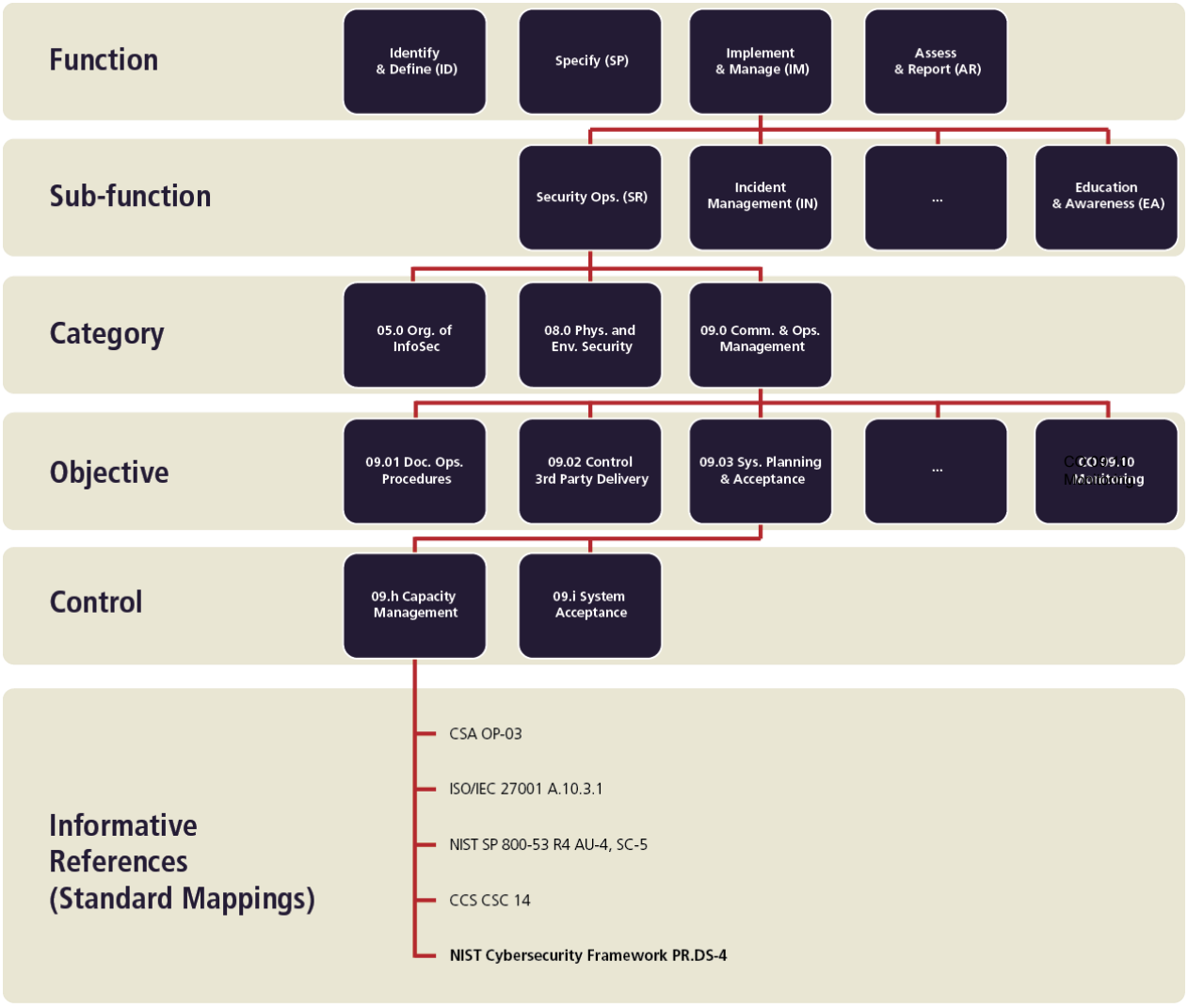
Figure 8. HITRUST CSF Structure



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).

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 Figure 9.

Figure 9. HITRUST RMF/CSF Core Structure

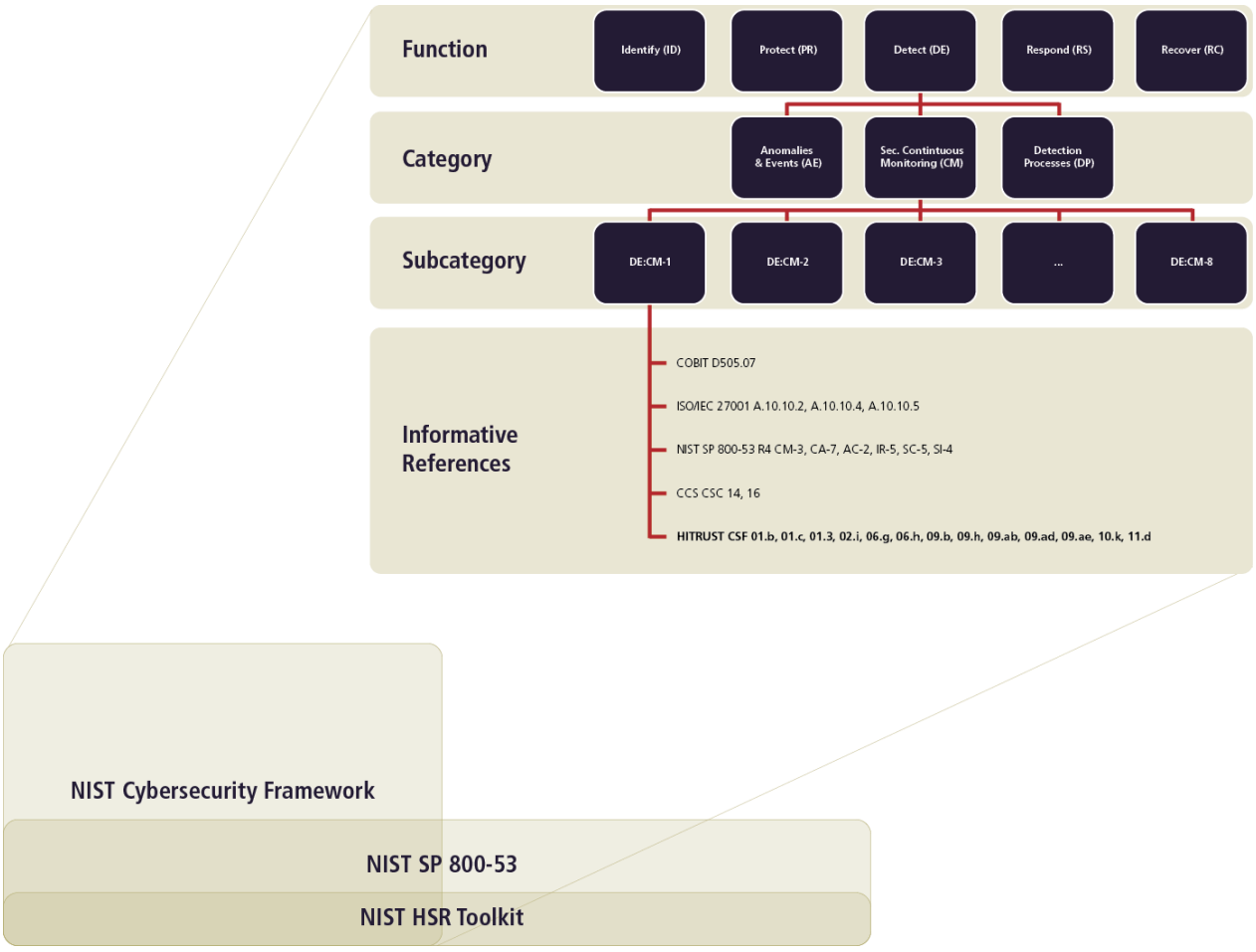


But there are a few differences between the two frameworks as depicted. One is that the functions and sub-functions listed in the figure are described in the HITRUST RMF, and the categories, objectives, controls, and standard mappings are contained in the HITRUST CSF itself. Another is that the HITRUST 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 provided in Appendix E – NIST CsF and HITRUST CSF Mapping.

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[63] as shown in Figure 10. Note, one could also incorporate other tools such as the DHHS Security Risk Assessment (SRA) Toolkit[64] at this level.

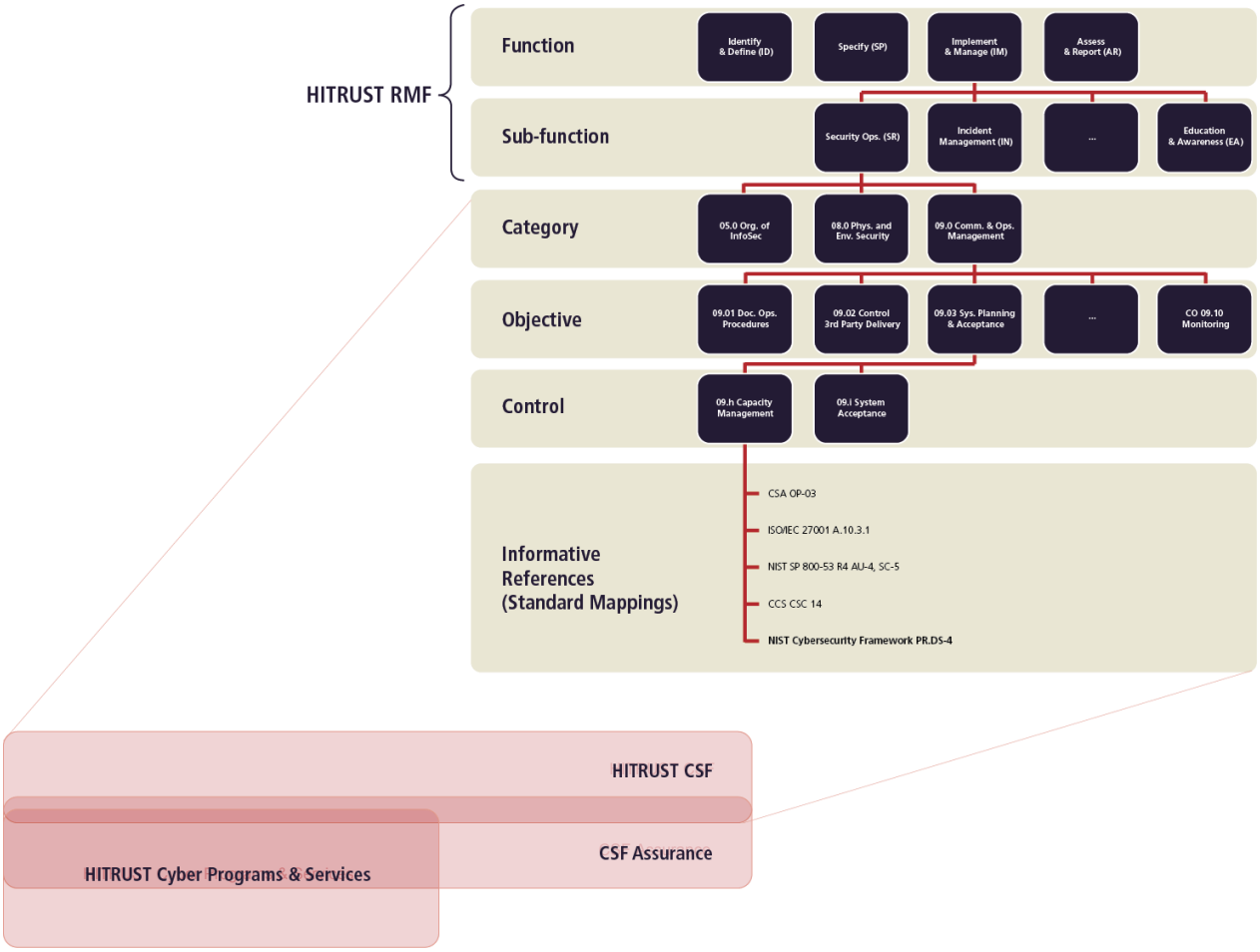
Figure 10. Depth and Breadth of the NIST CsF and Supporting Resources for Healthcare



63 http://scap.nist.gov/hipaa/
64 http://www.healthit.gov/providers-professionals/security-risk-assessment-tool

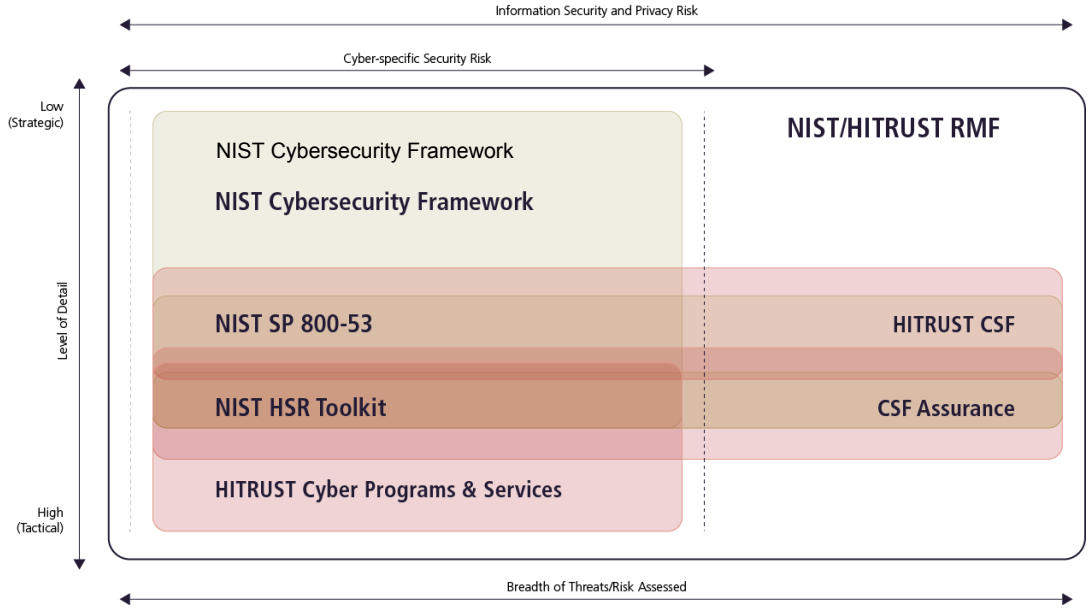
And, as with the NIST CsF, the HITRUST CSF can be similarly represented for depth and breadth of coverage. HITRUST provides industry-specific cyber intelligence and provides a mechanism for organizations to share information and collaborate on responses to specific incidents. These capabilities are included in Figure 11, 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.

Figure 11. Depth and Breadth of the HITRUST CSF and Supporting Resources for Healthcare



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 Figure 12.

Figure 12. Comparing Depth & Breadth of NIST and HITRUST Framework Coverage



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 provides additional information to address "gaps" in the NIST CsF, as recommended.

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[65] is based on a control maturity model described in NIST Interagency Report (IR) 7358, Program Review of Information Security Management Assistance (PRISMA),[66] 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.[67] 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.

---

[65] Cline, B. (2014b), pp. 9-12
[66] Bowen, P. and Kissel, R. (2007). Program Review for Information Security Management Assistance (PRISMA), NISTIR 7358, Wash., DC: NIST. Retrieved from http://csrc.nist.gov/publications/nistir/ir7358/NISTIR-7358.pdf.
[67] CM-SEI (2010). CMMI for Services (CMMI-SVC), V1.3, TR CMU/SEI-2010-TR-034, Hanscom AFB, MA: ESC (DoD), p. 23. Retrieved from http://www.sei.cmu.edu/reports/10tr034.pdf.

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 the organizational units and systems within scope of the assessment. For example, are all elements of a particular requirement statement 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.

Table 12. Maturity Level Requirements

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 • 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

Maturity Level	Points	General Requirements
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
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), descriptions for which are provided in Table 13.

Table 13. Maturity Level Scoring Model

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 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 in Table 14.

Table 14. Maturity Score to Rating Conversion

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 in Table 15.

Table 15. Maturity Rating Descriptions

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 HITRUST 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 **many** of these control specifications are routinely measured to ensure they function as intended and as required by the HITRUST 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, implemented, and routinely measured to ensure they function as intended and as required by the HITRUST 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 HITRUST 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 HITRUST 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 HITRUST 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. Table 16 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.

Table 16. Comparison of HITRUST Maturity and NIST Implementation Tiers

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-

NIST CsF Tiers	Cybersecurity Implementation Tier Description	Approximate HITRUST Maturity Levels	Approx. HITRUST Maturity Rating
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 role in "ecosystem" but has not formalized capabilities to interact/share info externally.	Level 1 – Partial Level 2 – Compliant Level 3 – Compliant Level 4 – Non-compliant Level 5 – Non-compliant	3- to 3+
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).

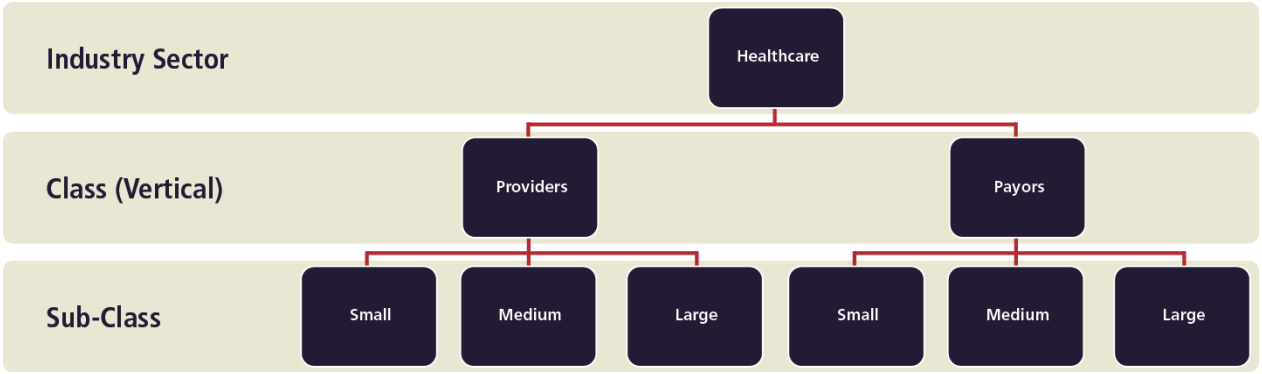
HITRUST further expands on the evaluation of maturity by proposing a multidimensional model that considers an organization's implementation of specific classes of cyber-relevant controls, overall risk management, and its ability to consume, share, and ultimately act upon threat intelligence in a meaningful way. An explanation of this model is provided in Appendix H – Cybersecurity Preparedness Maturity Model.

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,[68] 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[69] to tailor the initial comprehensive baseline[70] 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 that 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. Figure 13 provides 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.

Figure 13. Illustrative Industry Sector Classes and Sub-classes



[68] An overlay is "a fully specified set of security controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance … for community-wide use or to address specialized requirements, technologies, or unique missions/environments of operation." NIST (2013, p.40)
[69] Cline, B. (2015). HITRUST CSF Risk Factors: How HITRUST Uses and Updates Risk Factors to Help Healthcare Organizations Dynamically Tailor CSF Control and Create a Targeted, Common Baseline to Meet Their Information Protection Needs. Frisco, TX: HITRUST.
[70] Tailored baselines can be developed for "unique circumstances/environments and promulgated to large communities of interest—thus achieving standardized security capabilities, consistency of implementation, and cost-effective security solutions. (Ibid., p.40)

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.[71] 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."[72] Examples are provided in Table 17.

Table 17. Examples of Predisposing Conditions

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:

[71] NIST (2012), p.8
[72] Ibid., p. 10

- **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.[73]

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"[74] 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.[75] Note, risk analysis is one of those implementation specifications.[76]

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.

Summary

The NIST CsF provides a high-level framework by which critical infrastructure industries can develop and implement industry, sector, or organizational-level risk management programs that are holistic, based upon a common set of principles, and can be communicated with stakeholders regardless of organization, sector or industry.

More specifically:

- The NIST Cybersecurity Framework categorizes cybersecurity controls according to an incident response process (functions and sub-functions) as opposed to a traditional RMF.

[73] NIST (2013), p. ix
[74] HIPAA (2006), § 164.306(b)
[75] HIPAA (2006), § 164.306(b)(i) thru (iv)
[76] HIPAA (2006), § 164.308(a)(ii)(A)

- The NIST Cybersecurity Framework incorporates 80% of the NIST SP 800-53 r4 security controls for the moderate level baseline by reference, whereas the CSF fully incorporates the NIST security controls and has recently incorporated the privacy controls from Appendix J.
- The HITRUST CSF provides an integrated, harmonized set of requirements specific to healthcare as compared to individual references to controls in NIST and other frameworks.
- The CSF Assurance Program supports the CSF with a defined assessment methodology and an integrated maturity model. The CSF Assurance Program also provides a pool of vetted assessor organizations and centralized quality assurance processes to ensure consistent and repeatable assessments.
- HITRUST provides operational-level support for organizational cyber incident management processes, which NIST does not provide.

The HITRUST RMF for the Healthcare Sector is fully consistent with the NIST CsF and either meets or exceeds the NIST CsF's requirements by addressing non-cyber threats and providing a robust assurance program and specific operational support to the industry through HITRUST's cybersecurity programs and services, training programs, and other initiatives. In fact, the HITRUST RMF is a model implementation of the NIST Cybersecurity Framework for the Healthcare Sector.

Appendix E – NIST CsF and HITRUST CSF Mapping

The following table is based on initial mappings of the controls in the 2015 CSF v7 release to the NIST CsF subcategories.

Table 18. NIST CsF to HITRUST CSF Mapping

Function	Category	Subcategory	Supporting HITRUST CSF Controls
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	07.a Inventory of Assets
		ID.AM-2: Software platforms and applications within the organization are inventoried	07.a Inventory of Assets
		ID.AM-3: Organizational communication and data flows are mapped	01.m Segregation in Networks 05.i Identification of Risks Related to Third Parties 09.m Network Controls 09.n Security of Network Services
		ID.AM-4: External information systems are catalogued	01.i Policy on the Use of Network Services 09.e Service Delivery 09.n Security of Network Services
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	07.a Inventory of Assets 07.b Ownership of Assets 07.d Classification Guidelines 12.a Including Information Security in the Business Continuity Management Process 12.c Developing and Implementing Continuity Plans Including Information Security 12.d Business Continuity Planning Framework
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	02.a Roles and Responsibilities 02.c Terms and Conditions of Employment 02.d Management Responsibilities 05.k Addressing Security in Third Party Agreements 07.b Ownership of Assets 09.n Security of Network Services 10.k Change Control Procedures 10.m Control of Technical Vulnerabilities 11.d Learning from Information Security Incidents 12.a Including Information Security in the Business Continuity Management Process 12.c Developing and Implementing Continuity Plans Including Information Security 12.d Business Continuity Planning Framework 12.e Testing, Maintaining and Re-assessing Business Continuity Plans

Function	Category	Subcategory	Supporting HITRUST CSF Controls
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	05.d Authorization Process for Information Assets and Facilities 09.g Managing Changes to Third Party Services 10.l Outsourced Software Development
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	05.a Management Commitment to Information Security 12.b Business Continuity Management
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	03.a Risk Management Program Development 05.a Management Commitment to Information Security
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	08.h Supporting Utilities 12.b Business Continuity Management 12.c Developing and Implementing Continuity Plans Including Information Security
		ID.BE-5: Resilience requirements to support delivery of critical services are established	12.a Including Information Security in the Business Continuity Management Process 12.c Developing and Implementing Continuity Plans Including Information Security 12.d Business Continuity Planning Framework
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational	**ID.GV-1:** Organizational information security policy is established	04.a Information Security Policy Document 04.b Review of the Information Security Policy
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	05.b Information Security Coordination 05.c Allocation of Information Security Responsibilities 05.k Addressing Security in Third Party Agreements

Function	Category	Subcategory	Supporting HITRUST CSF Controls
	requirements are understood and inform the management of cybersecurity risk.	**ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	01.a Access Control Policy 02.a Roles and Responsibilities 02.c Terms and Conditions of Employment 02.e Information Security Awareness, Education and Training 04.a Information Security Policy Document 04.b Review of the Information Security Policy 06.a Identification of Applicable Legislation 06.c Protection of Organizational Records 06.d Data Protection and Privacy of Covered Information 06.f Regulation of Cryptographic Controls 09.ab Audit Logging 09.n Security of Network Services 09.s Information Exchange Policies and Procedures 09.v Electronic Messaging 09.x Electronic Commerce Services 09.z Publically Available Information 10.f Policy on the Use of Cryptographic Controls 11.a Reporting Information Security Events 11.c Responsibilities and Procedures 11.e Collection of Evidence 12.e Testing, Maintaining and Re-assessing Business Continuity Plans 06.g Compliance with Security Policies and Standards
		ID.GV-4: Governance and risk management processes address cybersecurity risks	0.a Information Security Management Program 03.a Risk Management Program Development 03.d Risk Evaluation 04.a Information Security Policy Document 05.h Independent Review of Information Security
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	03.b Performing Risk Assessments 03.d Risk Evaluation 06.h Technical Compliance Checking 09.ab Audit Logging 09.r Security of System Documentation 10.m Control of Technical Vulnerabilities 12.b Business Continuity Management
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	05.g Contact with Special Interest Groups 10.m Control of Technical Vulnerabilities
		ID.RA-3: Threats, both internal and external, are identified and documented	03.b Performing Risk Assessments 03.d Risk Evaluation 10.l Outsourced Software Development 12.b Business Continuity Management
		ID.RA-4: Potential business impacts and likelihoods are identified	03.b Performing Risk Assessments 03.d Risk Evaluation 07.d Classification Guidelines 10.k Change Control Procedures 10.m Control of Technical Vulnerabilities 12.b Business Continuity Management

Function	Category	Subcategory	Supporting HITRUST CSF Controls
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	03.b Performing Risk Assessments 03.d Risk Evaluation 07.d Classification Guidelines 10.k Change Control Procedures 10.m Control of Technical Vulnerabilities 12.b Business Continuity Management
		ID.RA-6: Risk responses are identified and prioritized	03.c Risk Mitigation 06.g Compliance with Security Policies and Standards 06.h Technical Compliance Checking 10.l Outsourced Software Development 10.m Control of Technical Vulnerabilities
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	03.a Risk Management Program Development 05.h Independent Review of Information Security
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	03.a Risk Management Program Development 05.h Independent Review of Information Security
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	03.a Risk Management Program Development 05.h Independent Review of Information Security 12.b Business Continuity Management
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	01.b User Registration 01.d User Password Management 01.f Password Use 01.j Policy on the Use of Network Services 01.k Equipment Identification in Networks 01.p Secure Log-on Procedures 01.q User Identification and Authentication 01.r Password Management System 02.i Removal of Access Rights 06.f Regulation of Cryptographic Controls 09.m Network Controls 10.i Protection of System Test Data
		PR.AC-2: Physical access to assets is managed and protected	01.g Unattended User Equipment 08.a Physical Security Perimeter 08.b Physical Entry Controls 08.c Securing Offices, Rooms, and Facilities 08.e Working in Secure Areas 08.h Supporting Utilities 08.i Cabling Security 10.i Protection of System Test Data
		PR.AC-3: Remote access is managed	01.j Policy on the Use of Network Services 01.n Network Connection Control 01.y Teleworking 05.j Addressing Security When Dealing with Customers 09.s Information Exchange Policies and Procedures 10.i Protection of System Test Data

Function	Category	Subcategory	Supporting HITRUST CSF Controls
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	01.b User Registration 01.c Privilege Management 01.e Review of User Access Rights 01.m Segregation in Networks 01.s Use of System Utilities 01.v Information Access Restriction 02.i Removal of Access Rights 09.c Segregation of Duties 09.z Publically Available Information 10.i Protection of System Test Data
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	01.m Segregation in Networks 01.n Network Connection Control 01.o Network Routing Control 01.w Sensitive System Isolation 09.m Network Controls 09.w Interconnected Business Information Systems 10.i Protection of System Test Data
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	02.d Management Responsibilities 02.e Information Security Awareness, Education and Training 11.c Responsibilities and Procedures 12.c Developing and Implementing Continuity Plans Including Information Security 12.d Business Continuity Planning Framework
		PR.AT-2: Privileged users understand roles & responsibilities	02.d Management Responsibilities 02.e Information Security Awareness, Education and Training
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	02.d Management Responsibilities 05.j Addressing Security When Dealing with Customers 05.k Addressing Security in Third Party Agreements 09.e Service Delivery 09.f Monitoring and Review of Third Party Services 09.g Managing Changes to Third Party Services 09.n Security of Network Services 09.t Exchange Agreements 10.k Change Control Procedures 10.l Outsourced Software Development
		PR.AT-4: Senior executives understand roles & responsibilities	02.d Management Responsibilities 02.e Information Security Awareness, Education and Training
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	02.d Management Responsibilities 02.e Information Security Awareness, Education and Training

Function	Category	Subcategory	Supporting HITRUST CSF Controls
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	01.x Mobile Computing and Communications 01.y Teleworking 06.d Data Protection and Privacy of Covered Information 08.j Equipment Maintenance 09.x Electronic Commerce Services 09.y On-line Transactions 10.f Policy on the Use of Cryptographic Controls 10.g Key Management 10.i Protection of System Test Data 12.c Developing and Implementing Continuity Plans Including Information Security
		PR.DS-2: Data-in-transit is protected	09.m Network Controls 09.u Physical Media in Transit 09.v Electronic Messaging 09.x Electronic Commerce Services 09.y On-line Transactions 10.d Message Integrity 10.f Policy on the Use of Cryptographic Controls 10.g Key Management 10.i Protection of System Test Data
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	01.y Teleworking 07.a Inventory of Assets 07.b Ownership of Assets 08.k Security of Equipment Off-premises 08.l Secure Disposal or Re-use of Equipment 08.m Removal of Property 09.p Disposal of Media 09.q Information Handling Procedures
		PR.DS-4: Adequate capacity to ensure availability is maintained	09.h Capacity Management 12.c Developing and Implementing Continuity Plans Including Information Security

Function	Category	Subcategory	Supporting HITRUST CSF Controls
		PR.DS-5: Protections against data leaks are implemented	01.c Privilege Management 01.m Segregation in Networks 01.n Network Connection Control 01.o Network Routing Control 01.s Use of System Utilities 01.v Information Access Restriction 02.b Screening 02.c Terms and Conditions of Employment 05.e Confidentiality Agreements 07.c Acceptable Use of Assets 07.d Classification Guidelines 07.e Information Labeling and Handling 09.c Segregation of Duties 09.m Network Controls 09.p Disposal of Media 09.v Electronic Messaging 09.x Electronic Commerce Services 09.y On-line Transactions 10.b Input Data Validation 10.d Message Integrity 10.j Access Control to Program Source Code
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	09.z Publically Available Information 10.b Input Data Validation 10.c Control of Internal Processing 10.d Message Integrity
		PR.DS-7: The development and testing environment(s) are separate from the production environment	09.d Separation of Development, Test, and Operational Environments 10.h Control of Operational Software
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	01.i Policy on the Use of Network Services 01.l Remote Diagnostic and Configuration Port Protection 01.m Segregation in Networks 01.x Mobile Computing and Communications 01.y Teleworking 09.w Interconnected Business Information Systems 09.z Publically Available Information 10.h Control of Operational Software 10.k Change Control Procedures
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	10.a Security Requirements Analysis and Specification 10.k Change Control Procedures 10.l Outsourced Software Development
		PR.IP-3: Configuration change control processes are in place	09.b Change Management 10.h Control of Operational Software 10.k Change Control Procedures
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	09.l Back-up

Function	Category	Subcategory	Supporting HITRUST CSF Controls
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	08.d Protecting Against External and Environmental Threats 08.g Equipment Siting and Protection 08.h Supporting Utilities
		PR.IP-6: Data is destroyed according to policy	08.l Secure Disposal or Re-use of Equipment 09.p Disposal of Media
		PR.IP-7: Protection processes are continuously improved	0.a Information Security Management Program 03.c Risk Mitigation 05.h Independent Review of Information Security 11.a Reporting Information Security Events 12.c Developing and Implementing Continuity Plans Including Information Security 12.e Testing, Maintaining and Re-assessing Business Continuity Plans
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	05.h Independent Review of Information Security
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	11.c Responsibilities and Procedures 12.a Including Information Security in the Business Continuity Management Process 12.c Developing and Implementing Continuity Plans Including Information Security 12.e Testing, Maintaining and Re-assessing Business Continuity Plans
		PR.IP-10: Response and recovery plans are tested	12.e Testing, Maintaining and Re-assessing Business Continuity Plans
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening)	02.a Roles and Responsibilities 02.b Screening 02.c Terms and Conditions of Employment 02.d Management Responsibilities 02.f Disciplinary Process 02.g Termination or Change Responsibilities 02.h Return of Assets 02.i Removal of Access Rights 05.k Addressing Security in Third Party Agreements 06.e Prevention of Misuse of Information Assets 11.e Collection of Evidence 12.a Including Information Security in the Business Continuity Management Process
		PR.IP-12: A vulnerability management plan is developed and implemented	03.c Risk Mitigation 06.h Technical Compliance Checking 10.m Control of Technical Vulnerabilities

Function	Category	Subcategory	Supporting HITRUST CSF Controls
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	08.j Equipment Maintenance
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	08.j Equipment Maintenance
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	06.c Protection of Organizational Records 06.i Information Systems Audit Controls 09.aa Audit Logging 09.ab Monitoring System Use 09.ac Protection of Log Information 09.ad Administrator and Operator Logs 09.ae Fault Logging 09.af Clock Synchronization 09.h Capacity Management 10.i Protection of System Test Data 10.m Control of Technical Vulnerabilities
		PR.PT-2: Removable media is protected and its use restricted according to policy	01.h Clear Desk and Clear Screen Policy 07.e Information Labeling and Handling 09.o Management of Removable Media 09.q Information Handling Procedures 09.u Physical Media in Transit
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	01.i Policy on the Use of Network Services 01.l Remote Diagnostic and Configuration Port Protection 01.s Use of System Utilities 01.v Information Access Restriction 10.i Protection of System Test Data 10.j Access Control to Program Source Code 10.k Change Control Procedures 10.m Control of Technical Vulnerabilities
		PR.PT-4: Communications and control networks are protected	01.j Policy on the Use of Network Services 01.m Segregation in Networks 01.n Network Connection Control 01.o Network Routing Control 09.n Security of Network Services
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	01.m Segregation in Networks 01.n Network Connection Control 05.i Identification of Risks Related to Third Parties 09.m Network Controls 09.n Security of Network Services 09.w Interconnected Business Information Systems 11.d Learning from Information Security Incidents
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	09.ab Monitoring System Use 11.d Learning from Information Security Incidents

Function	Category	Subcategory	Supporting HITRUST CSF Controls
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	09.ab Monitoring System Use 11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents
		DE.AE-4: Impact of events is determined	11.d Learning from Information Security Incidents 12.a Including Information Security in the Business Continuity Management Process
		DE.AE-5: Incident alert thresholds are established	12.d Business Continuity Planning Framework
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	01.j Policy on the Use of Network Services 01.n Network Connection Control 09.aa Audit Logging 09.ab Monitoring System Use 09.m Network Controls 10.k Change Control Procedures
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	08.a Physical Security Perimeter 08.b Physical Entry Controls 08.c Securing Offices, Rooms, and Facilities
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	01.b User Registration 01.c Privilege Management 06.b Intellectual Property Rights 06.e Prevention of Misuse of Information Assets 08.c Securing Offices, Rooms, and Facilities 09.aa Audit Logging
		DE.CM-4: Malicious code is detected	09.ab Monitoring System Use 09.j Controls Against Malicious Code 10.l Outsourced Software Development
		DE.CM-5: Unauthorized mobile code is detected	09.k Controls Against Mobile Code
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	02.d Management Responsibilities 05.k Addressing Security in Third Party Agreements 09.e Service Delivery 09.f Monitoring and Review of Third Party Services 09.n Security of Network Services 09.z Publically Available Information 10.l Outsourced Software Development
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	06.g Compliance with Security Policies and Standards 08.a Physical Security Perimeter 08.b Physical Entry Controls 08.c Securing Offices, Rooms, and Facilities 09.aa Audit Logging 09.ab Monitoring System Use 09.n Security of Network Services 10.k Change Control Procedures
		DE.CM-8: Vulnerability scans are performed	06.h Technical Compliance Checking 10.m Control of Technical Vulnerabilities

Function	Category	Subcategory	Supporting HITRUST CSF Controls
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	02.a Roles and Responsibilities 02.d Management Responsibilities 06.g Compliance with Security Policies and Standards 06.i Information Systems Audit Controls 06.j Protection of Information Systems Audit Tools
		DE.DP-2: Detection activities comply with all applicable requirements	06.d Data Protection and Privacy of Covered Information 06.i Information Systems Audit Controls 08.a Physical Security Perimeter 08.b Physical Entry Controls 08.c Securing Offices, Rooms, and Facilities 09.ab Monitoring System Use
		DE.DP-3: Detection processes are tested	08.b Physical Entry Controls
		DE.DP-4: Event detection information is communicated to appropriate parties	05.b Information Security Coordination 05.f Contact with Authorities 06.g Compliance with Security Policies and Standards 06.i Information Systems Audit Controls 09.ab Monitoring System Use
		DE.DP-5: Detection processes are continuously improved	10.m Control of Technical Vulnerabilities
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	11.c Responsibilities and Procedures 12.c Developing and Implementing Continuity Plans Including Information Security 12.d Business Continuity Planning Framework 12.e Testing, Maintaining and Re-assessing Business Continuity Plans
		RS.CO-2: Events are reported consistent with established criteria	05.f Contact with Authorities 09.ab Monitoring System Use 11.a Reporting Information Security Events 11.c Responsibilities and Procedures
		RS.CO-3: Information is shared consistent with response plans	05.f Contact with Authorities 08.b Physical Entry Controls 09.ab Monitoring System Use 10.m Control of Technical Vulnerabilities 11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents

Function	Category	Subcategory	Supporting HITRUST CSF Controls
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	05.g Contact with Special Interest Groups 11.c Responsibilities and Procedures
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	08.b Physical Entry Controls 09.ab Monitoring System Use 11.d Learning from Information Security Incidents
		RS.AN-2: The impact of the incident is understood	11.d Learning from Information Security Incidents 11.e Collection of Evidence
		RS.AN-3: Forensics are performed	11.c Responsibilities and Procedures
		RS.AN-4: Incidents are categorized consistent with response plans	11.c Responsibilities and Procedures
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents
		RS.MI-2: Incidents are mitigated	11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	03.a Risk Management Program Development 03.c Risk Mitigation 06.h Technical Compliance Checking 10.m Control of Technical Vulnerabilities
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents
		RS.IM-2: Response strategies are updated	11.c Responsibilities and Procedures 11.d Learning from Information Security Incidents
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	11.d Learning from Information Security Incidents 12.c Developing and Implementing Continuity Plans Including Information Security
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	11.d Learning from Information Security Incidents 12.e Testing, Maintaining and Re-assessing Business Continuity Plans
		RC.IM-2: Recovery strategies are updated	11.d Learning from Information Security Incidents 12.e Testing, Maintaining and Re-assessing Business Continuity Plans
	Communications (RC.CO): Restoration	**RC.CO-1:** Public relations are managed	11.d Learning from Information Security Incidents

Function	Category	Subcategory	Supporting HITRUST CSF Controls
	activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-2:** Reputation after an event is repaired	11.d Learning from Information Security Incidents
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	11.d Learning from Information Security Incidents 12.c Developing and Implementing Continuity Plans Including Information Security

Appendix F – NIST CsF and HIPAA Security Rule Mapping

The following table provides OCR's April 2016 mapping of the NIST CsF subcategories and the HIPAA Security Rule standards and implementation specifications. The RM SG intends to work with OCR and NIST to review the mappings and provide an updated crosswalk in the next release of the Guide.

Table 19. NIST CsF and HIPAA Security Rule Mapping

Function	Category	Subcategory	HIPAA Security Rule
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	164.308(a)(1)(ii)(A) 164.310(a)(2)(ii) 164.310(d)
		ID.AM-2: Software platforms and applications within the organization are inventoried	164.308(a)(1)(ii)(A) 164.308(a)(7)(ii)(E)
		ID.AM-3: Organizational communication and data flows are mapped	164.308(a)(1)(ii)(A) 164.308(a)(3)(ii)(A) 164.308(a)(8) 164.310(d)
		ID.AM-4: External information systems are catalogued	164.308(a)(4)(ii)(A) 164.308(b) 164.314(a)(1) 164.314(a)(2)(i)(B) 164.314(a)(2)(ii) 164.316(b)(2)
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	164.308(a)(7)(ii)(E)
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	164.308(a)(2) 164.308(a)(3) 164.308(a)(4) 164.308(b)(1) 164.314
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	164.308(a)(1)(ii)(A) 164.308(a)(4)(ii) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.310(a)(2)(i) 164.314 164.316
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	164.308(a)(1)(ii)(A) 164.308(a)(4)(ii) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.310(a)(2)(i) 164.314 164.316
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.310(a)(2)(i) 164.316

Function	Category	Subcategory	HIPAA Security Rule
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	164.308(a)(7)(i) 164.308(a)(7)(ii)(E) 164.310(a)(2)(i) 164.312(a)(2)(ii) 164.314(a)(1) 164.314(b)(2)(i)
		ID.BE-5: Resilience requirements to support delivery of critical services are established	164.308(a)(1)(ii)(B) 164.308(a)(6)(ii) 164.308(a)(7) 164.308(a)(8) 164.310(a)(2)(i) 164.312(a)(2)(ii) 164.314(b)(2)(i)
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established	164.308(a)(1)(i) 164.316
		ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	164.308(a)(1)(i) 164.308(a)(2) 164.308(a)(3) 164.308(a)(4) 164.308(b) 164.314
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	164.306 164.308 164.310 164.312 164.314 164.316
		ID.GV-4: Governance and risk management processes address cybersecurity risks	164.308(a)(1) 164.308(b)
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	164.308(a)(1)(ii)(A) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.310(a)(1) 164.312(a)(1) 164.316(b)(2)(iii)
		ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	None
		ID.RA-3: Threats, both internal and external, are identified and documented	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.308(a)(5)(ii)(A) 164.310(a)(1) 164.310(a)(2)(iii) 164.312(a)(1) 164.312(c) 164.312(e) 164.314 164.316
		ID.RA-4: Potential business impacts and likelihoods are identified	164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(6) 164.308(a)(7)(ii)(E) 164.308(a)(8) 164.316(a)

Function	Category	Subcategory	HIPAA Security Rule
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(1)(ii)(D) 164.308(a)(7)(ii)(D) 164.308(a)(7)(ii)(E) 164.316(a)
		ID.RA-6: Risk responses are identified and prioritized	164.308(a)(1)(ii)(B) 164.314(a)(2)(i)(C) 164.314(b)(2)(iv)
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	164.308(a)(1)(ii)(B)
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	164.308(a)(1)(ii)(B)
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	164.308(a)(1)(ii)(B) 164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E) 164.310(a)(2)(i)
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	164.308(a)(3)(ii)(B) 164.308(a)(3)(ii)(C) 164.308(a)(4)(i) 164.308(a)(4)(ii)(B) 164.308(a)(4)(ii)(C) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iii) 164.312(d)
		PR.AC-2: Physical access to assets is managed and protected	164.308(a)(1)(ii)(B) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.310(a)(1) 164.310(a)(2)(i) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.310(d)(1) 164.310(d)(2)(iii)
		PR.AC-3: Remote access is managed	164.308(a)(4)(i) 164.308(b)(1) 164.308(b)(3) 164.310(b) 164.312(e)(1) 164.312(e)(2)(ii)
		PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii)
		PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	164.308(a)(4)(ii)(B) 164.310(a)(1) 164.310(b) 164.312(a)(1) 164.312(b) 164.312(c) 164.312(e)
	Awareness and Training (PR.AT): The	**PR.AT-1:** All users are informed and trained	164.308(a)(5)

Function	Category	Subcategory	HIPAA Security Rule
	organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-2:** Privileged users understand roles & responsibilities	164.308(a)(2) 164.308(a)(3)(i) 164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D)
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	164.308(b) 164.314(a)(1) 164.314(a)(2)(i) 164.314(a)(2)(ii)
		PR.AT-4: Senior executives understand roles & responsibilities	164.308(a)(2) 164.308(a)(3)(i) 164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D)
		PR.AT-5: Physical and information security personnel understand roles & responsibilities	164.308(a)(2) 164.308(a)(3)(i) 164.308(a)(5)(i) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D) 164.530(b)(1)
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected	164.308(a)(1)(ii)(D) 164.308(b)(1) 164.310(d) 164.312(a)(1) 164.312(a)(2)(iii) 164.312(a)(2)(iv) 164.312(b) 164.312(c) 164.312(d) 164.314(b)(2)(i)
		PR.DS-2: Data-in-transit is protected	164.308(b)(1) 164.308(b)(2) 164.312(e)(1) 164.312(e)(2)(i) 164.312(e)(2)(ii) 164.314(b)(2)(i)
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	164.308(a)(1)(ii)(A) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(a)(2)(iv) 164.310(d)(1) 164.310(d)(2)
		PR.DS-4: Adequate capacity to ensure availability is maintained	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7) 164.310(a)(2)(i) 164.310(d)(2)(iv) 164.312(a)(2)(ii)
		PR.DS-5: Protections against data leaks are implemented	164.308(a)(1)(ii)(D) 164.308(a)(3) 164.308(a)(4) 164.310(b) 164.310(c) 164.312(a) 164.312(e)

Function	Category	Subcategory	HIPAA Security Rule
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	164.308(a)(1)(ii)(D) 164.312(b) 164.312(c)(1) 164.312(c)(2) 164.312(e)(2)(i)
		PR.DS-7: The development and testing environment(s) are separate from the production environment	164.308(a)(4)
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	164.308(a)(8) 164.308(a)(7)(i) 164.308(a)(7)(ii)
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	164.308(a)(1)(i)
		PR.IP-3: Configuration change control processes are in place	164.308(a)(8)
		PR.IP-4: Backups of information are conducted, maintained, and tested periodically	164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(D) 164.310(a)(2)(i) 164.310(d)(2)(iv)
		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	164.308(a)(7)(i) 164.308(a)(7)(ii)(C) 164.310 164.316(b)(2)(iii)
		PR.IP-6: Data is destroyed according to policy	164.310(d)(2)(i) 164.310(d)(2)(ii)
		PR.IP-7: Protection processes are continuously improved	164.306(e) 164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)
		PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	164.308(a)(6)(ii)
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	164.308(a)(6) 164.308(a)(7) 164.310(a)(2)(i) 164.312(a)(2)(ii)
		PR.IP-10: Response and recovery plans are tested	164.308(a)(7)(ii)(D)
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., de-provisioning, personnel screening)	164.308(a)(1)(ii)(C) 164.308(a)(3)
		PR.IP-12: A vulnerability management plan is developed and implemented	164.308(a)(1)(i) 164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B)
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	164.308(a)(3)(ii)(A) 164.310(a)(2)(iv)

Function	Category	Subcategory	HIPAA Security Rule
	components is performed consistent with policies and procedures.	**PR.MA-2:** Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	164.308(a)(3)(ii)(A) 164.310(d)(1) 164.310(d)(2)(ii) 164.310(d)(2)(iii) 164.312(a) 164.312(a)(2)(ii) 164.312(a)(2)(iv) 164.312(b) 164.312(d) 164.312(e) 164.308(a)(1)(ii)(D)
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(C) 164.310(a)(2)(iv) 164.310(d)(2)(iii) 164.312(b)
		PR.PT-2: Removable media is protected and its use restricted according to policy	164.308(a)(3)(i) 164.308(a)(3)(ii)(A) 164.310(d)(1) 164.310(d)(2) 164.312(a)(1) 164.312(a)(2)(iv) 164.312(b)
		PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	164.308(a)(3) 164.308(a)(4) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.312(a)(1) 164.312(a)(2)(i) 164.312(a)(2)(ii) 164.312(a)(2)(iv)
		PR.PT-4: Communications and control networks are protected	164.308(a)(1)(ii)(D) 164.312(a)(1) 164.312(b) 164.312(e)
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	164.308(a)(1)(ii)(D) 164.312(b)
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	164.308(6)(i)
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.308(a)(8) 164.310(d)(2)(iii) 164.312(b) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii)
		DE.AE-4: Impact of events is determined	164.308(a)(6)(ii)
		DE.AE-5: Incident alert thresholds are established	164.308(a)(6)(i)
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(8) 164.312(b) 164.312(e)(2)(i)

Function	Category	Subcategory	HIPAA Security Rule
	intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events	164.310(a)(2)(ii) 164.310(a)(2)(iii)
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	164.308(a)(1)(ii)(D) 164.308(a)(3)(ii)(A) 164.308(a)(5)(ii)(C) 164.312(a)(2)(i) 164.312(b) 164.312(d) 164.312(e)
		DE.CM-4: Malicious code is detected	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)
		DE.CM-5: Unauthorized mobile code is detected	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B)
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	164.308(a)(1)(ii)(D)
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.310(a)(1) 164.310(a)(2)(ii) 164.310(a)(2)(iii) 164.310(b) 164.310(c) 164.310(d)(1) 164.310(d)(2)(iii) 164.312(b) 164.314(b)(2)(i)
		DE.CM-8: Vulnerability scans are performed	164.308(a)(1)(i) 164.308(a)(8)
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	164.308(a)(2) 164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(4) 164.310(a)(2)(iii) 164.312(a)(1) 164.312(a)(2)(ii)
		DE.DP-2: Detection activities comply with all applicable requirements	164.308(a)(1)(i) 164.308(a)(8)
		DE.DP-3: Detection processes are tested	164.306(e)
		DE.DP-4: Event detection information is communicated to appropriate parties	164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii)
		DE.DP-5: Detection processes are continuously improved	164.306(e) 164.308(a)(8)
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	164.308(a)(6)(ii) 164.308(a)(7)(i) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.312(a)(2)(ii)

Function	Category	Subcategory	HIPAA Security Rule
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	164.308(a)(2) 164.308(a)(7)(ii)(A) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.308(a)(6)(i) 164.312(a)(2)(ii)
		RS.CO-2: Events are reported consistent with established criteria	164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C) 164.314(a)(2)(iii)
		RS.CO-3: Information is shared consistent with response plans	164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.314(a)(2)(i)(C)
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	164.308(a)(6) 164.308(a)(7) 164.310(a)(2)(i) 164.312(a)(2)(ii)
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	164.308(a)(6)
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	164.308(a)(1)(i) 164.308(a)(1)(ii)(D) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(6)(ii) 164.312(b)
		RS.AN-2: The impact of the incident is understood	164.308(a)(6)(ii) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.308(a)(7)(ii)(E)
		RS.AN-3: Forensics are performed	164.308(a)(6)
		RS.AN-4: Incidents are categorized consistent with response plans	164.308(a)(6)(ii)
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained	164.308(a)(6)(ii)
		RS.MI-2: Incidents are mitigated	164.308(a)(6)(ii)
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(6)(ii)
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)
		RS.IM-2: Response strategies are updated	164.308(a)(7)(ii)(D) 164.308(a)(8)

Function	Category	Subcategory	HIPAA Security Rule
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after an event	164.308(a)(7) 164.310(a)(2)(i)
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	164.308(a)(7)(ii)(D) 164.308(a)(8) 164.316(b)(2)(iii)
		RC.IM-2: Recovery strategies are updated	164.308(a)(7)(ii)(D) 164.308(a)(8)
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed	164.308(a)(6)(i)
		RC.CO-2: Reputation after an event is repaired	164.308(a)(6)(i)
		RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	164.308(a)(6)(ii) 164.308(a)(7)(ii)(B) 164.308(a)(7)(ii)(C) 164.310(a)(2)(i) 164.314(a)(2)(i)(C)

Appendix G – Summary of Healthcare Implementation Activities

Table 20. Healthcare Implementation Activities by Step

Step 1: Prioritize and Scope		
Inputs	Activities	Outputs
1. Risk management strategy 2. Organizational objectives and priorities 3. Asset inventory 4. HITRUST RMF	1. Organization determines where it wants to apply the HITRUST RMF to evaluate and potentially guide the improvement of the organization's capabilities 2. Threat analysis 3. Business impact analysis 4. System categorization (based on sensitivity & criticality)	1. Usage scope 2. Unique threats
Step 2: Orient		
Inputs	Activities	Outputs
1. Usage scope 2. Risk management strategy 3. HITRUST RMF	1. Organization identifies in-scope systems and assets (e.g., people, information, technology and facilities) and the appropriate regulatory and other authoritative sources (e.g., cybersecurity and risk management standards, tools, methods and guidelines)	1. In-scope systems and assets 2. In-scope requirements (e.g., organizational, system, regulatory)

Step 3: Create a Target Profile		
Inputs	Activities	Outputs
1. Organizational objectives 2. Risk management strategy 3. Detailed usage scope 4. Unique threats 5. HITRUST RMF	1. Organization selects a HITRUST CSF control overlay and tailors the overlay based on unique threats identified in the prioritization and scoping phase 2. Organization determines level of maturity desired in the selected controls	1. Target Profile (Tailored HITRUST CSF control overlay) 2. Target Tier
Step 4: Conduct a Risk Assessment		
Inputs	Activities	Outputs
1. Detailed usage scope 2. Risk management strategy 3. Target Profile 4. HITRUST RMF	1. Perform a risk assessment for in-scope systems and organizational elements	1. Risk assessment reports
Step 5: Create a Current Profile		
Inputs	Activities	Outputs
1. Risk assessment reports 2. HITRUST RMF	1. Organization identifies its current cybersecurity and risk management state	1. Current Profile (Implementation status of selected controls) 2. Current Tier (Implementation maturity of selected controls, mapped to NIST CsF Implementation Tier model)

Step 6: Perform Gap Analysis		
Inputs	Activities	Outputs
1. Current Profile 2. Target Profile 3. Organizational objectives 4. Impact to critical infrastructure 5. Gaps and potential consequences 6. Organizational constraints 7. Risk management strategy 8. Risk assessment/analysis reports 9. HITRUST RMF	1. Analyze gaps between Current and Target Profiles in organization's context 2. Evaluate potential consequences from gaps 3. Determine which gaps need attention 4. Identify actions to address gaps 5. Perform cost-benefit analysis (CBA) or similar analysis on actions 6. Prioritize actions (CBA or similar analysis and consequences 7. Plan to implement prioritized actions	1. Prioritized gaps and potential consequences 2. Prioritized implementation plan
Step 7: Implement Action Plan		
Inputs	Activities	Outputs
1. Prioritized implementation plan 2. HITRUST RMF	1. Implement actions by priority 2. Track progress against plan 3. Monitor and evaluate progress against key risks using metrics or other suitable performance indicators	1. Project tracking data 2. New security measures implemented

Table 21. Relationship of Cyber Implementation and HHS Risk Analysis Processes

Cyber Implementation Process	Modified HHS Risk Analysis Process
1. Prioritize & Scope	• Conduct a complete inventory of where ePHI lives
	• Perform a BIA on all systems with ePHI (criticality)
	• Categorize & evaluate these systems based on sensitivity & criticality
2. Orient	• *Conduct a complete inventory of where ePHI lives*
3. Create a Target Profile	• Select an appropriate framework baseline set of controls
	• Apply an overlay based on a targeted assessment of threats unique to the organization
4. Conduct a Risk Assessment	• Evaluate residual risk
5. Create a Current Profile	
6. Perform Gap Analysis	• Rank risks and determine risk treatments
	• Make contextual adjustments to likelihood & impact, if needed, as part of the corrective action planning process
7. Implement Action Plan	• Implement corrective actions and monitor the threat environment

Appendix H – Cybersecurity Preparedness Maturity Model

While the use of a standardized control baseline to manage risks makes the process of control selection easier for an organization that doesn't have the expertise or resources to perform the threat modeling necessary to develop a custom set of reasonable and appropriate controls, it is still expected to tailor these controls to any unique threats it may reasonably anticipate. Unfortunately—in many cases due to the lack of expertise cited earlier—many, if not most, organizations take the position that the minimum baseline set of controls is simply "good enough."

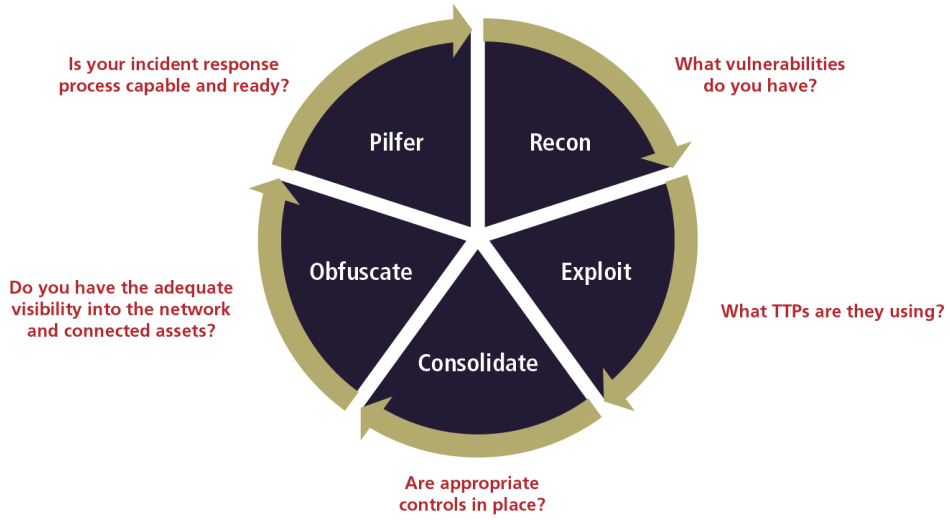
This is one of the reasons why HITRUST is actively engaged in keeping the CSF current with the assistance of the CSF Governance Committee, which is supported by CISOs from various provider, payer and professional services firms in the Healthcare Sector. The HITRUST CSF is updated at least annually based on relevant new or updated authoritative sources, such as regulations, standards, and best practices, as well as due to changes in technology or root causes of data losses and breaches. Even so, the CSF may not be as responsive to a changing threat environment as it must in order to remain current, since the frequency of updates to the underlying authoritative sources varies, ranging from almost a decade—as with ISO/IEC 27001—to years—as with NIST.

So despite all good intentions, the framework remains relatively static with respect to the cyber threat environment. Consequently, organizations relying on the next release of any control framework rather than conducting the analyses necessary to address unique, active or emerging threats—including the CSF—will always be reactive. HITRUST has decided to take the lead and address this problem of providing more timely updates to the CSF by leveraging the HITRUST ISAO's cyber threat intelligence sharing capabilities, so that organizations leveraging the CSF can better address active and emerging threats.

The HITRUST ISAO has been providing shared threat intelligence to aid participating organizations in preparing and responding to cyber threats and events for almost two years. Now, in cooperation with the Department of Health and Human Services (HHS), the ISAO is providing monthly cyber threat briefings and alerts to all qualified organizations. A qualified organization is any organization employing a function or activity involving the disclosure of individually identifiable health information, provided that said organization does not provide security products or services. Additionally, any federal, state, or local agency or department may qualify and participate in these shared intelligence briefings.

As the NIST CsF clearly indicates, organizations must address all aspects of the incident management process to effectively deal with cyber threats. HITRUST also recommends organizations think about the "kill chain" used by malicious human threat actors and ask specific questions about their capabilities in relation to each stage.

Figure 14. Malicious Threat Actor "Kill Chain"



By using this view, organizations are better able to anticipate threats and put better protections in place, regardless of their approach to control design or selection. However, not all organizations are capable of consuming and subsequently acting upon this threat intelligence in a meaningful way. Two common problems are that organizations have an incomplete understanding of their environment and its associated vulnerabilities, and they typically only use threat intelligence for basic situational awareness if they receive it at all.

As shown in Table 22. Organizational Cyber Threat Maturity, maturity can range from the very basic to a fully integrated incident management capability. In many cases, the resources and competencies are simply not available to the organization due to various organizational, fiscal, or other factors.

Table 22. Organizational Cyber Threat Maturity

	Organizational Cyber Threat Maturity			
	Basic	**Aspirational**	**Developing**	**Integrated**
Description	Rudimentary implementation of security policies. No implementation of security procedures or technologies.	Policies establish a continuing cycle of assessing risk and implementation and use monitoring for program effectiveness. Formal, up-to-date, documented procedures are provided to implement the security controls identified by the defined policies.	IT security procedures and controls are implemented in a consistent manner everywhere that the procedure(s) apply and are reinforced through training. Initial testing is performed to ensure controls are operating as intended.	Effective implementation of IT security controls is second nature. Policies, procedures, implementations, and tests are continuously reviewed and improvements are made. A comprehensive IT security program is an integral part of the culture.
Value Add	Awareness of healthcare-specific vulnerabilities and sector-wide threats.	Prioritization of healthcare-specific vulnerabilities and sector-wide threats.	Indicators of emerging threats to the healthcare sector.	Collaboration on emerging threats to the healthcare sector.

	Organizational Cyber Threat Maturity			
	Basic	**Aspirational**	**Developing**	**Integrated**
Primary Benefits	Increased understanding of threats and need for security investment.	Ability to apply resources to high priority issues; efficiency gains from prioritization.	Early warning of threats to entity based on detection and analysis of threats to like entities.	Dynamic understanding of threats to the healthcare industry and increased ability to analyze potential targeted threats (specific intent to harm).

Organizations should move from a compliance posture of evaluating controls to acting upon threat intelligence as they mature their organization's incident management capabilities. There are greater risks with the lower approaches, although just how much may be hard to say. But those engaging in threat detection, for example, can remediate vulnerabilities more rapidly than those waiting on alerts and other threat intelligence, which must evaluate and modify their relevant controls or, if using a framework, leverage control updates when they occur.

An example of how an organization can leverage threat intelligence follows.

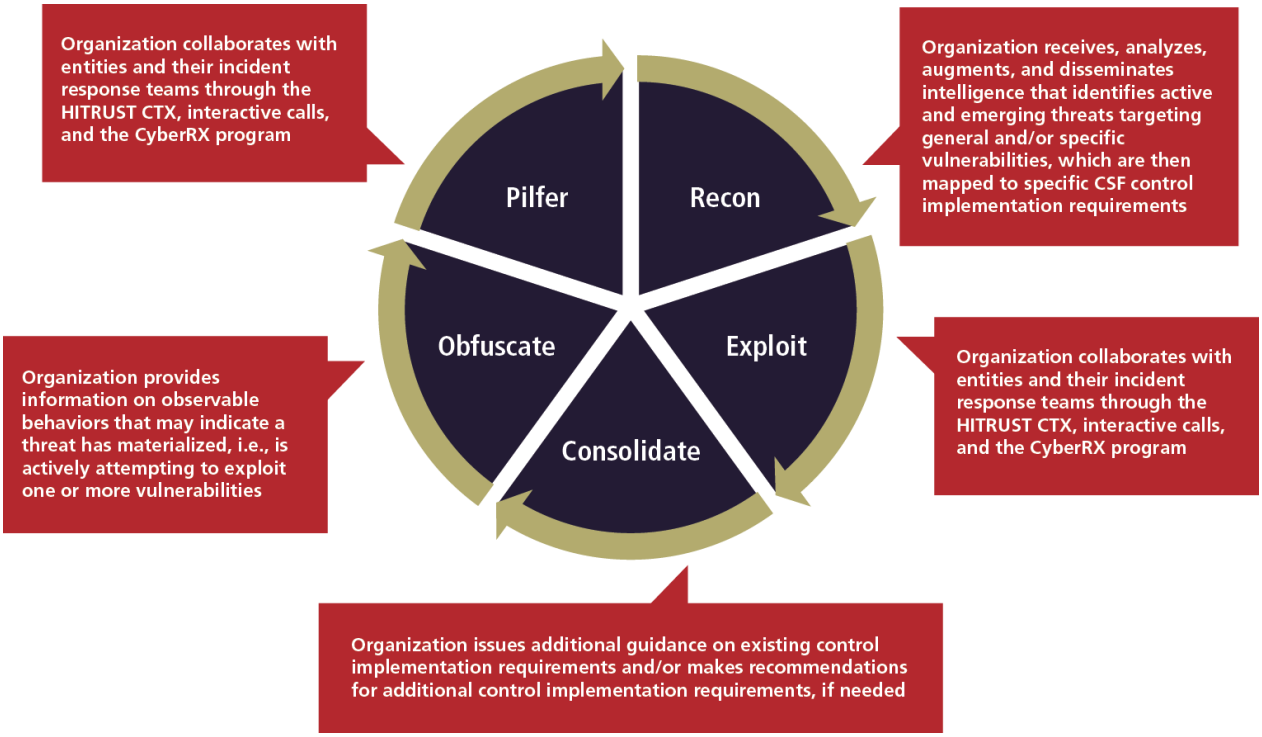
> *On March 28, 2014, at 9:14 PM EDT, an unknown actor posted over 900 email addresses and associated clear-text passwords to a popular content-sharing website. Included in the post was one healthcare entity's email address and password. The data didn't appear elsewhere on the publicly-searchable Internet, suggesting that the leaked content was original and not a repost from previously stolen information. The source of the data was unknown at this time. Although the posting of this data did not appear to pose a serious threat to the healthcare organization, there was the potential for increased exposure if the employee utilized this email password on other systems, as those accounts could also be susceptible to compromise.*

More specifically, the threat this example considers is essentially the compromise of a user password resulting in possible loss of confidentiality, integrity, and availability of information and information resources. There are many user authentication-related controls in the CSF, including some specific to password use that could be implemented to prevent such a breach. Such controls include CSF 01.b, User Registration; 01.d, Password Management; 01.f, Password Use; and 02.e, Information Security Awareness, Education and Training.

Some possible preventive or corrective measures another organization might consider reviewing based on this incident, would be to consider the use of tokens or biometrics in addition to passwords on sensitive systems, making sure that existing password expiration and reuse requirements are satisfactorily addressed, and—since the threat intelligence didn't indicate how the password was compromised—ensuring passwords are encrypted in storage and transmission for all systems and networks in the environment. Given the possible reuse of passwords across multiple systems, an organization could verify annual training addresses the safeguarding of passwords and password reuse along with timely awareness messaging to the workforce on these issues.

In the context of the kill chain presented previously, an organization should consider implementing capabilities to support the following activities:

Figure 15. Meaningful Consumption of Threat Intelligence



Given that cybersecurity preparedness involves so many different elements – as shown by the incident management approach to the NIST CsF Functions, the multitude of activities necessary to support each Function, and the activities required to meaningfully consume and respond to threat intelligence – HITRUST proposes a multi-dimensional Cybersecurity Preparedness Maturity Model for Healthcare Sector organizations to provide a more complete assessment and understanding of an organization's cybersecurity capabilities.

Table 23. Proposed Multi-dimensional Cybersecurity Preparedness Maturity Model

HITRUST Cyber-security Prepared-ness Maturity Level	Range of Min. Avg. CSF Maturity / Score – Most Relevant CSF Controls[77]	Range of Min. Avg. CSF Maturity / Score – Relevant CSF Controls	Range of Min. Avg. CSF Maturity / Score – Least Relevant CSF Controls	Acceptable HITRUST CSF Report Types (Level of Assurance)	Risk Mgmt. Maturity (Related CSF Controls)	Cyber Intelligence Consumption Capability (Related CSF Controls)	Cyber Intelligence Sharing Capability (Related CSF Controls)	Cyber Intelligence Response Tier (Related CSF Controls)	Cyber Incident Management Capability (Related CSF Controls)	Related NIST Cyber-security Implemen-tation Tier
Level 1 – Basic (Poor)	1 to 3- / 0 to 60	1 to 3- / 0 to 60	1 to 3- / 0 to 60	Self or Validated	Ad Hoc - Has not yet implemented a formal, threat-aware risk management process and may implement some portions of a cybersecurity framework on a case-by-case basis	Basic – May receive some form of threat intelligence to support basic situational awareness	None - May not have the capability to share cybersecurity information internally and might not have processes in place to participate, coordinate or collaborate with other entities	Evaluate – Assesses controls related to threat intelligence to ensure compliance	Internal - Conducts internal cybersecurity incident response exercises	**Tier 1 - Partial**
Level 2 – Aspirational (Fair)	3 to 3+ / 61 to 79	3 to 3+ / 61 to 79	1 to 3- / 0 to 60	Validated or Certified	Formal - Uses formal, threat-aware risk mgmt. process to develop control requirements	Aspirational – Receives threat intelligence to support prioritized remediation of related controls	Internal Only - Aware of role in "ecosystem" but does not have formal capability to interact / share cyber threat information externally	Evaluate – Assesses controls related to threat intelligence to ensure compliance	Local - Actively participates in cybersecurity incident response exercises with local partners and/or city/county agencies	**Tier 2 – Risk-Informed**
Level 3 – Developing (Good)	4- to 5- / 80 to 94	3 to 3+ / 61 to 79	3 to 3+ / 61 to 79	Certified	Responsive - Regularly updates controls due to changing threats on a formal basis	Developing – Obtains early warning of threats based on internal detection as well as analysis of threats to similar organizations	Partner Receive - Understands dependencies / partners and can consume information from these partners	Engage – Modifies or enhances controls in response to threat intelligence	State/Regional - Actively participates in cybersecurity incident response exercises with partners and agencies at the state or regional level (e.g., CyberRX)	**Tier 3 – Repeatable**
Level 4 – Integrated (Excellent)	5 to 5+ / 95 to 100	4 to 5- / 80 to 94	3 to 3+ / 61 to 79	Certified	Proactive - Proactively updates controls based on predictive indicators; actively adapts to changing / evolving cyber threats	Integrated – Customizes threat intelligence based on the analysis of potential targeted threats (incl. specific intent to harm)	Partner Send – Manages and actively shares information with partners to ensure accurate, current information is distributed and consumed to improve cybersecurity before it occurs	Act – Provides tailored and measured response based on customized threat intelligence	Industry - Actively participates in industry-wide cybersecurity incident response exercises (e.g., CyberRX)	**Tier 4 – Adaptive**

[77] Cline, B. (2014d). Using the HITRUST CSF to Assess Cybersecurity Preparedness. Frisco, TX; HITRUST. Retrieved from https://hitrustalliance.net/content/uploads/2014/06/HiTrustCSFCybersecurityTable.pdf.

Appendix I – Small Organization Implementation Guidance

RESERVED (To be developed [TBD] following pilot of the Small Organization Health Information Assurance Program [SOHIA] by the Texas Health Services Authority [THSA] and the Texas Medical Association [TMA].)

Appendix J – Cybersecurity Program Policy Guidance

RESERVED (TBD using a control framework-based policy architecture.)

Appendix K – Executive Marketing/Summary – Template

RESERVED (TBD; intent is to provide a set of presentation slides to summarize and sell implementation of the healthcare framework, e.g., background, purpose, key processes, controls and implementation guidance.)

Appendix L – Healthcare CsF Structure – Example

RESERVED (TBD; intent is to provide an example of the CsF structure, e.g., Function, Sub-function, Category, Objective, Control, Maturity Model, Assessment Procedures, Metrics and Authoritative Sources.)

Appendix M – Corrective Action Plan – Example

RESERVED (TBD)

Appendix N – Communications Plan – Template

RESERVED (TBD; intent is to ensure communication amongst multiple stakeholders, e.g., the board of directors, executive leadership, business units and technical staff.)

Appendix O – Medical Device Security

RESERVED (TBD; focus is on any additional guidance that may be needed to help organizations protect medical devices from cyber threats.)

Appendix P – Industry Resource Mappings

RESERVED (TBD; will provide mappings to the industry resources identified earlier in the Guide.)

Appendix Q – Cloud-based Services Implementation Guidance

RESERVED (TBD with a focus on relevant guidance for Cloud-based services, e.g., standard contract language/requirements that could be used with vendors that provide Cloud-based services and how service providers can attest to the effectiveness of specified controls.)

Appendix R – Frequently Asked Questions

RESERVED (TBD with a focus on expected challenges with framework implementation.)