The HITRUST Approach to Cyber Resilience

Leveraging HITRUST to Implement the NIST Cybersecurity Framework

Version 2.0

Version History

Version	Date	Published By	Brief Description
1.0	Jun 2014	HITRUST Standards	Originally titled *Healthcare's Model Approach to Critical Infrastructure Cybersecurity: How the Industry is Leading the Way with its Information Security Risk Management Framework*. Provided initial guidance to HITRUST Organizations and Assessors for implementing the NIST Cybersecurity Framework based on the HITRUST Approach.
2.0	Feb 2024	HITRUST Strategy, Research and Innovation Center of Excellence	Title changed to The *HITRUST Approach to NIST Cybersecurity Framework Implementation*. Updates the guidance on implementing the NIST Cybersecurity Framework to reflect changes in the HITRUST Approach, the work led by HITRUST in expanding upon v1.0 to support development of public-private sector guidance on the NIST Cybersecurity Framework's implementation, as well as relevant changes in v2.0 of the Framework. We also generalize the guidance for use by HITRUST Organizations and Assessors regardless of industry while supporting an approach for future development of industry and/or technology-specific supplements.

Preface

> *So[,] wisdom is knowing what one ought to do next. Skill is knowing how to do it, because one might know what to do, and yet be ignorant of how to put his knowledge into action. Virtue is actually doing it.*
>
> *– David Star Jordan*[1]

HITRUST wrote the initial iteration of this guidance[2] shortly after the National Institute of Standards and Technology[3] (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[4] (NIST Cybersecurity Framework) was released in February 2014. In the year that followed, Sector Specific Agencies (SSAs)[5] for chemical, commercial facilities, critical manufacturing, dams, and others developed and issued supplemental guidance on how to implement the NIST Cybersecurity Framework within specific sectors. HITRUST was subsequently asked in October of 2015 to develop similar guidance for the Healthcare and Public Health (HPH) Sector by the chairs of the Sector Coordinating Council (SCC)[6] and Government Coordinating Council (GCC)[7].

As the industry co-chair of the Joint HPH Cybersecurity Working Group (CWG) Risk Management Sub-Working Group, HITRUST led the expansion of the original 2014 guidance and published the first version of the *HPH Sector Cybersecurity Framework Implementation Guide*[8] in February of 2016. A subsequent 508-compliant[9] version 1.1 was released in May 2016. The new HPH sector guide expanded upon the initial HITRUST-issued guidance based on the HITRUST Approach.[10]

HITRUST also led development of the most recent version of the HPH sector guidance[11] published in Mar 2023 as the chair of the Risk Assessment Task Group under a restructured HPH Sector CWG.[12] Changes included updates to reflect v1.1 of the NIST Cybersecurity Framework[13] as well as additional content around enterprise risk management (ERM) and the new Online Informative Reference (OLIR) Program.[14] This version of the sector guidance was also expanded to help organizations understand how to leverage the NIST Cybersecurity Framework's Core Informative References[15] using a comprehensive controls framework such as NIST Special Publication (SP) 800-53[16] and the HITRUST CSF[17] as well as narrower approaches such as Factor Analysis for Information Risk (FAIR).[18] This was made possible by the new HPH sector guidance retaining the central concept of control framework-based risk analysis[19] and its use to establish an organization's Target Profile[20] earlier in the NIST Cybersecurity Framework implementation process.[21]

The rationale for this specific update to the original 2014 HITRUST guidance on NIST Cybersecurity Framework implementation is three-fold. First, HITRUST's view of NIST Cybersecurity Framework implementation has matured in the decade since the Framework was first released as a preliminary draft in July 2013. Second, the latest version of joint public-private sector guidance on NIST Cybersecurity Framework implementation in the HPH sector is more general and supports the use of other Informative References in addition to HITRUST programs, products, and services. And finally, many organizations that want to use HITRUST to implement the NIST Cybersecurity Framework may support other sectors besides Healthcare and Public Health.

HITRUST guidance on NIST Cybersecurity Framework implementation will subsequently have two major components going foward: a non-sector-specific guide (this document) and multiple sector-specific supplements issued as separate documents as need and demand warrant beginnng with the HPH Sector.

HITRUST believes this guidance has the potential to provide significant value for organizations that use or plan to use the HITRUST Approach as the basis for their information risk management programs, not only due to the power of the approach but also its ability to help organizations communicate the state of their programs to regulatory agencies and other stakeholders that use the NIST Cybersecurity Framework,[22] including those in the HPH sector that seek allowable mitigations under recent Health Insurance Portability and Accountability Act (HIPAA) 'Safe Harbor' legislation.[23]While the NIST Cybersecurity Framework is currently viewed as voluntary guidance, this stance may very well change at some point in the future. The most recent National Cybersecurity Strategy released by The White House in Mar 2023 indicates a potential shift from voluntary guidance to a mix of voluntary and mandatory standards over time[24] [25]

Table of Contents

Table of Figures

Table of Tables

Introduction

> *The Internet continues to connect individuals, businesses, communities, and countries on shared platforms that enable scaled business solutions and international exchange. But this accelerating global interconnectivity also introduces risks. An attack on one organization, sector, or state can rapidly spill over to other sectors and regions, as happened during Russia's 2017 "NotPetya" cyberattack on Ukraine, which spread across Europe, Asia, and the Americas, causing billions of dollars in damage. The potential cost of attacks like this will only grow as interdependencies increase.*
>
> *– National Cybersecurity Strategy*[26]

It comes as no real surprise that the threat of cybers attacks on public and private sector organizations continues to increase in both prevalence and sophistication.[27] A trend that has been ongoing for decades, it is no longer a question of 'if' an organization will be attacked and suffer a breach but one of 'when' and 'how bad.' While this seems rather dire on its face, knowing one will be attacked and potentially suffer a breach can also be empowering in that such certainty can help facilitate an organization's change or shift in the old paradigm[28] of preventative cybersecurity to a new one of cyber resilience.[29]

The U.S. government's recent foray into the push for cyber resilience in the private sector nominally began with Presidential Policy Directive 21 – Critical Infrastructure Security and Resilience,[30] Executive Order (EO) 13636 – Improving Critical Infrastructure Cybersecurity,[31] and the Cybersecurity Enhancement Act of 2014[32] that formalized publication of the voluntary cybersecurity guidance required under the EO,[33] which is now widely known as the NIST Cybersecurity Framework.

However, "while voluntary approaches to critical infrastructure cybersecurity have produced meaningful improvements, [the U.S. government is of the opinion that] the lack of mandatory requirements has resulted in inadequate and inconsistent [cybersecurity] outcomes."[34]

To address these issues, government intends to:

(1) Use existing statutory authorities to issue new or updated cybersecurity regulations,
(2) Identify and close gaps in existing statutory authorities to regulate the private sector, and
(3) Encourage state or independent regulators to use their authorities in "a deliberate and coordinated manner"[35] to support these efforts.

Among the various strategic objectives promulgated in the National Cybersecurity Strategy to promote cyber resilience,[36] HITRUST also notes the government intends to shift liability for insecure software products and services to developers and providers as well as hold those responsible for implementing data usage and security policies accountable for cybersecurity failures.[37]

The ramifications for industry from the government's new strategic approach to cybersecurity are potentially quite significant.

Without regard to the government's continued focus on regulation and liability as a primary catalyst for improvements in cybersecurity, the government fortunately recognizes that none of the five pillars of its cybersecurity strategy can be achieved without "unprecedented levels of collaboration across its respective stakeholder communities, including the public sector, private industry, [and] civil society…."[38] Together, industry and government must drive effective and equitable collaboration to correct market failures, minimize the harms from cyber incidents to society's most vulnerable, and defend our shared digital ecosystem."[39] To that end, the government intends to work with industry to harmonize existing cybersecurity regulations as well as promote performance-based regulations that "leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance—including … the [NIST Cybersecurity Framework[i]]."[40]

[i] Unless specified otherwise, we generally use 'Framework' to mean the NIST Cybersecurity Framework in this guidance document.

Cyber Resilience

Resilience is all about being able to overcome the unexpected. Sustainability is about survival. The goal of resilience is to thrive.

– James Cascio[41]

Most of us understand that cybersecurity is focused on protecting information assets from cyber-related threats, but what does it mean to be cyber resilient?

In physics, resilience refers to elasticity or the ability of a material to return to its original shape after it is deformed by bending, stretching, or compression.[42] In more general terms; however, it refers to one's ability to withstand or recover quickly from some type of adversity.[43]

While incorporating the concept of elasticity, it is this more general view of resilience that informs our definition of cyber resilience, which is the "ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment."[44]

Achieving Resiliency

So how does an organization become resilient? Or, more specifically, how does this concept of cyber resilience relate to an organization's cybersecurity program?

Anticipate

How well one can anticipate "adverse conditions, stresses, attacks, or compromises on systems"[45] comes directly from how well and how often an organization performs a risk analysis, which specifically assesses this issue and helps organizations determine how they should address associated risk. Although there are many different approaches, a typical risk analysis consists of seven specific activities—generally categorized as decision support and variance reduction controls (e.g., inventory management and risk management)—as shown in the following figure.

Figure 1. General Risk Analysis Process

Although shown as a process, the activities are not necessarily sequential. However, all activities are important; the failure to conduct any one of them—or any of them well—will impact the organization's ability to anticipate adverse events and subsequently specify the requisite cybersecurity controls needed to address these events.

Withstand

Withstanding adversity is an essential component of elasticity and is directly related to an organization's ability to protect itself and continue essential operations until adversity is overcome. In terms of an organization's cybersecurity program, this ability is provided by its preventive controls (e.g., access control and network security), detective (e.g., audit logs), and responsive controls (e.g., incident response).[46] [ii]

[ii] These various types of controls are addressed in more detail in the next section.

Recover

The other component of elasticity is the ability to return to a state of normalcy after the organization is impacted by an adverse event, which in the world of cybersecurity is provided by its recovery controls (e.g., disaster recovery).[47]

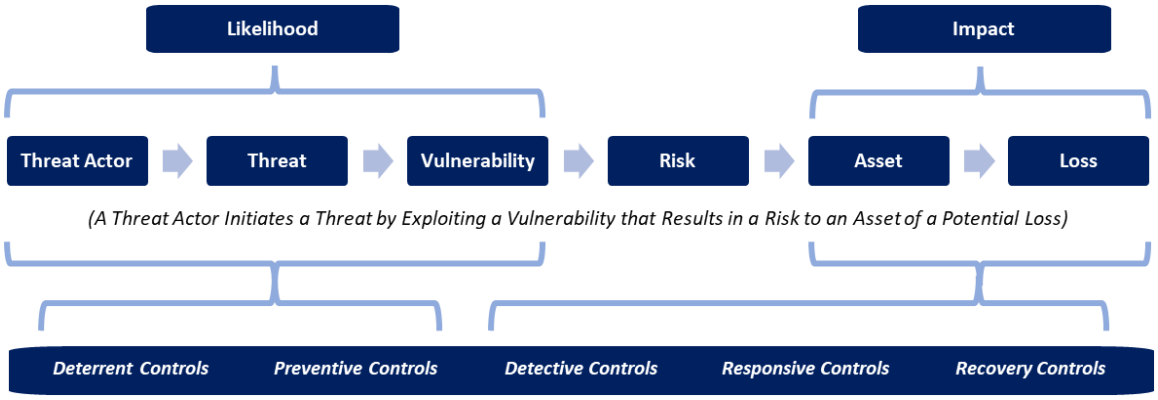
Adapt

Elasticity around anticipated adverse events is—in and of itself—a necessary but insufficient condition for true cyber resilience. To achieve this, organizations must be able to continue normal operations when systemic changes in the threat environment occur, i.e., when operating under a 'new normal.' This capability is generally provided by an organization's decision making and variance reduction controls (e.g., risk management, of which risk analysis is a part, continuous monitoring, and change management).[48]

Resilience Through Risk Management

Resilience can only be achieved through the proper application of controls that mitigate risk in different ways. To illustrate this, the figure[49] below breaks out risk into its two major components (likelihood and impact), maps elements of a threat statement to the relative risk component, and then identifies the types of controls that interact with those elements based on how they function against (or interact with) a threat.

Figure 2. Basic Risk Management Ontology



Deterrent controls discourage a threat actor from initiating a cybersecurity (threat) event. The concept of deterrent controls is somewhat similar to another approach that focuses on an organization's workforce, whether as a positive force to enhance security or as a potential threat actor.[50] While deterrent controls can also be considered a preventive control, HITRUST identifies these controls separately given how they generally interact with threat actor motivation as opposed to capability.[51] Examples include but are not limited to disciplinary processes and security patrols.

Preventive controls act to stop a cybersecurity event from occurring.[52] Some may reduce the frequency with which a threat actor comes into contact with an asset, make a threat agent's job more difficult in a malicious or act-of-nature scenario, or make the threat agent's job easier in a human error scenario.[53] Examples include but are not limited to firewalls and both logical and physical user access controls.

Detective controls act to identify when a cybersecurity event occurs.[54] Examples include but are not limited to intrusion detection, file monitoring, and video surveillance systems.

Responsive controls are corrective in nature as they act to limit the potential impact of a detected cybersecurity event once it has occurred[55] and typically focus on addressing errors or irregularities in information systems due to the event.[56] Examples include but are not limited to system patching and business continuity and incident response plans.

Recovery controls are also corrective in nature and generally support restoration of information systems back to pre-cybersecurity event conditions.[57] Examples include but are not limited to equipment repair/replacement and disaster recovery plans.

While not identified in the preceding figure as they do not interact directly with elements of the threat statement, there are two other types of controls that help organizations *manage* risk. This is because management may be viewed as a problem-solving process,[58] which includes the problem-solving activities that make up related business process and the business processes themselves.[59] Problem-solving is essentially a *decision-making* process, and in business a 'good' process is one that is well-controlled—i.e., measured, managed, and continuously improved—to *reduce variation* in the process output.

HITRUST therefore defines two types of management-related cybersecurity controls: decision support and variance reduction.

Decision Support controls help improve the quality of risk-related decision-making. Examples include but are not limited to controls associated with an organization's asset and risk management programs.

Variance Reduction controls help reduce variability in the performance (effectiveness) of other controls. Examples include but are not limited to organizational governance and security education, training, and awareness programs.

The place of these management-related controls in the risk ontology will become clear later in the next section, which shows how an organization can achieve a state of cyber resilience when its information risk management program is founded upon the HITRUST Approach and implemented through the lens of the NIST Cybersecurity Framework.

NIST Cybersecurity Framework

> *Although the Cybersecurity Framework was developed initially with a focus on our critical infrastructure, such as transportation and the electric power grid, today it is having a much broader, positive impact in this country and around the world.*
>
> *– Walter G. Copan, Under Secretary of Commerce and NIST Director*[60]

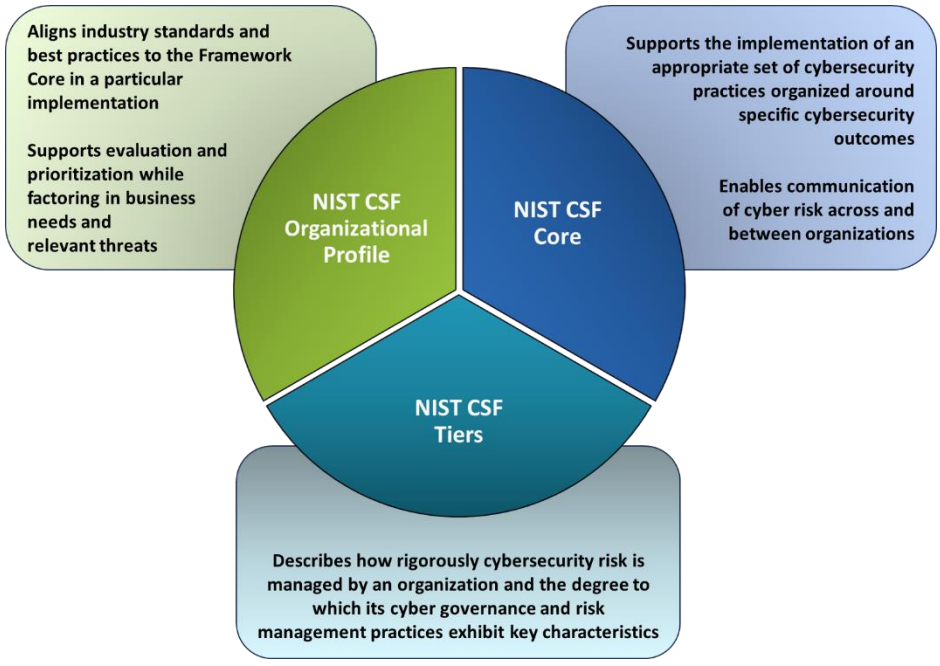
The NIST Cybersecurity Framework was originally published as voluntary guidance for critical infrastructure sector organizations, both public and private. Its principal goal is to provide "a common taxonomy and mechanism for organizations to:

- "Describe their current cybersecurity posture,
- "Describe their target state for cybersecurity,
- "Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process,
- "Assess progress towards the target state, and
- "Communicate among internal and external stakeholders about cybersecurity risk."[61]

Components

The NIST Cybersecurity Framework consists of three major components, as shown in the figure below.

Figure 3. NIST Cybersecurity Framework Components[62]



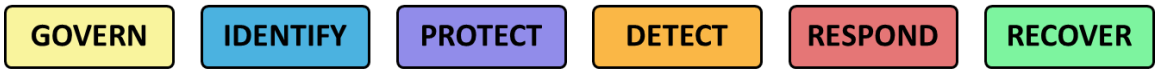
Framework Core

The cornerstone of the NIST Cybersecurity Framework is the Framework Core, which is composed of four elements: Functions, Categories, Subcategories, and Informative References. The Framework Core provides the overarching structure for the assignment of cybersecurity activities that support specific cybersecurity outcomes (objectives).[63]

Functions

Performed concurrently and continually, the six Functions of the Framework Core organize the basic, high-level cybersecurity activities needed to help organizations manage cybersecurity risk consistent with existing methodologies for cybersecurity incident management.[64]

Figure 4. NIST Cybersecurity Framework Core Functions



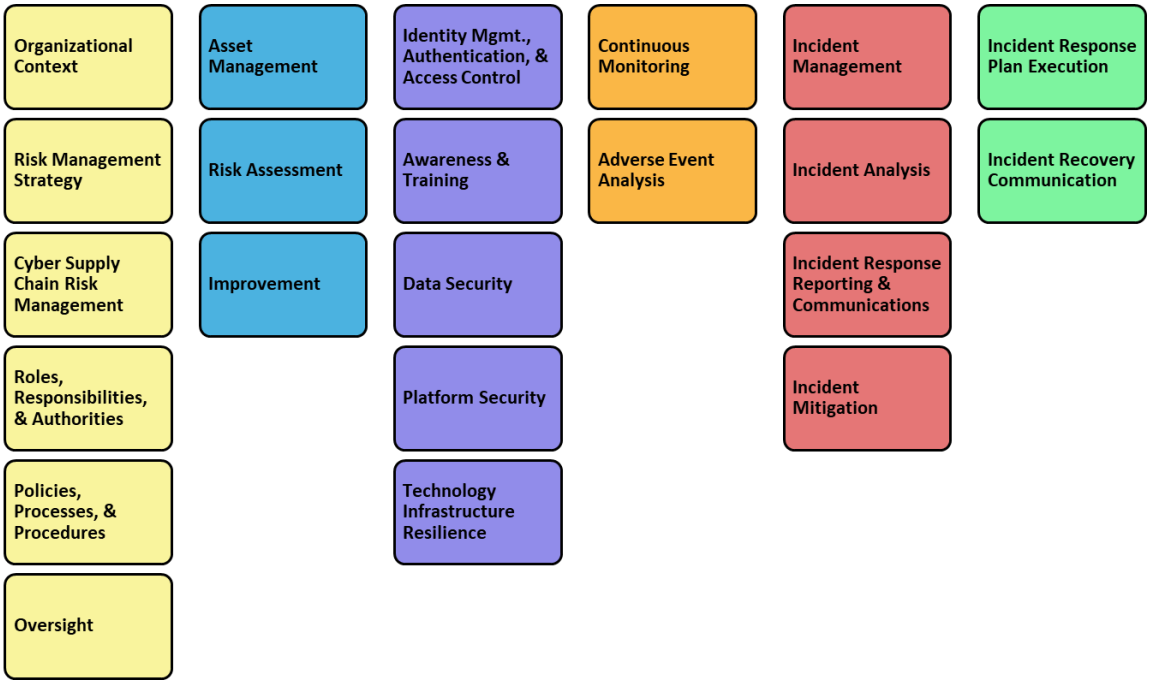
- The activities in the **Govern Function** are foundational for the effective use of the Framework by helping an organization establish and monitor its cybersecurity risk management strategies, policies, and overall expectations.[65]
- The activities in the **Identify Function** help organizations focus and prioritize cybersecurity activities in a manner consistent with its risk management strategy and mission needs.[66]
- The **Protect Function** supports an organization's ability to prevent or limit the likelihood or impact of a potential cybersecurity event by developing and implementing appropriate cybersecurity safeguards to ensure delivery of critical products and services.
- The **Detect Function** enables timely discovery of cybersecurity events through the development and implementation of appropriate activities such as monitoring and alerting to identify the occurrence of a cybersecurity event.
- The **Respond Function** supports an organization's ability to contain a potential cybersecurity incident and mitigate its impact after the event has been identified.[67]
- The **Recover Function** supports timely recovery of information systems to normal operations to further reduce the impact of a cybersecurity incident through the maintenance of recovery plans and the restoration of system capabilities or services impaired due to the incident.

The NIST Cybersecurity Framework Core Functions are inherently designed to ensure organizations establish a cybersecurity program that addresses all the required elements of cyber resilience, i.e., the ability to anticipate, withstand, recover from, and adapt to adverse cyber events.

Categories

Core Categories subdivide Functions into groups of cybersecurity outcomes that are generally topical in nature and closely tied to specific cybersecurity needs and activities (e.g., access control).

Figure 5. NIST Cybersecurity Framework Core Categories



This is similar to how other control frameworks like the HITRUST CSF are organized.[68]

Subcategories

Core Subcategories further subdivide Categories into specific cybersecurity outcomes (objectives) similar to Control Objectives and Control Specifications in the HITRUST CSF.

Figure 6. NIST Cybersecurity Framework Core Subcategories (Example)

Function	Category	Cat. ID
Govern	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Subcategory
GV.RM-01: Risk management objectives are established and agreed to by organizational stakeholders (formerly ID.RM-01)
GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained (formerly ID.RM-02, ID.RM-03)
GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes (formerly ID.GV-04)
GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated
GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties
GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated
GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions

It is through the use of Categories and Subcategories—organized like an incident response process—that the NIST Cybersecurity Framework helps ensure organizations use multiple types of controls to comprehensively address the risk from a wide range of threats across their respective kill chains.

Informative References

The NIST Framework Core Informative References are external standards, frameworks, guidelines, and best practices like the HITRUST CSF that support the cybersecurity outcomes specified by each Core Subcategory.[69]

Implementation Examples

NIST also added Implementation Examples in its most recent release of the Cybersecurity Framework, which—like Informative References—offer "concise, action-oriented steps"[70] or activities that can also help organizations achieve its cybersecurity outcomes.

Framework Profiles

NIST Cybersecurity Framework Organizational Profiles "are used to understand, tailor, assess, prioritize, and communicate the Core's outcomes by considering an organization's mission objectives, stakeholder expectations, threat landscape, and requirements."[71] 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).

Framework Tiers

The NIST Cybersecurity Framework Tiers are intended to provide context around how organizations view and manage cybersecurity risk by how their cybersecurity practices exhibit specific characteristics.[72] A notional illustration of how one might "characterize the rigor of an organization's cybersecurity risk governance practices [as described by the Governance Function] and … risk management practices [as described the remaining Core Functions]"[73] follows:

(1) Tier 1 – Partial
   - Cybersecurity Risk Governance: Application of organizational risk management strategy is managed in an ad hoc fashion.
   - Cybersecurity Risk Management: Limited awareness of cybersecurity risk at the organizational level.

(2) Tier 2 – Risk Informed
   - Cybersecurity Risk Governance: Management practices are approved by management but may not be established as organization-wide policy.
   - Cybersecurity Risk Management: While aware, there is no organization-wide approach to managing cybersecurity risk.

(3) Tier 3 – Repeatable
   - Cybersecurity Risk Governance: Practices are supported by policy and updated regularly based on changes in the threat environment.
   - Cybersecurity Risk Management: There is an organization-wide approach to risk management.

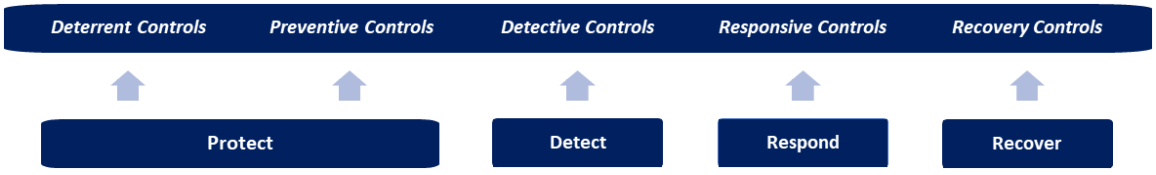
(4) Tier 4 – Adaptive
   - Cybersecurity Risk Governance: There is an organization-wide approach to managing cyber risk as part of a broader enterprise risk management program based on current and predicted risk consistent with organizational risk tolerances.
   - Cybersecurity Risk Management: Cybersecurity practices are continuously improved and adapted to a changing technological landscape and evolving threats.[74]

Although having all the earmarks of a maturity model,[iii] NIST has expressly stated Organizational Tiers are not meant to represent a specific level of maturity[75] but rather the rigor of an organization's cybersecurity risk governance and management outcomes.[76] However, NIST still encourages Tier 1 organizations to move to Tier 2 or greater. They also recommend organizations move to higher Tiers "when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk".[77]

Supporting Resilience

The NIST Cybersecurity Framework structure—and most especially the Framework Core--is inherently designed to support the implementation of comprehensive cybersecurity programs that can provide organizations with a high degree of resilience. It therefore comes as no surprise that the NIST Cybersecurity Framework Core Protect, Detect, Respond and Recover Functions have prima facie relationship with many of the types of controls we identified previously based on how they interact with (function against) a threat.

Figure 7. Relationship of NIST Core Functions to Control Types



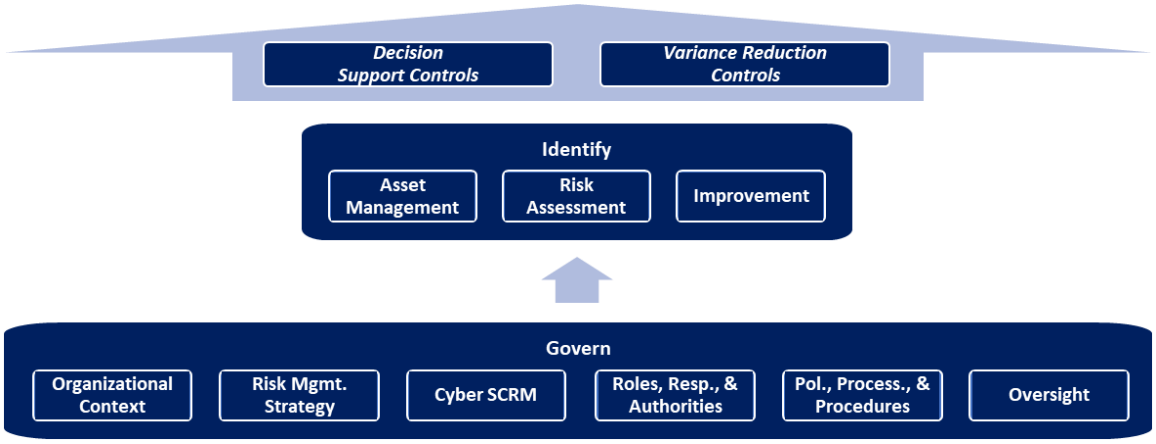
However, the Govern and Identify Functions' relationship to control types is not as clear as the other Core Functions.

[iii] A maturity model provides the basis for comparing the maturity of practices in a specified discipline and is generally used to improve and appraise a group's capability to perform that discipline.

NIST describes the Govern Function as 'cross-cutting' in that its outcomes are meant to "inform what an organization may do to achieve and prioritize the outcomes of the other … Functions,"[78] including the Identify Function. Similarly, the Identify Function prescribes outcomes that impact the Protect, Detect, Respond, and Recover Functions to help an organization "prioritize its efforts consistent with its risk management strategy and the mission needs identified [in the Govern Function and] … inform efforts under all six Functions."[79]

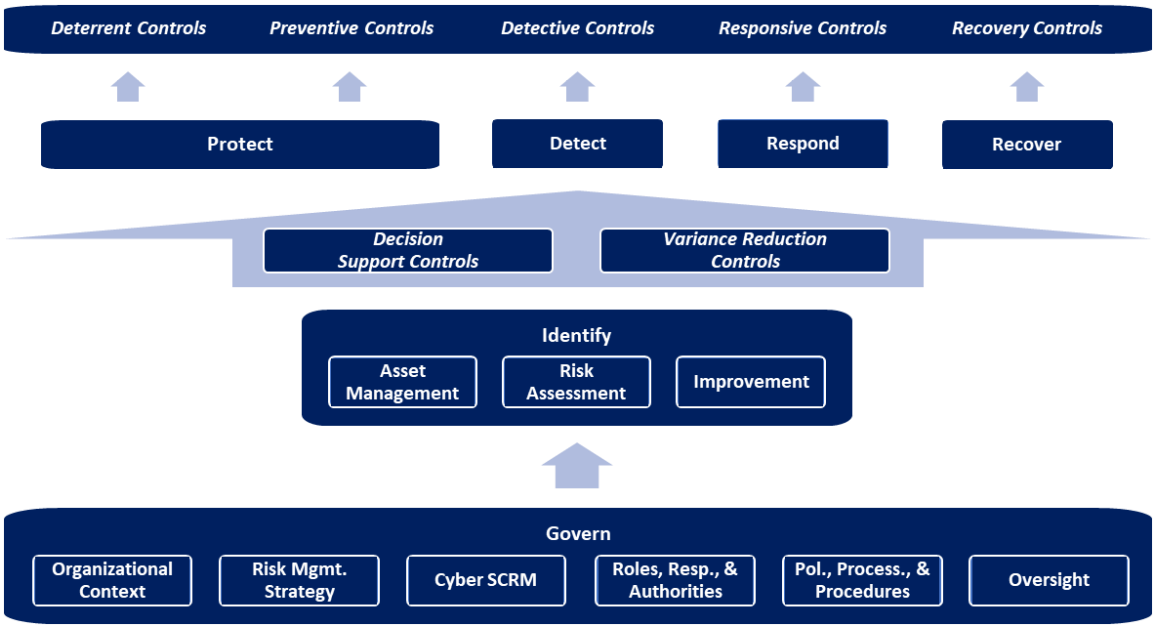
HITRUST subsequently posit the relationship of the Govern and Identify Functions to specific control types[80] [81] as shown in below.

Figure 8. The Govern and Identify Functions' Core Categories



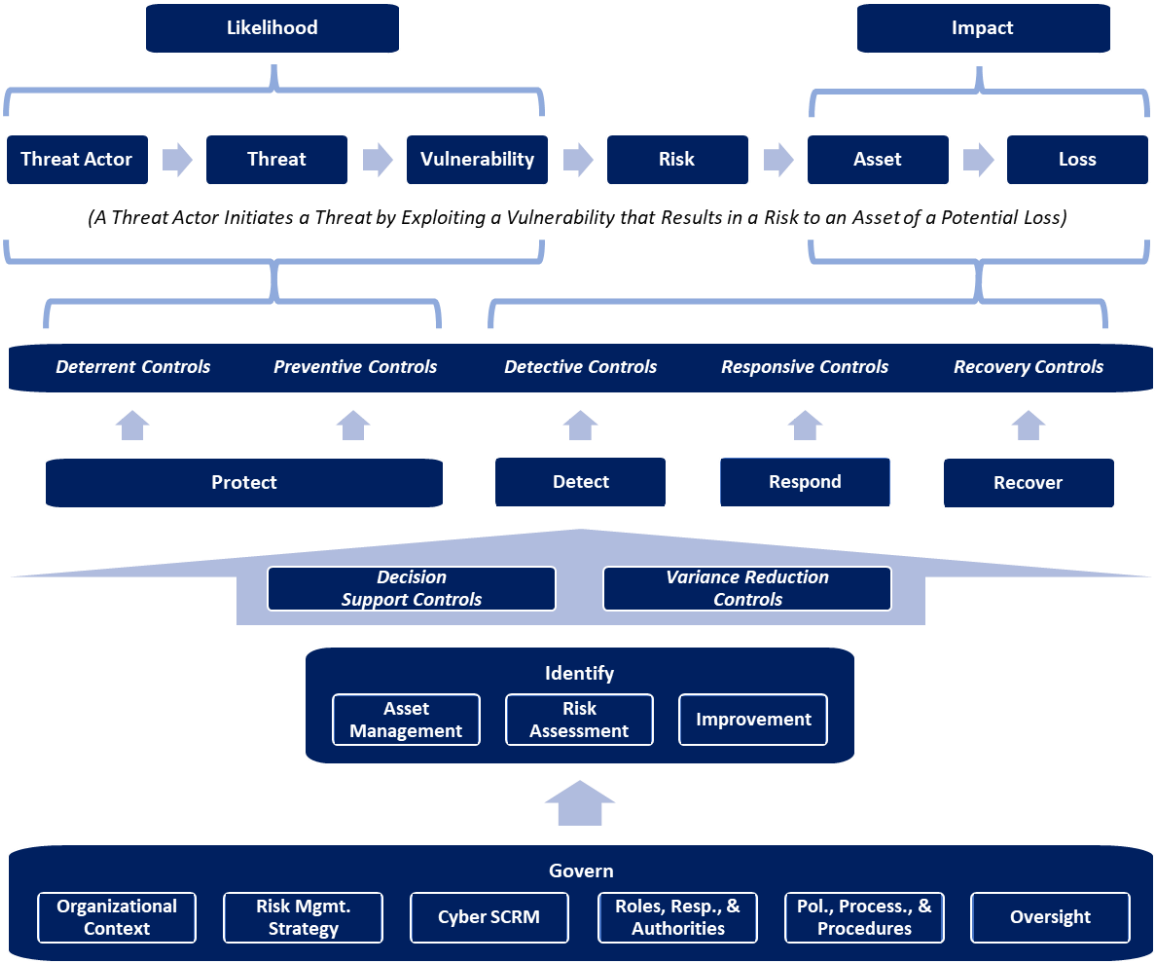
The decision support and variance reduction controls in the Core Categories of the Govern and Identify Functions subsequently help influence and support the deterrent, preventive, detective, responsive, and recovery controls in the Protect, Detect, Respond, and Recover Functions.

Figure 9. Relationship between NIST Core Functions and Controls



The final step is integration of the NIST Cybersecurity Framework Core into the basic risk management ontology presented earlier to provide a more comprehensive picture of how cybersecurity controls help organizations manage cyber risk.

Figure 10. Comprehensive Risk Management Ontology



Limitations

The NIST Cybersecurity Framework is meant to have maximum flexibility, so that it may be applied to any organization regardless of size, industry or other relevant demographic. It achieves this by limiting itself to specifying cybersecurity outcomes—the 'what'—in its Core Subcategories and leaving specification of supporting controls from its Informative References—the 'how'—to the organization. And even these cybersecurity outcomes can be selected based on an organization's specific business needs and capabilities.

This flexibility, however, necessarily limits an organization's ability to implement the NIST Cybersecurity Framework without relying on other standards and best practice frameworks contained in the OLIR. But, while the number and type of Informative References in the OLIR continue to grow over time, they only provide a library of potential controls from which an organization can select.

To complicate matters further, although NIST states the Cybersecurity Framework is risk-based, a risk-based approach to selecting controls from one or more Informative References is not specified. NIST CSF Tiers could potentially help, but they do not currently provide a meaningful approach to supporting control selection. NIST only states they may prove useful when a cost-benefit analysis indicates a positive return on investment for a control's implementation relative to an estimated reduction in risk.

The NIST Cybersecurity Framework only 'works' if an organization is able to provide what it is missing.

Notional NIST Cybersecurity Framework Structure

HITRUST offers the following figure to show what the NIST Cybersecurity Framework provides. Then—as this discussion continues—the missing pieces can be 'filled in' by leveraging the HITRUST Approach.

Figure 11. NIST Cybersecurity Framework Structure

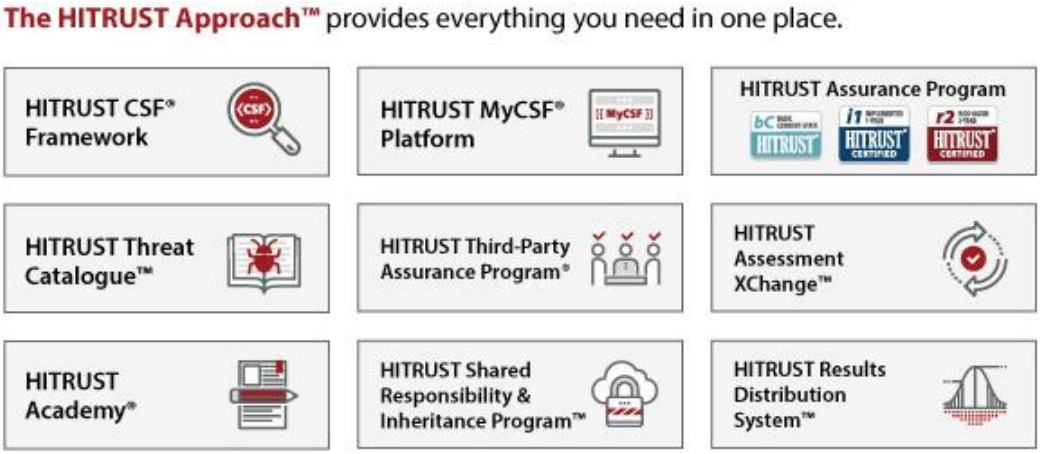
The HITRUST Approach

Taking some liberties from William Law's famous quote, "if we ask ourselves why …these breaches occur… your own heart will tell you that it is neither through ignorance nor inability, but purely because you never thoroughly intended it." … Intentionality requires a measurable goal and a steadfast commitment to improvement. It means placing security as a variable early in the planning phase and aggressively adhering to the risk thresholds and security posture put in place.[82]

The HITRUST Approach can be thought of as the HITRUST programs, products, and services and their underlying methodologies that help organizations manage information risk, including compliance with related laws, regulations, standards, and other business requirements through every step of the risk management process: (1) identify risks and define protection requirements, (2) specify cybersecurity controls, (3) implement and manage cybersecurity controls, and (4) assess cybersecurity controls and report.[83]

Figure 12. Support for Every Step of the Risk Management Process

Figure 13. The HITRUST Approach's Products and Services



HITRUST CSF

The first step of risk management is centered around the 7-step risk analysis process presented earlier and shown again here for convenience.

Figure 14. Risk Analysis Process

Unfortunately, this process can be problematic for many organizations to perform.[84] In particular, threat, vulnerability, and impact analysis can prove difficult for many organizations due to a lack of personnel with the requisite expertise or relevant information. In fact, even the U.S. government does not take this 'textbook' approach to risk analysis in its own risk management framework.[85]

Instead, federal agencies categorize their information systems based on one of "three levels of potential impact on organizations or individuals should there be breach of security (i.e., a loss of confidentiality, integrity, or availability)"[86] and then select an appropriate control baseline,[87] which is a select set of cybersecurity and privacy controls intended to address the protection needs of low, medium, or high-impact information systems for the purpose of managing associated information risk.

Figure 15. Control Framework-Based Risk Analysis

Once the baseline is selected after completing the initial risk analysis, agencies must then customize the baseline to fit their specific needs, which includes but is not limited to any unique business requirements or threats to information. NIST refers to this type of customization as *tailoring*, which includes the following activities:

(1) Scale controls by selecting an appropriate baseline from which to begin.
(2) Scope the scaled baseline by adding or enhancing controls, as needed.
(3) Specify compensating controls for baseline controls that cannot be implemented.
(4) Continue the tailoring process by reviewing and potentially revising organization-defined parameters.
(5) Review the resulting overlay[iv] periodically or otherwise as needed.[88]

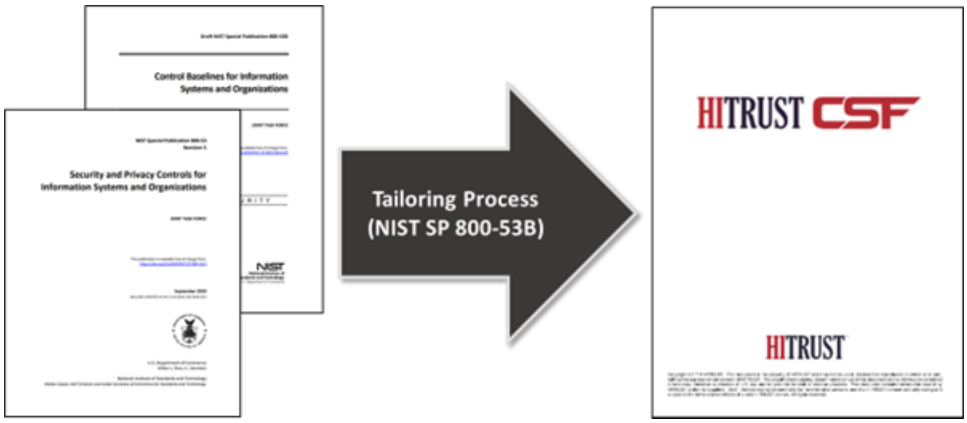
The U.S. government has used this approach to control framework-based risk analysis to create multiple overlays of the NIST SP 800-53 control baselines for use by various government agencies. For example, the Centers for Medicare and Medicaid Services (CMS) produces an overlay of all three NIST control baselines for their use and that of their contractors [4].[89] CMS also produces a separate overlay of a NIST control baseline for Health Insurance Exchanges [3].[90] The Internal Revenue Service (IRS) publishes an overlay of a

[iv] An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.

NIST baseline for federal, state, and local organizations that handle Federal Tax Information (FTI),[91] and the Federal Risk and Authorization Management Program (FedRAMP) offers overlays of all three NIST control baselines for use by Cloud Service Providers (CSPs) that support the Federal government.[92]

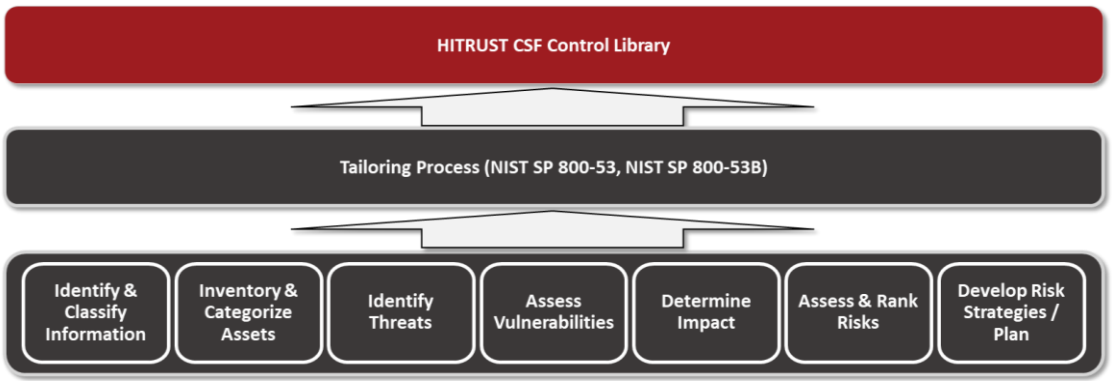
HITRUST took the same approach when developing its industry-level, enhanced overlay[v] of the NIST SP 800-53 moderate impact control baseline—the HITRUST CSF.

Figure 16. HITRUST Overlay of NIST SP 800-53



As HITRUST builds out the NIST Cybersecurity Framework Structure in the next section, the preceding two figures are consolidated to show the entire control framework-based risk analysis and tailoring process used to specify the HITRUST CSF controls in the enhanced overlay.

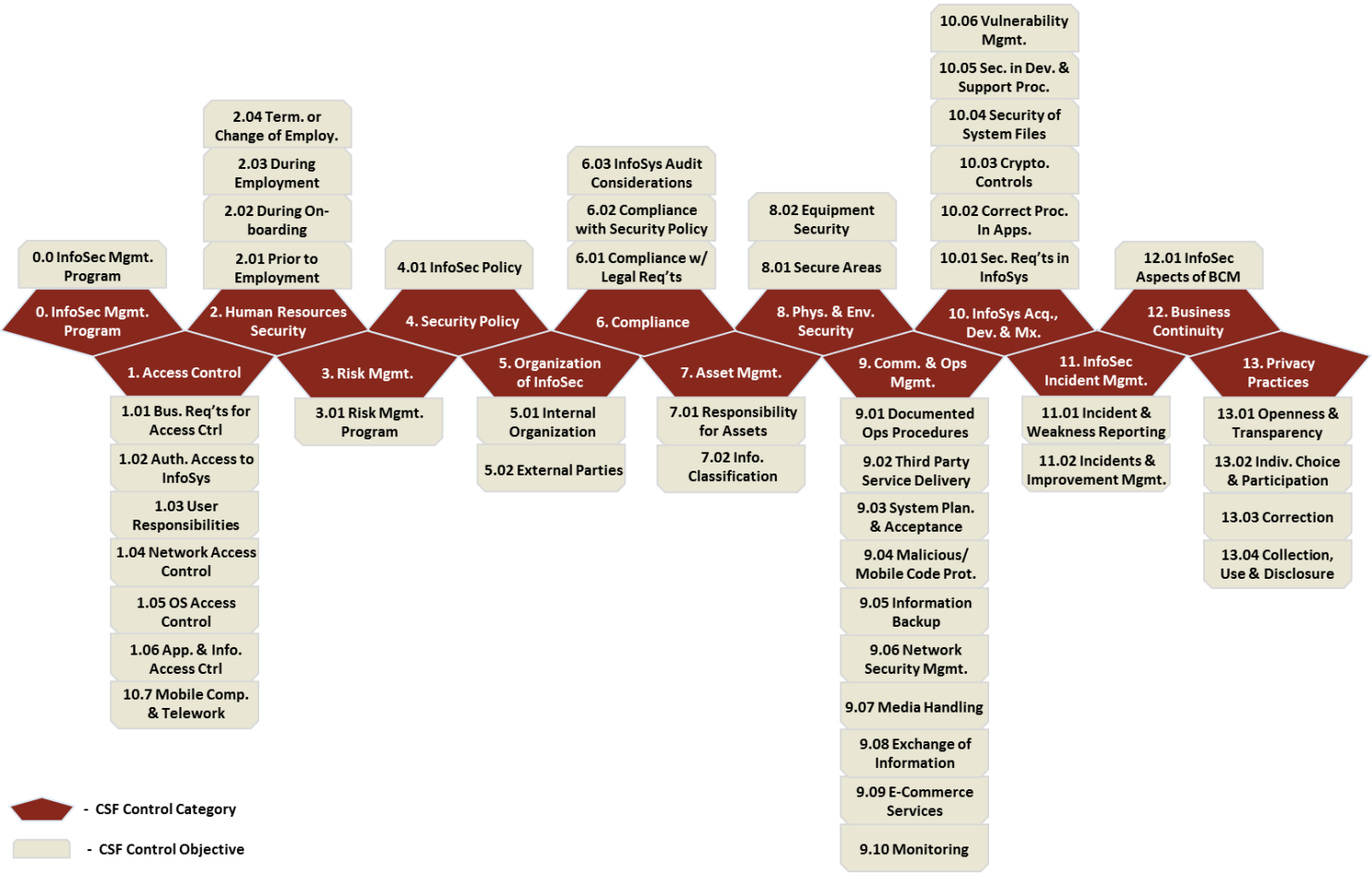
Figure 17. Building the HITRUST CSF Enhanced Overlay



Structurally, the HITRUST CSF is similar to ISO 27001 as it consists of control categories, control objectives, and controls. However, the HITRUST CSF controls are much more granular than those found in ISO 27001 or even NIST SP 800-53. A HITRUST CSF control consists of a Control Reference, which includes a number and a name; a Control Specification, which provides the intended cybersecurity outcome; and multiple control requirements, which are intended to achieve the desired outcome and are selected based on inherent risk factors relevant to a specific organization. Inherent risk factors are categorized as organizational factors (e.g., amount of sensitive information processed), technical factors (e.g., number of system interfaces), and compliance factors (e.g., subject to HIPAA).[93]

[v] An enhanced overlay adds processes, controls, enhancements, and additional implementation guidance specific to the purpose of the overlay.

Figure 18. HISTRUST CSF Framework Structure

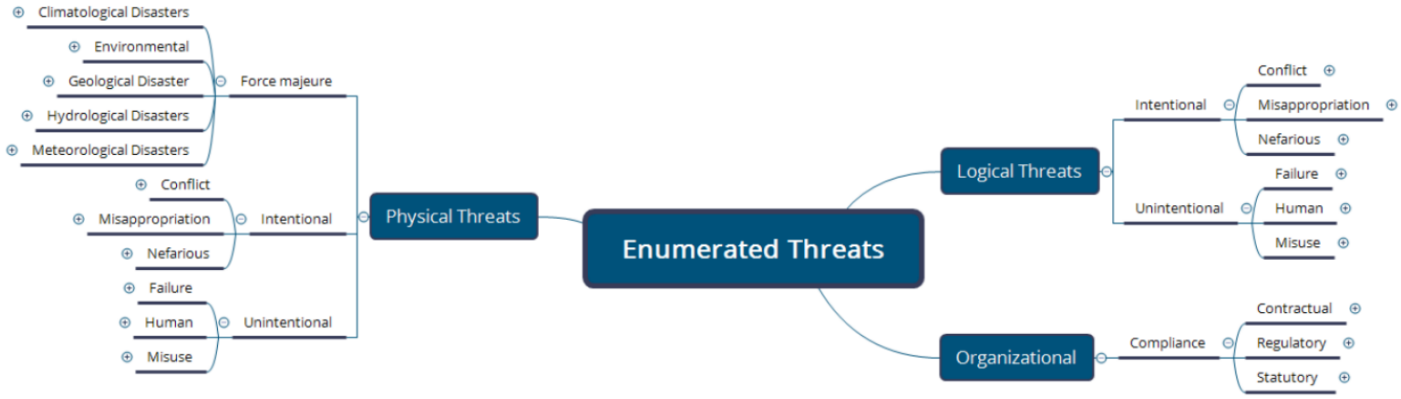


It is by selecting all the inherent risk factors relevant to a specific scope of application that an organization can obtain a subset of control requirements from each HITRUST CSF control to produce an initial control baseline from the HITRUST CSF control library. Additional tailoring to address its unique business needs and threat environment will produce the organization-specific overlay required for implementation and assessment.

HITRUST Threat Catalog

To help with this tailoring, HITRUST also provides a comprehensive cyber threat taxonomy along with a detailed mapping of the enumerated threats to HITRUST CSF controls in the HITRUST Threat Catalogue. The explicit alignment of threats to the HITRUST CSF produces a combination not found in other frameworks. It simplifies the risk analysis process for organizations and reduces some of the burden, costs, and confusion otherwise experienced when attempting to achieve this level of analysis. Identifying threats is a major component of a comprehensive risk analysis process for any organization seeking to protect their sensitive data and helps determine what adverse events are relevant to the organization and must be controlled.[94]

Figure 19. HITRUST Threat Taxonomy



HITRUST Assurance Program[vi]

The HITRUST Assurance Program provides industry with a common, standardized approach to evaluating cyber risk through the rigorous assessment of HITRUST CSF controls[95] specified in an organizational-level overlay, which also serves as its Target Profile and subsequently defines its risk target.[96] There are many features of the HITRUST Assurance Program's assessment and reporting approach that distinguishes HITRUST assessments[97] from other commercially available assessment available today in terms of the accuracy and precision of the results.[98] Examples include the Program's extensive assessment guidance,[99] the training and vetting of qualified assessors,[100] the implementation maturity model used to evaluate every HITRUST CSF control requirement,[101] and the centralized quality assurance review[102] of every assessment for which HITRUST issues a report. This results in a portfolio of assessments that have some of the highest rely-ability in the industry.[vii]

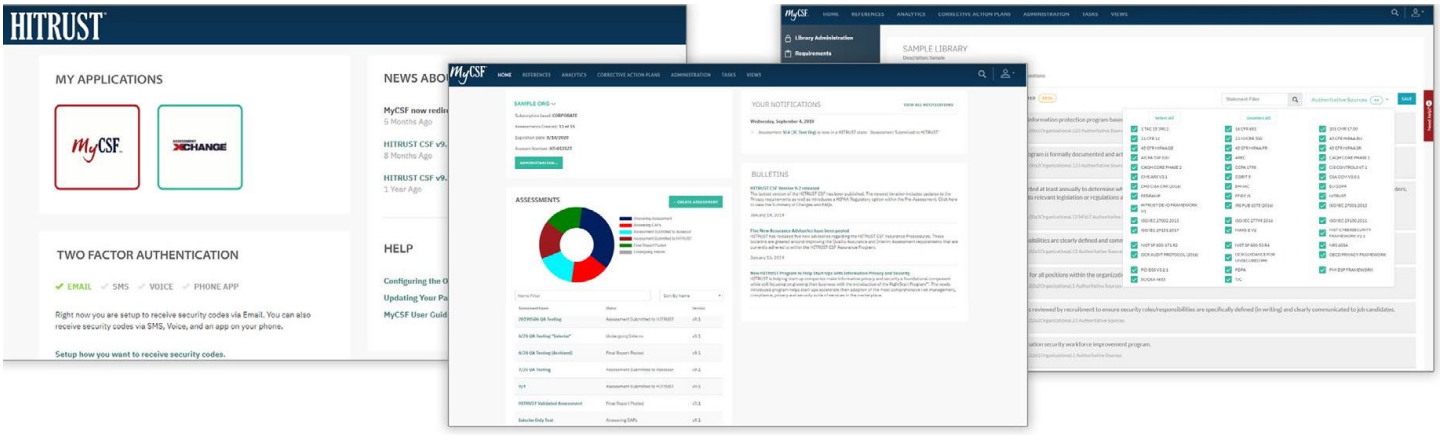
Organizations can also leverage the HITRUST Assurance Program to streamline third-party risk management (TPRM) processes.[103] By using a single comprehensive framework—the HITRUST CSF—to enable a single assessment to produce reports in multiple formats, the HITRUST Third-Party Assurance Program can result in significant reductions in both level of effort and overall cost. An increasing number of organizations are now requiring their third parties to undergo a HITRUST assessment rather than rely on proprietary information security questionnaires and on-site audits. By requiring a level of assurance commensurate with the inherent risk third parties present, organizations can reduce the significant number of hours and dollars spent on running a TPRM program and allow scarce resources to be more focused on those third parties that really matter.[104]

Other Programs, Products, and Services[viii]

The HITRUST MyCSF tool provides organizations of all sizes with a purposefully designed and engineered Software as a Service (SaaS) solution for performing assessments against the HITRUST CSF and managing corrective action plans (CAPs), including enhanced benchmarking and dashboards as well as integration with the HITRUST Assessment XChange™. This capability helps make the management of information risk and compliance with international, federal, and state security and privacy regulations easier and more cost-effective for any organization leveraging the HITRUST Approach. With the HITRUST MyCSF platform, organizations can address their evolving assessment needs as they manage risk in the ever-changing operational, cyber threat, and global regulatory landscape.[105]

[vi] Content in this section comes directly from their respective sources, either wholly or in part.
[vii] HITRUST defines rely-ability as the ability of a relying party to trust (or have confidence in) the results of an assessment in terms of its transparency, comprehensiveness, prescriptiveness, scalability, consistency, accuracy, and efficiency, all of which contribute to the overall rigor, suitability and impartiality of the approach. (Further definitions are provided in the glossary.)
[viii] Content in this section comes directly from their respective sources, either wholly or in part.

Figure 20. HITRUST MyCSF SaaS Platform

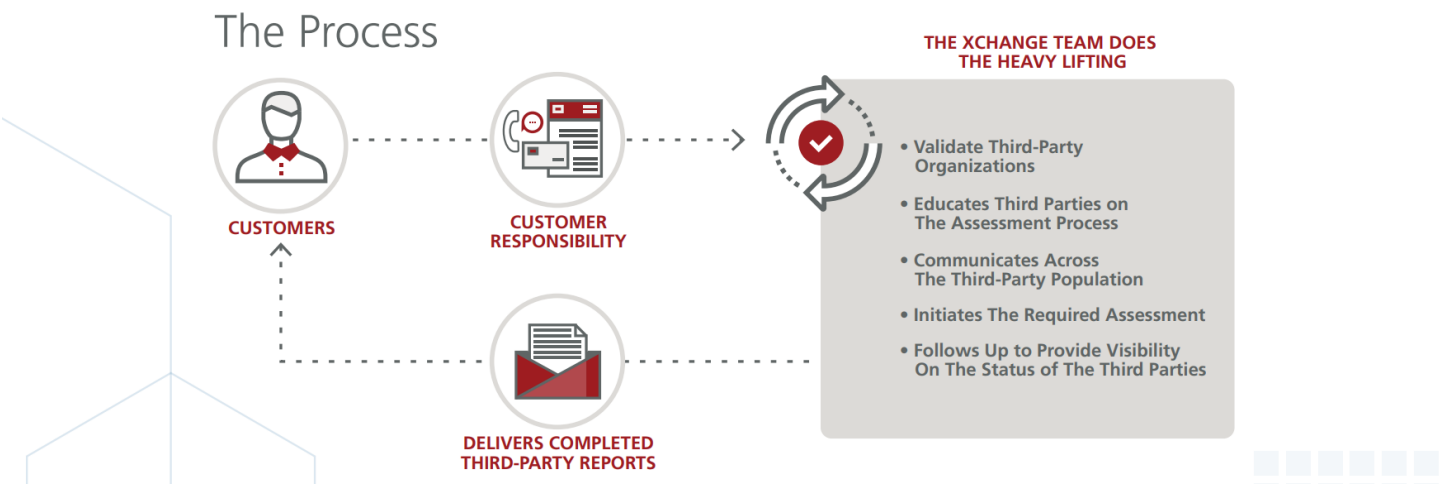


The HITRUST Assessment XChange ("the XChange") provides a turn-key program that you can leverage to manage the third-party assessment process. The XChange streamlines and simplifies the process of managing and maintaining risk assessment and compliance information from third parties. This is accomplished by offloading the time-consuming activities with which your organization is currently tasked, including:

- Identification of appropriate contacts responsible for security and privacy compliance within third parties
- Communication of contractual requirements and expectations
- Education of third parties on your process and expectations
- Facilitation of your organization's engagement when a third party is not appropriately meeting their requirements, allowing you to focus on managing risk rather than the administrative process

By participating in the XChange, organizations can constant visibility into their third parties' assessment statuses before, during, and after the assessment process. The XChange collects granular information about a third party's security posture, including CAPs, by providing the full HITRUST CSF Report. This detailed information is delivered electronically in a format that is easily integrated into your existing GRC or VRM solutions.[106]

Figure 21. The HITRUST Assessment XChange[107]

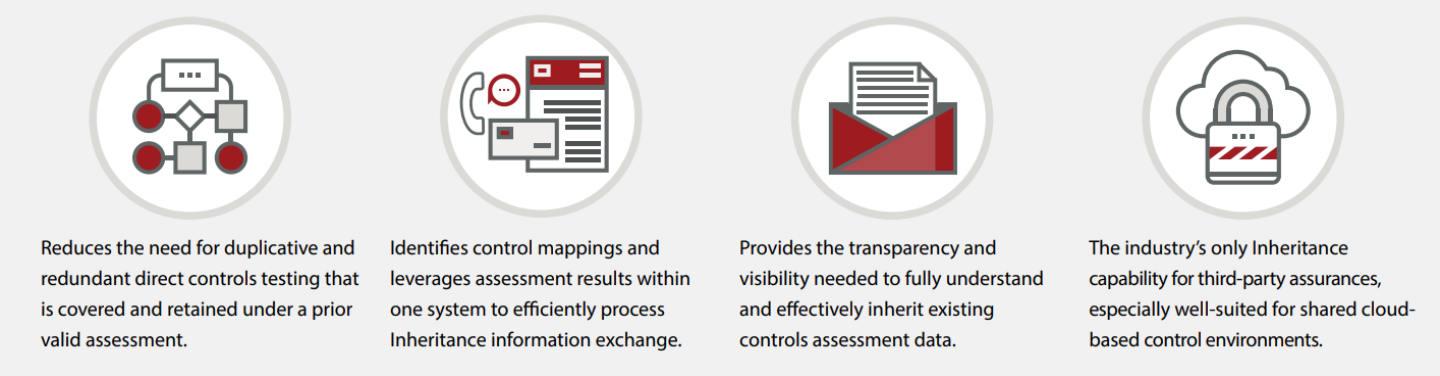


The HITRUST Shared Responsibility and Inheritance Program allows organizations to place reliance on shared information protection controls that are available from internal shared IT services and external third-party organizations, including: service providers, vendors and suppliers of cloud-enabled applications and technology platforms, colocation data center hosting services, and other managed services.

The HITRUST Shared Responsibility and Inheritance Program includes two highly innovative, efficient, integrated solutions that combine to create a unique means to save time and money by automatically identifying and importing control testing results and scoring from prior HITRUST Validated or Certified Assessments.

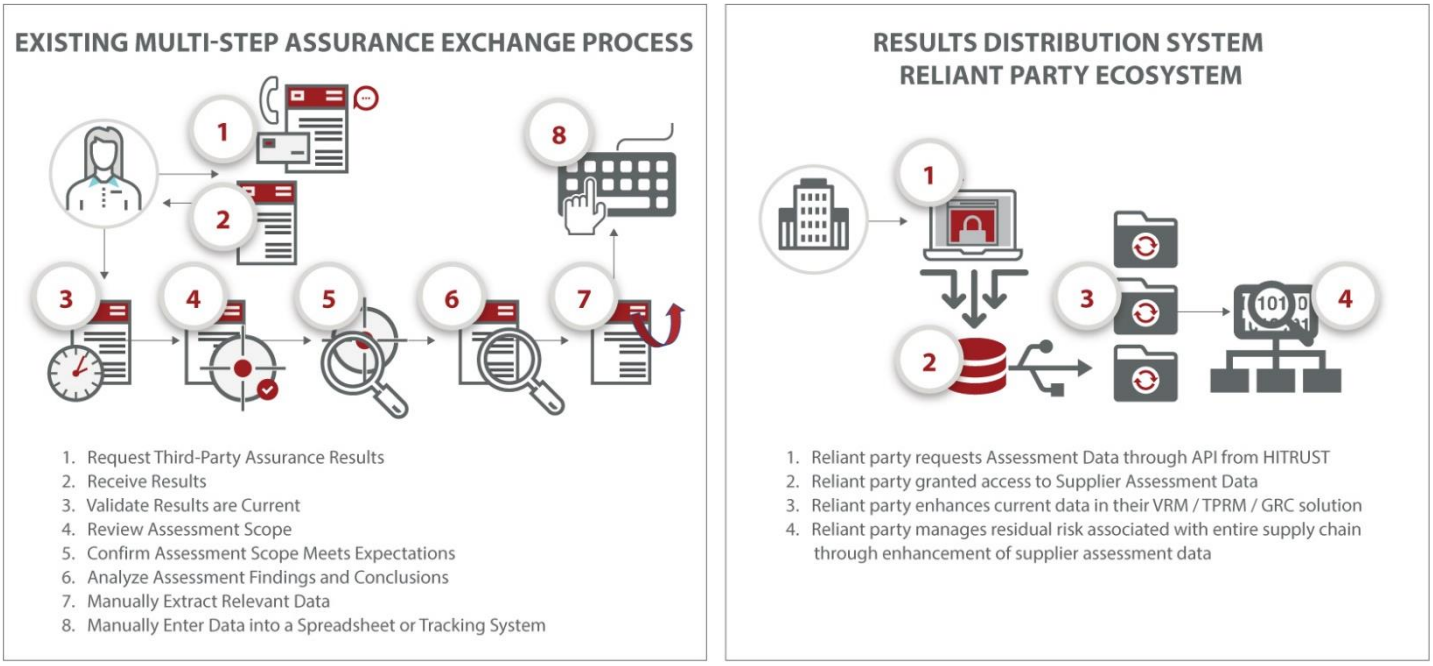
(1) The HITRUST Shared Responsibility Matrix® (SRM) is a no-cost, easy-to-use, out-of-box, baseline template with pre-populated shared responsibility and controls inheritability that are perfectly suitable for shared cloud environments. Commonly adopted by leading cloud service providers and their user communities of relying customers.
(2) When performing HITRUST Assessments, HITRUST Control Inheritance optimizes the use of prior HITRUST Validated or Certified Assessment results along with reliance on sharing cloud controls.
    a. MyCSF External Inheritance*. With a HITRUST MyCSF subscription, organizations can import control assessment results and scores from other HITRUST e1, i1, or r2 Validated Assessments that have been published (enabled) for External Inheritance by hosting, cloud, or other service providers.
    b. MyCSF Internal Inheritance. Organizations can leverage and repurpose their own prior controls assessment results and scores that are internally inheritable to or from other HITRUST Assessments belonging to that same organization. Reusing all or part of existing assessment results allows scoping centralized and decentralized control environments into smaller sub-divisions without the duplication of evidence-gathering and controls testing, scoring, and commentary.[108]

Figure 22. Key Benefits of Shared Responsibility and Inheritance[109]



The HITRUST Results Distribution System (RDS) makes it possible for assessed entities to share results from their HITRUST Assessments securely and electronically with any relying party. Those recipients can then manage and review essential information – such as assessment date, scope, control requirements, scores, CAPs, and more – using the API interface and their own TPRM solution. This automation adds efficiency and saves time by eliminating the multiple back-and-forth communications that are common between parties during the annual vendor review process. Whether relying parties manage hundreds or thousands of vendors, RDS delivers game-changing innovation and efficiencies.[110]

Figure 23. Improving the Results Distribution Process



And finally, the HITRUST Academy offers the only training courses designed to educate security and privacy professionals about information protection, privacy, assessing against the ever-evolving threat and compliance landscape, and utilizing the HITRUST CSF® framework to manage risk.[111]

Figure 24. HITRUST Academy Courses

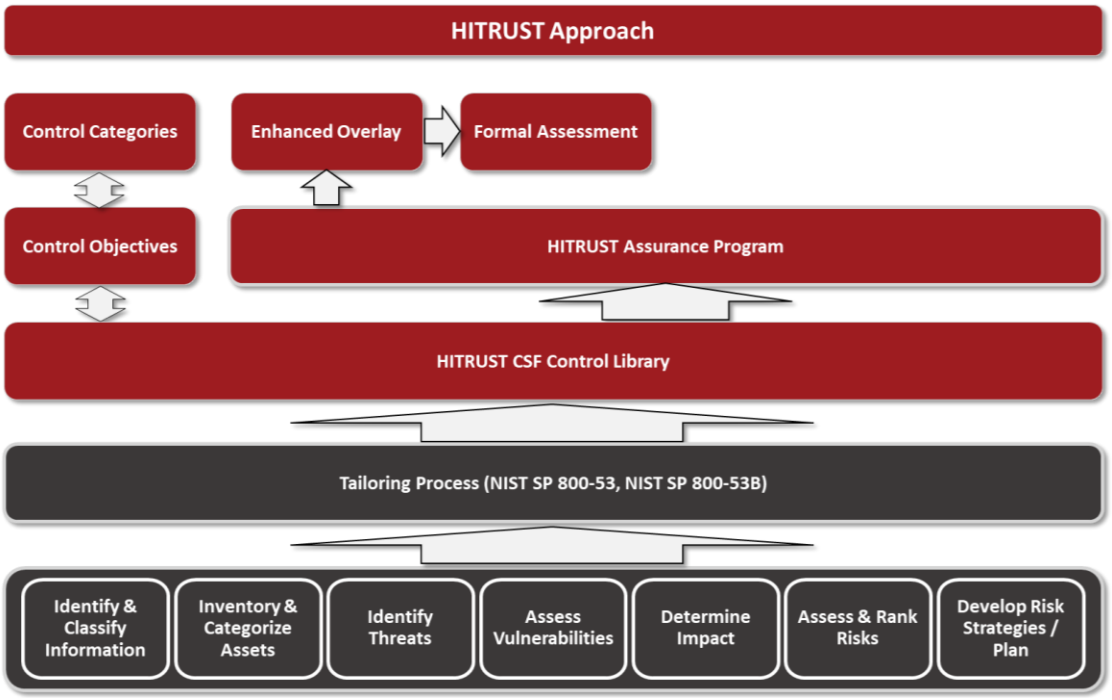
Notional HITRUST Approach Structure

The overall structure of the HITRUST Approach can now be shown in the same way the NIST Cybersecurity Framework Structure was depicted earlier. By leveraging control framework-based risk analysis and a NIST-based tailoring process, HITRUST developed an enhanced overlay of the NIST SP 800-53 moderate impact baseline designed to meet cybersecurity objectives in a wide range of topical areas.

By parsing controls in the HITRUST CSF enhanced overlay into essential 'good hygiene' practices, best/leading practices, and more robust practices in relevant control segments based on the inherent risk of an activity, process, technology, or a specific type or quantity of information, organizations can scale/scope the HITRUST control library to meet their particular needs through the tools available in the HITRUST Assurance Program (and MyCSF).

The HITRUST Assurance Program then supports the assessment of the resulting Control Specification in the organizational-level overlay to provide a wide range of highly 'rely-able' assessment and reporting options specifically designed to meet the needs of multiple internal and external stakeholders such as executive management, boards of directors, customers, business partners, and regulators.

Figure 25. HITRUST Approach Structure



Integrated Cyber Resilience Framework Implementation

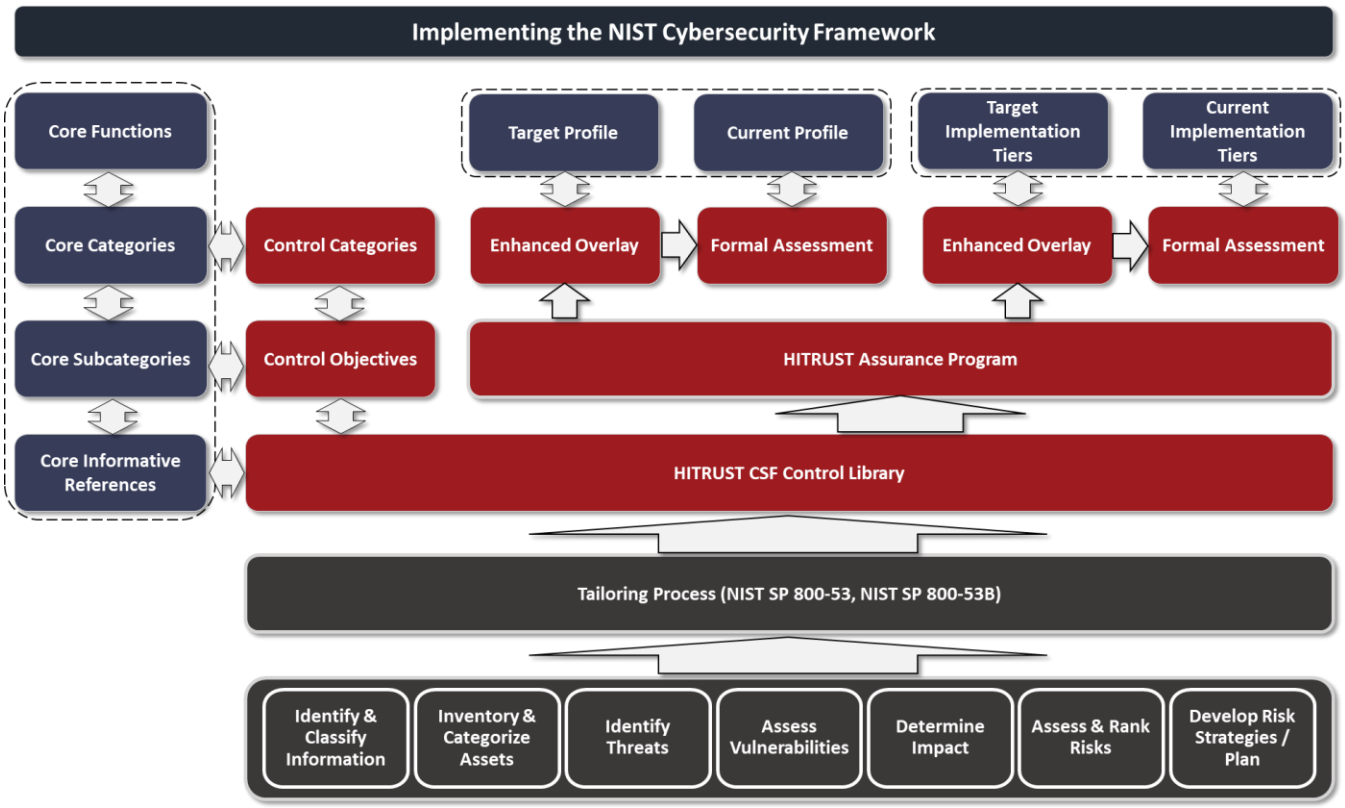
Always do right. This will gratify some people [and] astonish the rest.

– Mark Twain[112]

Integrated Cyber Resilience Framework

As stated previously, the NIST Cybersecurity Framework cannot be implemented without the addition of supporting control frameworks and risk management methodologies to support the selection of controls from these frameworks. Having depicted notional framework structures for both the NIST Cybersecurity Framework and the HITRUST Approach, it is now possible to show how the two separate framework structures can be integrated into a comprehensive approach to cyber resilience.

Figure 26. The HITRUST Approach to Cyber Resilience



The HITRUST CSF control library is the NIST Cybersecurity Framework Core Informative Reference used to for the Framework's implementation. HITRUST CSF Control Objectives and Categories are generally equivalent to the NIST Cybersecurity Framework Core Subcategories and Categories, respectively (although a case could also be made for the HITRUST CSF Control Specifications, which provide the overall objective of the underlying control requirements for each HITRUST CSF Control Reference). The NIST Cybersecurity Framework Core Functions exist at a higher level by organizing the lower-level structures in a way that incorporates major elements of a cyber incident response process.[113] The HITRUST Assurance Program then supports the specification of an organization's Target Profile via its organizational-level overlay, which is then used to assess the state of the organization's Target Profile and subsequently produce its Current Profile. And, although additional work needs to be done in this area, such a specification and assessment can potentially provide an indication of the organization's Target and Current Tiers.

Integrated Framework Implementation Process

The NIST Cybersecurity Framework outlines a relatively generic 5-step approach to implementing the Framework through the use of Profiles:[114]

Figure 27. NIST CSF 5-Step Implementation Approach

This approach differs from the 7-step approach previously articulated by NIST in that it doesn't specify the order in which the Current and Target Profiles are performed.[115] This is a step forward, as it allows organizations the flexibility of taking NIST's original approach to designing or specifying their own controls or leveraging a framework-based risk analysis to select and modify a control baseline or overlay.

Subsequently, organizations leveraging the HITRUST Approach should take the following steps to implementing the Framework.

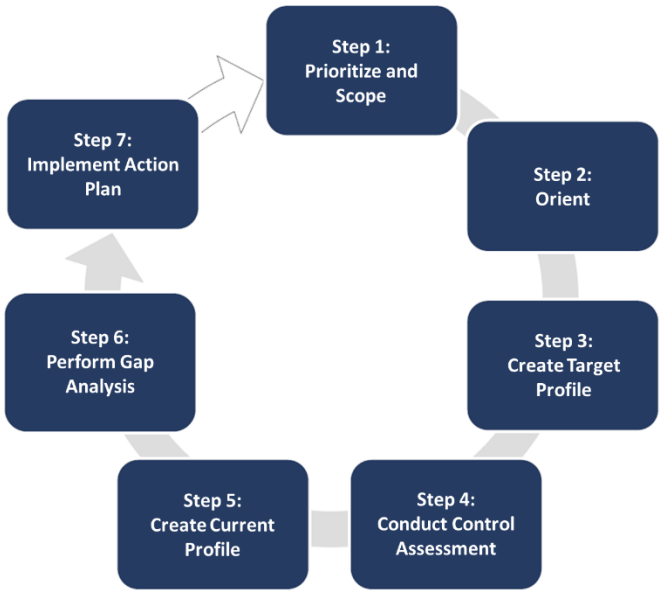
Step 1: Prioritize and scope organizational components for application of the framework
Step 2: Identify systems and existing risk management approaches within the scope
Step 3: Create a desired risk management profile based on the organization's risk factors (Target Profile)
Step 4: Conduct a control 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[116]

Target Profiles are easily obtained once organizations scope their organizational environment and systems, tailor the HITRUST CSF controls based on their organizational, system and compliance risk factors (i.e., a Community Profile[117]), and then further tailor the overlay to address any unique threats. Although there is no need to develop a Current Profile beforehand, some basic information about the state of the organization's cybersecurity program will necessarily be ascertained before the Target Profile is complete.

Through the creation of a Current Profile, organizations can examine the extent to which they are achieving the outcomes described in the Core Categories and Subcategories, aligned with the six high-level Functions: Govern, Identify, Protect, Detect, Respond, and Recover. An organization may find that it is already achieving the desired outcomes, thus managing cybersecurity commensurate with the known risk. Alternatively, an organization may determine that it has opportunities to (or needs to) improve. The organization can use that information to develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk. An organization may also find that it is overinvesting to achieve certain outcomes and use this information to reprioritize resources.

The figure on the next page further illustrates the seven-step process organizations can use to create a new cybersecurity program or improve an existing program. These steps should be repeated as necessary to continuously improve cybersecurity and their management of cyber-related risk.[118] And, as with the any 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.

Figure 28. Revised NIST Cybersecurity Framework Implementation Process



Each step is now discussed in more detail, first introduced by a table[119] describing the step's inputs, activities, and outputs followed by additional explanation. A table of the inputs, activities, and outputs for all seven steps is also included in **Error! Reference source n ot found.**.

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 Approach	1. Organization determines where it wants to apply the HITRUST Approach 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 many organizations, leveraging the HITRUST Approach is a central component of that strategy as it (1) forms the basis of their control framework-based risk analysis, (2) informs the organization on the minimum level of due care and due diligence required to adequately protect sensitive information and meet its multiple compliance obligations, and (3) 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 Approach (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,[120] availability of resources, and other internal and external factors. Current threat and vulnerability information may also help inform scoping decisions.

An organization leveraging the HITRUST Approach for the first time may 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 HITRUST Approach to a broader subset of operations or to additional parts of the organization as appropriate.

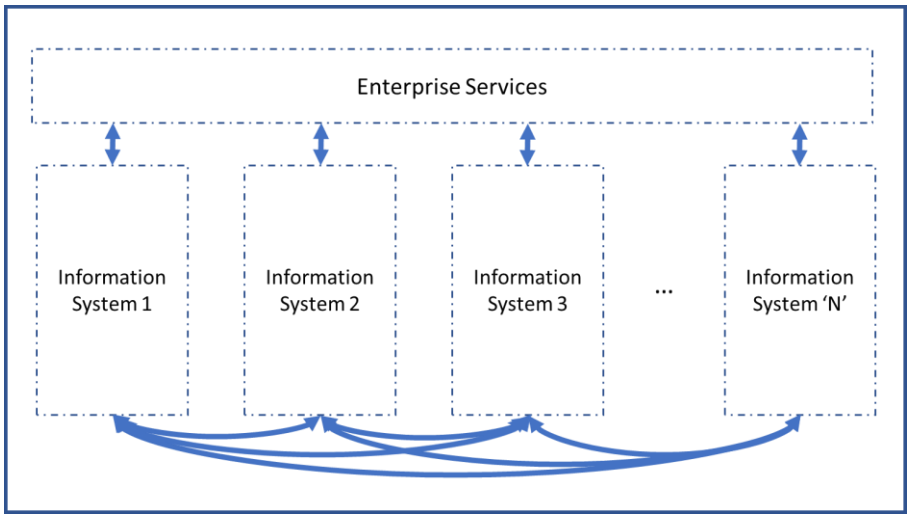
Step 2: Orient

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

Step 2: Orient		
Inputs	**Activities**	**Outputs**
1. Usage scope 2. Risk management strategy 3. HITRUST Approach	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 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. To do this, organizations should segment their information systems based on the sensitivity and/or criticality of the information they process and strictly define the interfaces between and amongst each segment or 'scope of application.'[121]

Figure 29. Segmenting the Organizational Environment



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 Approach	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 HITRUST CSF and then tailors the overlay further to account for any unique threats (as compared to other, similar organizations with the same risk factors).

This includes removing, modifying, or replacing controls in the overlay as well. 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 compliance 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.[122]

The organization should determine the 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 (which is determined based on a control assessment in the next step). 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 on NIST Cybersecurity Framework Implementation.

The organization should also determine its goals around the Risk Management Process, Integrated Risk Management Program, and External Participation for the target NIST Cybersecurity Framework Tier and identify (1) the HITRUST CSF control requirements needed to achieve them[ix] as well as (2) the equivalent levels of compliance for each level of the HITRUST CSF Control Maturity Model, i.e., around Policy (P), Procedure (Pr), Implemented (I), Measured (Me), and Managed (Ma), for these Tier-related control requirements.

[ix] HITRUST is working to identify specific HITRUST CSF control requirements that are representative of each NIST Cybersecurity Framework Tier for each of the topical areas addressed by the model: Risk Management Process, Integrated Risk Management Program, and External Participation. This information will be made available through the HITRUST website and/or MyCSF SaaS platform when the work is complete.

Table 4. Minimum Maturity Scores for Tier-Related HITRUST CSF Controls

NIST CSF Tier	Brief Tier Description	Control Maturity				
		P	Pr	I	Me	Ma
Tier 1 - Partial	• Risk managed in an ad hoc fashion. • Limited awareness of cybersecurity risk by the organization.					
Tier 2 – Risk-Informed	• Mgmt. activities informed by organizational risk objectives. • Aware but no org-wide approach to managing cyber risk.			FC		
Tier 3 – Repeatable	• Practices supported by policy and updated regularly. • Organization-wide approach to risk management.	FC	PC	FC		
Tier 4 – Adaptive	• Continuously improves cybersecurity activities. • Cyber risk is managed similar to other organizational risks.	FC	FC	FC	PC	PC

Legend: NC – Non-compliant; SC – Somewhat Compliant; PC – Partially Compliant; MC – Mostly Compliant; C – Compliant

(1) Since **Tier 1** is generally 'ad hoc' in nature and NIST specifically recommends organizations in this Tier move to a higher Tier, HITRUST does not identify specific minimums around the maturity of implementation of Tier-related controls.
(2) Organizations at **Tier 2** should be, at a minimum, fully compliant with the Implemented level of the maturity model.
(3) Organizations should be fully compliant for Policy at **Tier 3** since the Tier description specifically states this. HITRUST recommends an organization have procedures around its most critical practices to help ensure repeatability.
(4) **Tier 4** organizations should be fully compliant with Policy, Procedures, and Implemented for all related control requirements. And to be truly adaptive, i.e., support continuous improvement, HITRUST recommends the most important or critical cybersecurity controls related to this Tier level have formal documented metrics on their performance and they be actively managed based on those metrics.

Step 4: Conduct a Control Assessment

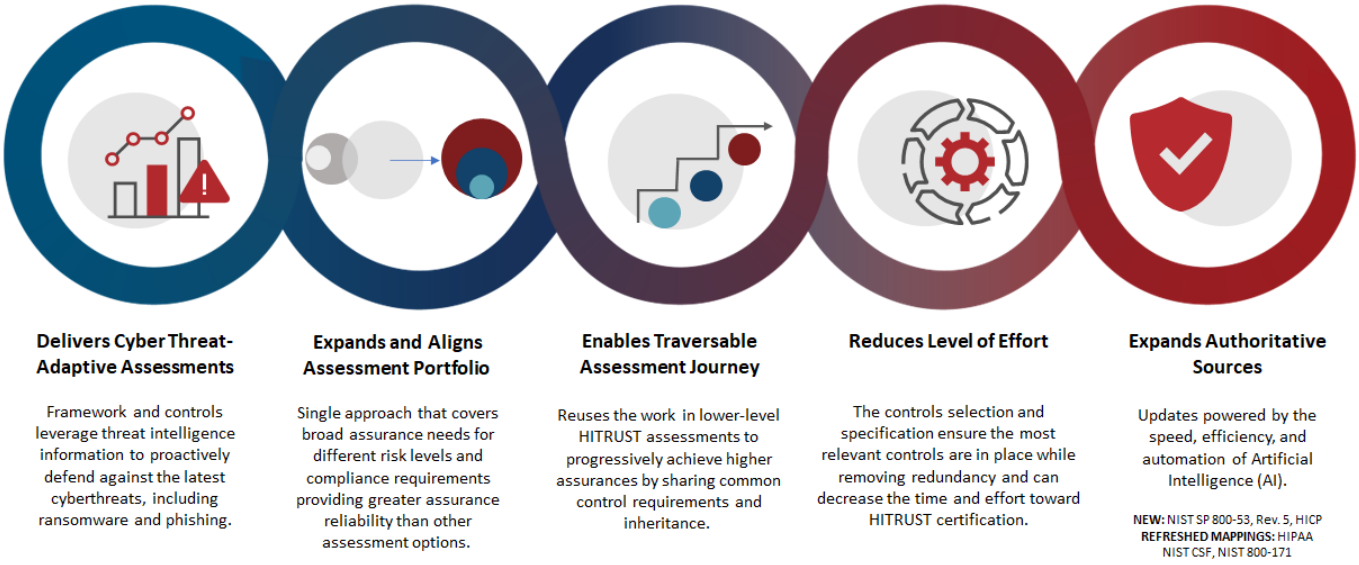
Table 5. Step 4: Risk Assessment Inputs, Activities, and Outputs

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

Evaluation of the maturity of the organization's control implementation through a control assessment—often if not somewhat inaccurately referred to as a risk assessment—is performed in this step. Organizations perform control assessments to identify and evaluate deviations in the implementation of controls specified in the Target Profile and—since the Target Profile helps define an organization's risk target—helps identify excessive residual risk due to control noncompliance. The output of the control assessment activities assists the organization in developing its Current Profile and Tier based on control maturity, which occurs in Step 5. For organizations 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 control assessment.

The HITRUST Assessment Portfolio[123] offers a wide range of 'rely-able' assessments, which allows organizations to efficiently tailor an assessment to meet the various assurance needs of their relying parties, both internal and external.

Figure 30. Rely-ability and Efficiency of the HITRUST Assessment Portfolio



However, organizations should perform a HITRUST Risk-based, 2-year (r2) Validated Assessment[124] tailored using all the inherent risk factors applicable to the assessments scope if they want the ability to automatically create their NIST Cybersecurity Framework Current Profile from the assessment.[x] And, if an organization wishes to assess HITRUST CSF control requirements for all 135 HITRUST CSF controls for a complete picture of its Current and Target Profiles, it should also select a comprehensive assessment rather than the baseline assessment of the 75 controls required for HITRUST CSF certification.

Step 5: Create a Current Profile

Table 6. Step 5: Current Profile Inputs, Activities, and Outputs

Step 5: Create a Current Profile		
Inputs	**Activities**	**Outputs**
1. Control assessment reports 2. HITRUST Approach	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 Cybersecurity Framework Tier model)

Once the quality assurance process for a HITRUST r2 Validated Assessment is complete, HITRUST will issue a HITRUST r2 Validated Assessment Report along with our NIST Cybersecurity Framework Validated or Certified Report.[125] The HITRUST r2 Assessment Report will provide the results of the assessment based on the HITRUST CSF control framework, and the NIST Cybersecurity Framework Report will provide both the Target Profile and the Current Profile based on the assessment maturity of the HITRUST CSF control requirements that map to the NIST Cybersecurity Framework Core Subcategories. A complete template for HITRUST's NIST Cybersecurity Framework Certification Report is provided in

[x] A HITRUST CSF r2 Readiness Assessment may also be used; however, this assessment does not offer HITRUST's NIST Cybersecurity Framework Validated or Certified Report. A Current Profile would subsequently need to be generated 'manually' using the HITRUST CSF to NIST Cybersecurity Framework mappings available on the HITRUST MyCSF SaaS platform.

Appendix C – NIST Cybersecurity Framework Certification Report.

Step 6: Perform Gap Analysis

Table 7. 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. Control assessment/analysis reports 9. HITRUST Approach	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 (CAPs)

The organization then evaluates its Current Profile and Tier against its Target Profile and Tier and identifies any gaps in the maturity of their implementation. When mapping back to the NIST Cybersecurity Framework, a gap exists when there is (1) a desired Category or Subcategory outcome in the Target Profile or (2) a program characteristic in the Target 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 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 (correct) them—a process referred to as mitigation—to reduce the risk.

HITRUST requires assessed entities requesting a Validated or Certified Report to prepare CAPs, which must describe the specific measures intended to remediate deficiencies identified during an assessment. A complete CAP should include, at a minimum, a control gap identifier, description of the control gap, CSF control mapping, point of contact, scheduled completion date, corrective actions, how the weakness was identified (assessment, Assessor, date), date identified, and current status. 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.

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—if desired—the requirements for CSF certification. However, while 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.[126]

To help with CAP prioritization, HITRUST provides non-contextual[xi] impact codes derived from similar codes previously used by the DoD[xii]and priority codes derived from their NIST counterparts[127] to help organizations prioritize corrective actions.[128]

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

Step 7: Implement Action Plan

Table 8. Step 7: Implement Action Plan Inputs, Activities, and Outputs

Step 7: Implement Action Plan		
Inputs	**Activities**	**Outputs**
1. Prioritized implementation plan (CAPs) 2. HITRUST Approach	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 its CAPs and tracks their 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.

Process Summary

This implementation approach can help organizations leverage the HITRUST Approach 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 Cybersecurity Framework, identify improvements, and communicate results. It can incorporate and align with processes and tools the organization is already using or plans to use.

The implementation process is also 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.

[xi] Impact codes are non-contextual in that they estimate the probable impact should a control fail while making no assumptions about the state of other controls specified in the Target Profile.
[xii] Impact codes were derived from similar codes used by the U.S. Department of Defense (DoD) in their legacy DoD Information Technology Security Certification and Accreditation Program (DITSCAP).
[xiii] Cline, B. (2023a).

Final Thoughts

While the NIST Cybersecurity Framework is currently viewed as voluntary guidance, this stance may very well change given the recent National Cybersecurity Strategy released by The White House in March 2023, which indicates a shift from voluntary guidance to a mix of voluntary and performance-based regulations that "leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance—including … the [NIST Cybersecurity Framework]." This shift in the national strategy has the potential to place significant responsibility on critical infrastructure owners and operators as well as federal contractors and technology companies that provide programs, products, and services to critical infrastructure. Organizations that use or intend to use HITRUST programs, products, and services will subsequently find this document extremely valuable as they integrate the NIST Cybersecurity Framework into their cybersecurity programs and subsequently communicate the state of these programs to relevant stakeholders, including industry, state, and federal regulators.

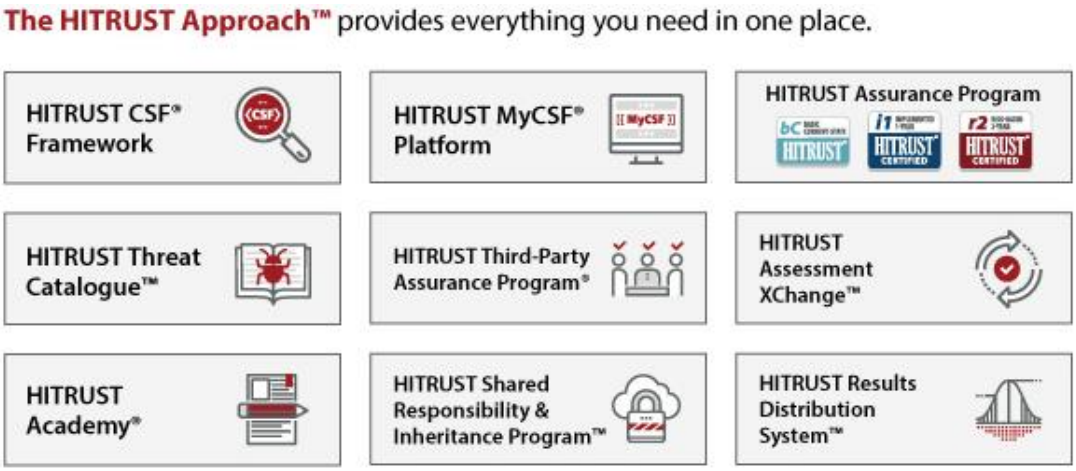
About the Author

Bryan Cline, Ph.D., Chief Research Officer, HITRUST

Bryan provides thought leadership on risk management and compliance and develops the methodologies used in various components of the HITRUST Approach. This includes a focus on the design of the HITRUST CSF and the assessment and certification models used in the HITRUST Assurance Programs, for which he provides technical direction and oversight. He is also responsible for addressing emerging trends impacting risk management and compliance to ensure the HITRUST Approach sets the bar for organizations seeking the most comprehensive privacy and security frameworks available. Bryan previously served as HITRUST's Vice President of Standards and Analysis

About HITRUST

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks, as well as related assessments and assurance methodologies.



HITRUST also actively participates in many efforts in government advocacy, community building, and cybersecurity education. For more information, visit www.hitrustalliance.net.

Appendix A – Glossary of Terms

Acceptable Risk	The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific IT system. [NIST Glossary]
Adequate Security [Protection]	Security [protection] commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [NIST Glossary]
Analysis Approach	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. [NIST Glossary]
Assessment	See Security Control Assessment or Risk Assessment.
Assessment Scope	The information systems and technology, infrastructure, and organizational elements that are the target of assessment. [HITRUST]
Asset(s)	Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). [NIST Glossary]
Assurance	Grounds for justified confidence that a claim has been or will be achieved. Note 1: Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated. Note 2: Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims. [NIST Glossary]
Attack	Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. [NIST Glossary]
Attack Surface	The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment. [NIST Glossary]
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NIST Glossary]
Availability	Ensuring timely and reliable access to and use of information. [NIST Glossary]
Avoidance Control	A general class of control that helps minimize a target's attack surface or otherwise reduce the frequency with which a threat actor comes into contact with an asset. [HITRUST]
Capability (Threat Actor)	The ability of a threat actor to successfully exploit one or more vulnerabilities to achieve an objective and generally consists of a threat actor's knowledge, skills, and tools (and other resources). [HITRUST]
Care	The process of protecting someone or something and providing what that person or thing needs. [Cambridge Dictionary]
Category [NIST]	See CSF Category [NIST]
Community Profile	See CSF Community Profile [NIST]

Compensating Security Control(s)	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. [NIST Glossary]
Compliance	An adherence to the laws, regulations, standards, guidelines, and other specifications [such as contractual obligations] relevant to an organization's business. [Adapted from the HITRUST Risk vs. Compliance Whitepaper, p. 3]
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [NIST Glossary]
Control Assessment	See Security Control Assessment
Control Category	The highest topical level in the HITRUST CSF control framework. [HITRUST]
Control Function	The manner in which a control addresses a threat to manage associated risk. [HITRUST]
Control Implementation Requirement	A granular, often prescriptive requirement or activity within a HITRUST CSF control intended to help an organization achieve the outcome indicated by its Control Specification. [HITRUST]
Control Maturity	The extent to which a control is defined, implemented, measured, managed/controlled, and effective. [HITRUST] Also, 'Control Implementation Maturity.'
Control Objective	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process. [ISACA]
Control Purpose	Synonymous with Control Function.
Control Requirement	See Control Implementation Requirement.
Control Specification	The policies, procedures, guidelines, practices, or organizational structures specified in a control, which can be of administrative, technical, management, or legal nature, to meet a control objective. [HITRUST]
Control(s)	The means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of an administrative, technical, management, or legal nature. An attribute assigned to an asset that reflects its relative importance or necessity in achieving or contributing to the achievement of stated goals. [NIST Glossary] Synonymous with 'Countermeasures' and 'Safeguards.' A [HITRUST CSF] control is a collection of implementation requirements intended to satisfy the objective or outcome [identified] by a control specification; includes a control reference, i.e., a control number and name, risk factors, topical area tags, and supporting authoritative sources. [HITRUST]
Core	See CSF Core [NIST]
Core Category	See CSF Category [NIST]
Core Function	See CSF Function [NIST]
Core Subcategory	See CSF Subcategory [NIST]

Corrective Action	Activities intended to remediate control deficiencies; actions taken to address causes of non-conformity, preclude hazards, or prevent the recurrence of a problem. [HITRUST]
Corrective Action Plan (CAP)	Corrective actions for an issuer for removing or reducing deficiencies or risks identified by the Assessor during the assessment of issuer operations. The plan identifies actions that need to be performed in order to obtain or sustain authorization. [NIST Glossary]
Countermeasure(s)	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. [NIST Glossary] Synonymous with 'Controls' or 'Safeguards.'
Course of Action	A time-phased or situation-dependent combination of risk response measures. [NIST Glossary]
Criticality	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. [NIST Glossary]
CSF [HITRUST]	The HITRUST risk-based cybersecurity, privacy, and compliance framework. [HITRUST]
CSF [NIST]	The NIST Cybersecurity Framework. [NIST Glossary]
CSF Category [NIST]	A group of related cybersecurity outcomes that collectively comprise a CSF Function. [NIST Glossary]
CSF Community Profile [NIST]	A baseline of CSF outcomes that is created and published to address shared interests and goals among a number of organizations. A Community Profile is typically developed for a particular sector, subsector, technology, threat type, or other use case. An organization can use a Community Profile as the basis for its own Target Profile. [NIST Glossary]
CSF Core [NIST]	A taxonomy of high-level cybersecurity outcomes that can help any organization manage its cybersecurity risks. Its components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome. [NIST Glossary]
CSF Current Profile [NIST]	A part of an Organizational Profile that specifies the Core outcomes that an organization is currently achieving (or attempting to achieve) and characterizes how or to what extent each outcome is being achieved. [NIST Glossary]
CSF Function [NIST]	The highest level of organization for cybersecurity outcomes. There are six CSF Functions: Govern, Identify, Protect, Detect, Respond, and Recover. [NIST Glossary]
CSF Implementation Example [NIST]	A concise, action-oriented, notional illustration of a way to help achieve a CSF Core outcome. [NIST Glossary]
CSF Informative Reference [NIST]	A mapping that indicates a relationship between a CSF Core outcome and an existing standard, guideline, regulation, or other content. [NIST Glossary]
CSF Organizational Profile [NIST]	A mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes. [NIST Glossary]
CSF Subcategory [NIST]	A group of more specific outcomes of technical and management cybersecurity activities that comprise a CSF Category. [NIST Glossary]
CSF Target Profile [NIST]	A part of an Organizational Profile that specifies the desired Core outcomes that an organization has selected and prioritized for achieving its cybersecurity risk management objectives. [NIST Glossary]

CSF Tier [NIST]	A characterization of the rigor of an organization's cybersecurity risk governance and management practices. There are four Tiers: Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). [NIST Glossary]
Current Profile	See CSF Current Profile [NIST]
Cyber Incident	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. [NIST Glossary]
Cyber Resilience/Resiliency	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment. [NIST Glossary]
Cyber Risk	Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system. [NIST Glossary]
Cybersecurity	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. [NIST Glossary]
Cyberspace	The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. [NIST Glossary]
Data	Information in a specific representation, usually as a sequence of symbols that have meaning [or] pieces of information from which 'understandable information' is derived. [NIST Glossary]
Data Processing	The collective set of data actions (i.e., the complete data life cycle, including, but not limited to collection, retention, logging, generation, transformation, use, disclosure, sharing, transmission, and disposal). [NIST Glossary]
Decision Analysis	Logical methods for improving decision-making … [including] models for decision-making under conditions of uncertainty or multiple objectives; techniques of risk analysis and risk assessment; experimental and descriptive studies of decision-making behavior; economic analysis of competitive and strategic decisions; techniques for facilitating decision-making by groups; and computer modeling software and expert systems for decision support. [Decision Analysis Society]
Decision Support Control	A general class of control that involves actions taken to facilitate the decision analysis process and improve decision-making. [HITRUST]
Detective Control	A general class of control that involves the monitoring and identification of potential threat events. [HITRUST]
Deterrent Control	A general class of control that helps discourage a threat actor from initiating or taking advantage of (exploit) a contact. [HITRUST]
Diligence	[The] earnest and persistent application of effort, especially as required by law. [FindLaw Dictionary]

Due Care	The care that an ordinarily reasonable and prudent person would use under the same or similar circumstances; also called 'ordinary care' or 'reasonable care.' [FindLaw Dictionary] The level of care expected from a reasonable person of similar competency under similar conditions. [ISACA Glossary]
Due Diligence	Such diligence as a reasonable person under the same circumstances would use; use of reasonable but not necessarily exhaustive efforts; also called 'reasonable diligence.' [FindLaw Dictionary] The performance of those actions that are generally regarded as prudent, responsible, and necessary to conduct a thorough and objective investigation, review, and/or analysis. [ISACA Glossary]
Enhanced Overlay	An overlay that adds controls, enhancements, or additional guidance to security control baselines in order to highlight or address needs specific to the purpose of the overlay. See Overlay. Synonymous with Tailored Overlay. [NIST Glossary]
Enterprise	An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information, and mission management. [NIST Glossary]
Enterprise Risk Management [ERM]	The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats; and it assesses enterprise performance against threats and adjusts countermeasures, as necessary. [NIST Glossary]
Event	Any observable occurrence in an information system. [NIST Glossary]
Factor Analysis of Information Risk (FAIR)	An international standard quantitative model for understanding, analyzing, and quantifying cyber risk and operational risk in financial terms. [FAIR]
Function	See Function [NIST]
Impact	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. [NIST Glossary]
Impact Level	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. [NIST Glossary] Synonymous with Impact Value.
Implementation Example	See CSF Implementation Example [NIST]
Incident	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. [NIST Glossary]

Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. [NIST Glossary] Not to be confused with the term 'Data.'
Information Processing	The acquisition, recording, organization, retrieval, display, and dissemination of information. [Britannica]
Information Security Risk	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. [NIST Glossary]
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information…. to achieve one or more stated purposes…. Interacting elements … include hardware, software, data, humans, processes, facilities, materials, and naturally occurring physical entities…. Systems of systems is included [in this definition]. [NIST Glossary, adapted]
Information System-Related Security Risk	Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, other organizations, and the Nation. A subset of Information Security Risk. See Risk. [NIST Glossary]
Informative Reference	See CSF Informative Reference [NIST]
Inherent Risk	Risk that exists when the status of key controls is not taken into consideration or is otherwise unknown. [HITRUST]
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. [NIST Glossary]
Likelihood	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. [NIST Glossary]
Likelihood of Occurrence	See Likelihood.
Management	A problem-solving process of effectively achieving organizational objectives through the efficient use of scarce resources in a changing environment. [Kreitner]
Maturity Model	A set of characteristics, attributes, or indicators that represent progression in a particular domain. A maturity model allows an organization or industry to have its practices, processes, and methods evaluated against a clear set of requirements (such as activities or processes) that define specific maturity levels. At any given maturity level, an organization is expected to exhibit the capabilities of that level. A tool that helps assess the current effectiveness of an organization and supports determining what capabilities they need in order to obtain the next level of maturity in order to continue progression up the levels of the model. [CERT RMM v1.2]

Measure(s)

The results of data collection, analysis, and reporting. [NIST Glossary]

A standard used to evaluate and communicate performance against expected results (measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction; reporting and monitoring measures help an organization gauge progress toward effective implementation of strategy). [ISACA Glossary]

Measurement

The process of data collection, analysis, and reporting. [NIST Glossary]

Measurements are "observations that quantitatively reduce uncertainty." [Hubbard, D., Seiersen, R., Geer Jr., D., and McClure, S. (2016)]

Metadata

Data that provides information about other data. [Merriam-Webster]

Metric(s)

Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. [NIST Glossary]

A quantifiable entity that allows the measurement of the achievement of a process goal (metrics should be SMART—specific, measurable, actionable, relevant, and timely; complete metric guidance defines the unit used, measurement frequency, ideal target value (if appropriate), and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment). [ISACA Glossary]

Motivation (Threat Actor)

The drivers—be it emotional or the pursuit of supremacy or material gain—that causes a threat actor to commit harmful acts. [Derived from Intel]

Ontology

In the context of computer and information sciences, an ontology defines a set of representational primitives with which to model a domain of knowledge or discourse. The representational primitives are typically classes (or sets), attributes (or properties), and relationships (or relations among class members). The definitions of the representational primitives include information about their meaning and constraints on their logically consistent application. [Gruber]

Operational Risk

Risk of loss resulting from inadequate or failed internal process, people, and systems or from external events. Includes legal risk, but excludes strategic and reputational risk [Basel Committee]

Organization

An entity of any size, complexity, or positioning within an organizational structure. See Enterprise. [NIST Glossary]

Organizational Profile

See CSF Organizational Profile [NIST]

Overlay

A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process that is intended to complement (and further refine) security control baselines [to fit the user's specific environment and mission]. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. [NIST Glossary]

Policy

Overall intention and direction as formally expressed by management, most often articulated in documents that record high-level principles or course of actions; the intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives, and strategic plans established by the enterprise's management teams. [Adapted from the ISACA Glossary]

Preventive Control	A general class of controls that help reduce the likelihood a threat event will occur (or decrease their frequency of occurrence). [HITRUST]
Procedure	A detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes. [Adapted from the ISACA Glossary]
Processing	See Data Processing and/or Information Processing.
Profile	A representation of the outcomes that a particular system or organization has selected from the [NIST CSF] Categories and Subcategories. [NIST Glossary] A profile is a baseline set of minimal cybersecurity requirements for mitigating described threats and vulnerabilities, as well as supporting compliance requirements for a defined scope and type of a particular use case (e.g., industry, information system(s)), using a combination of existing cybersecurity guidance, standards and/or specifications baseline documents or catalogs. A profile organizes selected guidance, standard(s) and/or specification(s) and may narrow, expand and/or otherwise tailor items from the starting material to address the requirements of the profile's target application. [NIST Glossary]
Qualitative Assessment	A set of methods, principles, or rules for assessing risk based on non-numerical categories or levels. [NIST Glossary]
Quantitative Assessment	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. [NIST Glossary]
Quasi-quantitative Assessment	See Semi-Quantitative Assessment.
Quasi-Quantitative Residual Risk Analysis (QQRRA)	HITRUST's patent-pending quasi-quantitative approach to the analysis of excessive residual risk an organization may incur from its use of sensitive information in the conduct of its business/operations.
Recovery Control	A general class of control that involves actions taken to restore an organization to a pre-threat event state. [HITRUST]
Rely-ability	The ability of a stakeholder to rely upon the assurances provided by an entity. (HITRUST)
Rely-able	Assurances that provide a high degree of rely-ability. [HITRUST]
Relying Party	An internal or external stakeholder that is the intended recipient of an attestation, assessment, or other form of assurance. [HITRUST]
Repeatable	The ability to repeat an assessment in the future, in a manner that is consistent with, and hence comparable to, prior assessments. [NIST Glossary]
Residual Risk	Portion of risk remaining after security measures have been applied. [NIST Glossary]
Resilience	Elasticity or the ability of a material to return to its original shape after it is deformed by bending, stretching, or compression. [Random House Unabridged Dictionary] The ability to withstand or recover quickly from some type of adversity. [Oxford Advanced Learner's Dictionary]

Responsive Control	A general class of control that involves actions taken to mitigate the potential impact of a threat event. [HITRUST]
Risk	The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [NIST Glossary]
Risk Acceptance	The formal acceptance of a specific amount of risk by an individual or organization. [HITRUST]
Risk Analysis	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. [NIST Glossary]
Risk Appetite	The types and amount of risk, on a broad level, an organization is willing to accept in its pursuit of value. [NIST Glossary]
Risk Assessment	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, risk assessment incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis. [NIST Glossary]
Risk Assessment Methodology	A risk assessment process, together with a risk model, assessment approach, and analysis approach. [NIST Glossary]
Risk Avoidance	The elimination of risk by not engaging in a specific activity. [HITRUST]
Risk Evaluation	The process of comparing the estimated risk against given risk criteria to determine the significance of the risk. [ISACA Glossary]
Risk Factor	A characteristic in a risk model as an input to determining the level of risk in a risk assessment. [NIST Glossary]
Risk Management	The total process of identifying, controlling, and eliminating or minimizing uncertain events that may adversely affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. [NIST Glossary]
Risk Management Framework	A structured approach used to oversee and manage risk. [NIST Glossary]
Risk Mitigation	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. [A subset of Risk Response.] [NIST Glossary]
Risk Model	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. [NIST Glossary]
Risk Monitoring	Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions. [NIST Glossary]

Risk Profile	A prioritized inventory of the most significant risks identified and assessed through the risk assessment process versus a complete inventory of risks. [NISTIR 8286]
Risk Response	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. [NIST Glossary]
Risk Target	The desired level of risk that optimizes an organization's business objectives. [HITRUST]
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result for a specific activity. [NIST Glossary, adapted]
Risk Transference	The redirecting or sharing of risk with another party, e.g., through insurance or indemnification. [HITRUST]
Risk Treatment	Selecting and implementing mechanisms to modify risk. Risk treatment options can include avoiding, optimizing, transferring, or retaining [accepting] risk. [ENISA]
Safeguard(s)	Protective measures prescribed to meet the privacy (e.g., data quality, transparency of use of personal data) and security (e.g., confidentiality, integrity, and availability) requirements specified for an information system. Safeguards may include privacy and security features, management constraints, personal data minimization, use limitations for personal data, personnel security, and security of physical structures, areas, and devices. Synonymous with 'Security Controls' and 'Countermeasures.' [NIST Glossary, adapted]
Scoping	The act of applying scoping guidance, which consists of 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. [NIST Glossary, adapted from Scoping Guidance]
Scoping Considerations	A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/ environmental, public access, scalability, common control, and security objective. [NIST Glossary]
Security Assessment	See Security Control Assessment.
Security Control Assessment	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. [NIST Glossary]
Security Control Baseline	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) that provides a starting point for the tailoring process. [NIST Glossary]
Security Control(s)	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. [NIST Glossary, adapted]

Semi-Quantitative Assessment	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. [NIST Glossary]
Sensitive Information	Information where the loss, misuse, or unauthorized access or modification could adversely affect the [organization] or the conduct of [organizational] programs [or services], or the privacy to which individuals are entitled [by law]. [NIST Glossary, adapted]
Sensitivity	A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. [NIST Glossary]
Service	An act or activity performed on behalf of another party. [HITRUST]
Standard of Care	The degree of care or competence that one is expected to exercise in a particular circumstance or role. [FindLaw Dictionary]
Subcategory	See CSF Subcategory [NIST]
Tailored Overlay	See Enhanced Overlay.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See Tailoring. [NIST Glossary]
Tailoring	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. [NIST Glossary]
Target Profile	See CSF Target Profile [NIST]
Taxonomy	A system for classifying multifaceted, complex phenomena according to common conceptual domains and dimensions. [Bradley]
Third Party	An individual or organization that is recognized as being independent with respect to an issue, such as a service, or a function, such as a risk assessment or IT service delivery. [HITRUST]
Threat	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. [NIST Glossary, adapted]
Threat Actor	An individual or group posing a threat. [NIST Glossary]
Threat Assessment/Analysis	Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat. [NIST Glossary]
Threat Event	An event or situation that has the potential for causing undesirable consequences or impact. [NIST Glossary]
Threat Intelligence	Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes. [NIST Glossary]
Threat Scenario	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time. [NIST Glossary]

Threat Source	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability. [NIST Glossary].
Tier	See CSF Tier [NIST]
Total Risk	The potential for the occurrence of an adverse event if no mitigating action is taken (i.e., the potential for any applicable threat to exploit a system vulnerability). [NIST Glossary]
Variance	The state of being variable, different, divergent, or deviate; a degree of deviation. [English Encyclopedia]
Variance Reduction Control	A general class of control that involves actions taken to reduce the variability in the output of a process without affecting its intended purpose. [HITRUST]
Variation	A change in data, characteristic or function caused by one of four factors: special causes, common causes, tampering or structural variation. [ASQ Glossary}
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source. [NIST Glossary]
Vulnerability Assessment/ Analysis	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. [NIST Glossary]
Weakness	A particular part or quality of someone or something that is not good or effective (e.g., an error or defect). [Cambridge Dictionary, adapted]

Appendix B – Integrated Implementation Process

The following table consolidates the activities for all steps in the Integrated Cyber Resilience Framework (NIST Cybersecurity Framework / HITRUST Approach) implementation process.

Table 9. Integrated Implementation Activities by Step

Implementation Process Steps	Inputs	Activities	Outputs
Step 1: Prioritize and Scope	1. Risk management strategy 2. Organizational objectives and priorities 3. Asset inventory 4. HITRUST Approach	1. Organization determines where it wants to apply the Informative Reference(s) 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	1. Usage scope 2. Risk management strategy 3. HITRUST Approach	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	1. Organizational objectives 2. Risk management strategy 3. Detailed usage scope 4. Unique threats 5. HITRUST Approach	1. Organization selects one or more Informative References and creates a tailored overlay based on a risk analysis that considers the unique threats identified in the prioritization and scoping phase 2. Organization determines level of effectiveness or maturity desired in the selected controls	1. Target Profile (Tailored overlay of one or more Informative References) 2. Target Tier

Implementation Process Steps	Inputs	Activities	Outputs
Step 4: Conduct a Control Assessment	1. Detailed usage scope 2. Risk management strategy 3. Target Profile 4. HITRUST Approach	1. Perform a control assessment for in-scope systems and organizational elements	1. Control assessment reports
Step 5: Create a Current Profile	1. Assessment reports 2. HITRUST Approach	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 Cybersecurity Framework Tier model)
Step 6: Perform Gap Analysis	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. Control assessment 9. HITRUST Approach	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 (CAPs)
Step 7: Implement Action Plan	1. Prioritized implementation plan (CAPs) 2. HITRUST Approach	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

Appendix C – NIST Cybersecurity Framework Certification Report

A template for HITRUST's 'NIST Cybersecurity Framework Certification Report' begins on the next page.

NIST Cybersecurity Framework Certification Report

Org Name

Valid for the period
November 7, 2022 - November 7, 2024

HITRUST®

HITRUST

Contents

1. The NIST Cybersecurity Framework Scorecard

The NIST Cybersecurity Framework complements rather than replaces an organization's existing risk management process and cybersecurity program by providing an overarching set of guidelines to provide a minimal level of consistency as well as depth, breadth, and rigor of industry's cybersecurity programs, as shown in Figure 1.

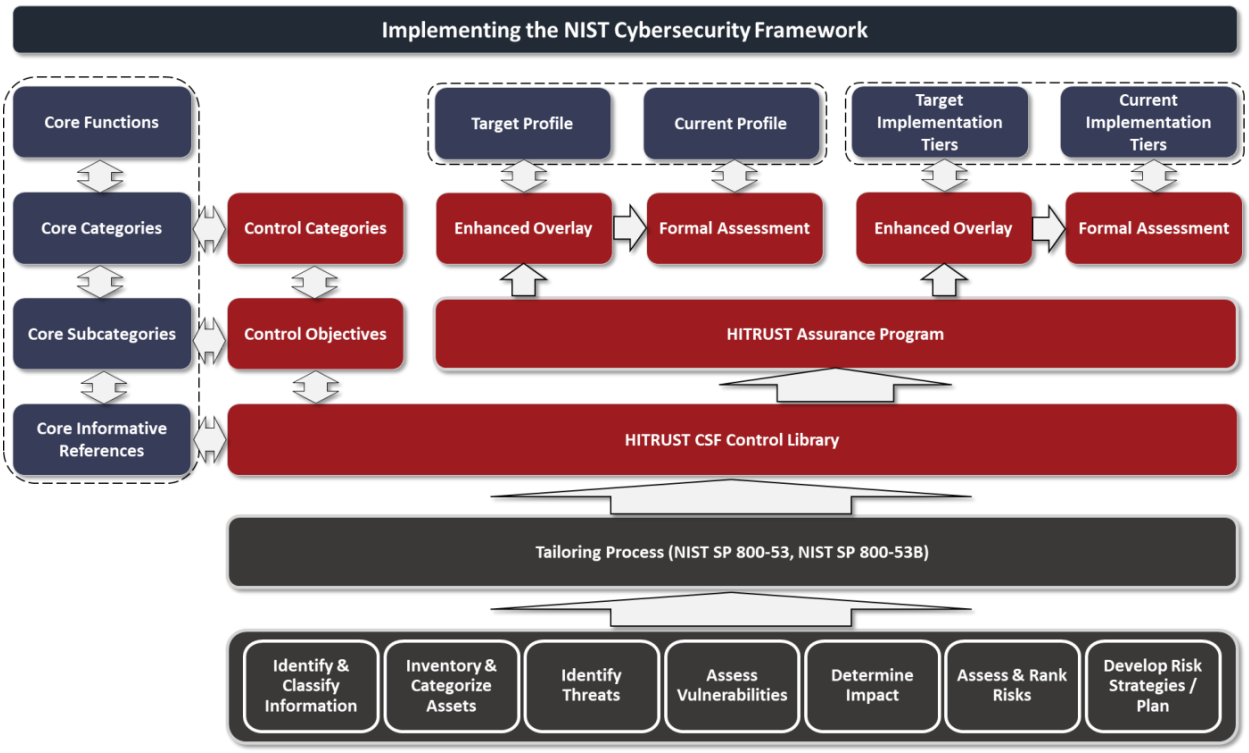


Figure 1. Implementing the NIST Cybersecurity Framework through the HITRUST CSF and CSF Assurance Program

The NIST Cybersecurity Framework Core is essentially a set of cybersecurity activities, desired outcomes, and applicable references that are common across government and industry. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across an organization from the executive level to the implementation/operations level, from one organization to another, and from one industry to another.

NIST Cybersecurity Framework Core Functions provide an incident response and recovery-oriented view of an organization's cybersecurity needs; the NIST Cybersecurity Framework Core Categories provide topical groupings of cybersecurity activities related to each of the Core Functions; and the NIST Cybersecurity Framework Core Subcategories provide the specific outcomes intended for each Core Category.

2. Letter of NIST Cybersecurity Framework Certification

Month Date, Year

Org Name
555 S Hoover Rd
Wichita, Kansas 67209-2349

Based on the results of a HITRUST® Risk-based, 2-year (r2) Validated Assessment performed by an Authorized External Assessor and documented in a HITRUST Risk-based, 2-year (r2) Validated Assessment Report ("Report"), the following platform, facility, and supporting infrastructure of the Organization ("Scope") is supported by an information protection program that is consistent with the objectives specified in the NIST Cybersecurity Framework v2:

Platform:

- Platform A residing at Data Center 1

Facility:

- Data Center 1 (Data Center) managed by Colo Provider A located in City, State, United States of America

More specifically, HITRUST determined that:

- The HITRUST CSF controls specified by the Entity's organizational, system and regulatory risk factors provide a fair representation of its Target Profile, and
- The maturity of the Entity's implemented HITRUST CSF controls, as validated by an Authorized External Assessor and reflected in the HITRUST Scorecard for the NIST Cybersecurity Framework, provide a fair representation of its Current Profile, and
- The aggregated maturity scores for each of the Core Categories meet HITRUST's criteria for certification of the Scope addressed by the assessment.

This certification is valid for as long as the Entity's associated HITRUST Risk-based, 2-year (r2) Certification remains valid but shall not exceed a period of two years from the date of this letter.

A full copy of the HITRUST Risk-based, 2-year (r2) Certification Report has been issued to the organization listed above. The full Report contains detailed information relating to the effectiveness of information protection controls as defined by the scoping factors selected by management. It also includes further details on the scope of the assessment, a representation letter from management, testing results, a benchmark report comparing the Organization's results to industry results, details on corrective action plans identified if applicable, and the

completed questionnaire. Such detailed information can best be leveraged by individuals/organizations who are familiar with and understand the services provided by the organization listed above. If interested in obtaining a copy of the full Report, you will need to contact the Organization directly. If there are questions on interpreting the detailed contents found in the full report, please refer to the document *Leveraging HITRUST Assessment Reports: A Guide for New Users* and can contact HITRUST customer support at *support@hitrustalliance.net.*

Additional information on the HITRUST Assurance Program used to support HITRUST's certification of the NIST Cybersecurity Framework can be found on the HITRUST website: *https://hitrustalliance.net.*

HITRUST

3. NIST Target and Current Profiles

The HITRUST CSF and HITRUST Assurance Program directly support an organization's implementation of the NIST Cybersecurity Framework by specifying the controls required for its Target Profile and the assessment methodology used to provide reliable assurances about its Current Profile. Figure 2 below depicts the Organization's Target Profile viewed through the lens of the HITRUST CSF control implementation levels and industry segments. The Target Profile specifies an industry acceptable level of due care for the protection of sensitive information as determined by its organizational, system and regulatory risk factors.

0 - ISMS	01 - Access Control																									02 - Human Resources Security									03 - Risk Management				04 - Security Policy	
00.a	01.a	01.b	01.c	01.d	01.e	01.f	01.g	01.h	01.i	01.j	01.k	01.l	01.m	01.n	01.o	01.p	01.q	01.r	01.s	01.t	01.u	01.v	01.w	01.x	01.y	02.a	02.b	02.c	02.d	02.e	02.f	02.g	02.h	02.i	03.a	03.b	03.c	03.d	04.a	04.b
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2				2	2		2	2	2	2	2	2	2	2			2	2	2	2	2	2	2	2	2	2	2		2	2	2	2	2		2
																3						3																		

05 - Organization of Information Security											06 - Compliance										07 - Asset Management					08 - Physical and Environmental Security												
05.a	05.b	05.c	05.d	05.e	05.f	05.g	05.h	05.i	05.j	05.k	06.a	06.b	06.c	06.d	06.e	06.f	06.g	06.h	06.i	06.j	07.a	07.b	07.c	07.d	07.e	08.a	08.b	08.c	08.d	08.e	08.f	08.g	08.h	08.i	08.j	08.k	08.l	08.m
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2		2	2	2	2	2	2		2	2	2	2	2			

09 - Communications and Operations Management																															
09.a	09.aa	09.ab	09.ac	09.ad	09.ae	09.af	09.b	09.c	09.d	09.e	09.f	09.g	09.h	09.i	09.j	09.k	09.l	09.m	09.n	09.o	09.p	09.q	09.r	09.s	09.t	09.u	09.v	09.w	09.x	09.y	09.z
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	2	2	2		2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2		2		2		2	2	2	2

10 - Information Systems Acquisition, Development, and Maintenance													11 - Information Security					12 - Business Continuity					13 - Privacy Practices																				
10.a	10.b	10.c	10.d	10.e	10.f	10.g	10.h	10.i	10.j	10.k	10.l	10.m	11.a	11.b	11.c	11.d	11.e	12.a	12.b	12.c	12.d	12.e	13.a	13.b	13.c	13.d	13.e	13.f	13.g	13.h	13.i	13.j	13.k	13.l	13.m	13.n	13.o	13.p	13.q	13.r	13.s	13.t	13.u
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	2		2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2			2						2	2		2								2

Denotes a control required for r2 certification

Figure 2. Target Profile - HITRUST CSF Controls

The Organization's Current Profile, depicted in Figure 3 below, is determined by the HITRUST Risk-based, 2-year (r2) Validated Assessment used to support HITRUST Risk-based, 2-year (r2) Certification, which is based on a purposive sample of 75 security controls contained in the HITRUST CSF framework. The sample ensures the assessment provides relying parties reasonable assurances about an organization's implementation of the HIPAA Security Rule standards and implementation specifications; AICPA Trust Services Criteria for Security, Confidentiality and Availability; and NIST Cybersecurity Framework Core Subcategories at a reasonable cost to the assessed organization.

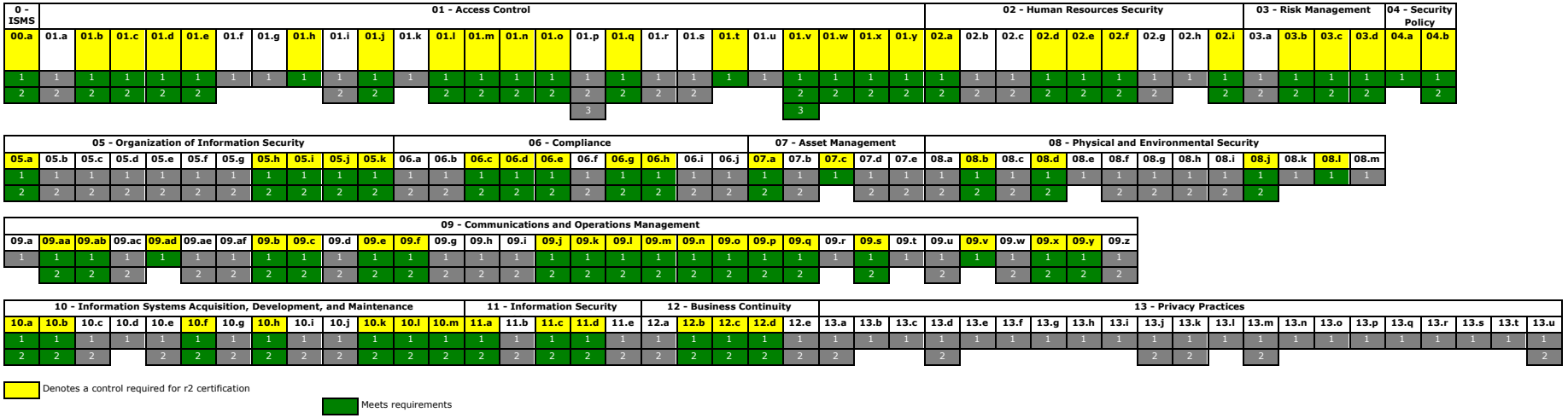


Figure 3. Current Profile - HITRUST CSF Controls (Purposive Sample)

Note more robust assurances, if needed, can be provided through a comprehensive assessment of all 135 HITRUST CSF security controls, as scoped by the Organization's risk factors.

4. HITRUST's NIST Cybersecurity Framework Scorecard

Although the Organization's Target and Current Profiles are expressed in terms of the HITRUST CSF controls, HITRUST certification of the Organization's NIST Cybersecurity Framework implementation is based on the NIST Cybersecurity Framework v2 Core and presented via HITRUST's NIST Cybersecurity Framework Scorecard. This Scorecard, presented in Figure 4 beginning on the next page, reflects the aggregated scores for the underlying HITRUST CSF controls as they are mapped by HITRUST to the NIST Cybersecurity Framework Core Subcategories. While HITRUST does its best to ensure the appropriate HITRUST CSF controls are mapped to each of the NIST Cybersecurity Framework v2 Subcategories, we make no representations around the suitability of the mappings as NIST might interpret them.

For more information on the HITRUST approach to assessment and certification, refer to the HITRUST Assessment Handbook, available from https://hitrustalliance.net/manual/.

More information about the controls framework-based approach to risk analysis and the HITRUST CSF as an industry overlay of the NIST SP 800-53 moderate-level baseline can be found in the Risk Management Handbook, available from https://cdn.manula.com/user/4996/docs/hitrust-risk-management-handbook-v1-0.pdf.

More information on how the HITRUST CSF is used to facilitate an organization's implementation of the NIST Cybersecurity Framework can be found in the HITRUST Approach to Cyber Resilience, available from https://23257256.fs1.hubspotusercontent-na1.net/hubfs/23257256/FY24%20-%20Q1%20-%20NIST%202.0%20Guidance/FY24%20-%20Q1%20-%20HITRUST%20Approach%20to%20Cyber%20Resilience%20-%20NIST%202.0%20Guidance.pdf.

Scorecard Color Legend

Requirements met (Avg. score of mapped HITRUST CSF requirements: 70-79.9)

Function	Status	Category	Status	Subcategory	Status
GOVERN (GV)		Govern: Organizational Context (GV.OC) (formerly ID.BE)		**GV.OC-01:** The organizational mission is understood and informs cybersecurity risk management (formerly ID.BE-02, ID.BE-03)	
				GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	
				GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed (formerly ID.GV-03)	
				GV.OC-04: Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated (formerly ID.BE-04, ID.BE-05)	
				GV.OC-05: Outcomes, capabilities, and services that the organization depends on are understood and communicated (formerly ID.BE-01, ID.BE-04)	
		Govern: Risk Management Strategy (GV.RM) (formerly ID.RM)		**GV.RM-01:** Risk management objectives are established and agreed to by organizational stakeholders (formerly ID.RM-01)	
				GV.RM-02: Risk appetite and risk tolerance statements are established, communicated, and maintained (formerly ID.RM-02, ID.RM-03)	
				GV.RM-03: Cybersecurity risk management activities and outcomes are included in enterprise risk management processes (formerly ID.GV-04)	
				GV.RM-04: Strategic direction that describes appropriate risk response options is established and communicated	
				GV.RM-05: Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties	
				GV.RM-06: A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated	
				GV.RM-07: Strategic opportunities (i.e., positive risks) are identified and included in organizational cybersecurity risk discussions	

Function	Status	Category	Status	Subcategory	Status
		Govern: Roles, Responsibilities, and Authorities (GV.RR) (formerly ID.GV-02)		**GV.RR-01:** Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving	
				GV.RR-02: Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced (formerly ID.AM-06, ID.GV-02, DE.DP-01)	
				GV.RR-03: Adequate resources are allocated commensurate with cybersecurity risk strategy, roles and responsibilities, and policies	
				GV.RR-04: Cybersecurity is included in human resources practices (formerly PR.IP-11)	
		Govern: Policy (GV.PO) (formerly ID.GV-01)		**GV.PO-01:** Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced (formerly ID.GV-01)	
				GV.PO-02: Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission (formerly ID.GV-01)	
		Govern: Oversight (GV.OV)		**GV.OV-01:** Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction	
				GV.OV-02: The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks	
				GV.OV-03: Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed	
				GV.SC-01: A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders (formerly ID.SC-01)	

Function	Status	Category	Status	Subcategory	Status
		Govern: Cybersecurity Supply Chain Risk Management (GV.SC) (formerly ID.SC)		**GV.SC-02:** Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally (formerly ID.AM-06)	
				GV.SC-03: Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes (formerly ID.SC-02)	
				GV.SC-04: Suppliers are known and prioritized by criticality	
				GV.SC-05: Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties (formerly ID.SC-03)	
				GV.SC-06: Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships	
				GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are identified, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship (formerly ID.SC-02, ID.SC-04)	
				GV.SC-08: Relevant suppliers and other third parties are included in incident planning, response, and recovery activities (formerly ID.SC-05)	
				GV.SC-09: Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle	
				GV.SC-10: Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement	

Function	Status	Category	Status	Subcategory	Status
IDENTIFY		Identify: Asset Management (ID.AM)		**ID.AM-01:** Inventories of hardware managed by the organization are maintained	
				ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	
				ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained (formerly ID.AM-03, DE.AE-01)	
				ID.AM-04: Inventories of services provided by suppliers are maintained	
				ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	
				ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	
				ID.AM-08: Systems, hardware, software, and services are managed throughout their life cycle (formerly PR.DS-03, PR.IP-02, PR.MA-01, PR.MA-02)	
		Identify: Risk Assessment (ID.RA)		**ID.RA-01:** Vulnerabilities in assets are identified, validated, and recorded (formerly ID.RA-01, PR.IP-12, DE.CM-08)	
				ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	
				ID.RA-03: Internal and external threats to the organization are identified and recorded	
				ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	
				ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk and inform risk prioritization	
				ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated (formerly ID.RA-06, RS.MI-03)	
				ID.RA-07: Changes and exceptions are managed, assessed for risk impact, recorded, and tracked (formerly part of PR.IP-03)	

Function	Status	Category	Status	Subcategory	Status
				ID.RA-08: Processes for receiving, analyzing, and responding to vulnerability disclosures are established (formerly RS.AN-05)	
				ID.RA-09: The authenticity and integrity of hardware and software are assessed prior to acquisition and use (formerly PR.DS-08)	
				ID.RA-10: Critical suppliers are assessed prior to acquisition	
		Identify: Improvement (ID.IM)		**ID.IM-01:** Improvements are identified from evaluations	
				ID.IM-02: Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties (formerly ID.SC-05, PR.IP-10, DE.DP-03)	
				ID.IM-03: Improvements are identified from execution of operational processes, procedures, and activities (formerly PR.IP-07, PR.IP-08, DE.DP-05, RS.IM-01, RS.IM-02, RC.IM-01, RC.IM- 02)	
				ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved (formerly PR.IP-09)	
PROTECT(PR)		**Protect: Identity Management and Access Control (PR.AA)** (formerly PR.AC)		**PR.AA-01:** Identities and credentials for authorized users, services, and hardware are managed by the organization (formerly PR.AC-01)	
				PR.AA-02: Identities are proofed and bound to credentials based on the context of interactions (formerly PR.AC-06)	
				PR.AA-03: Users, services, and hardware are authenticated (formerly PR.AC-03, PR.AC-07)	
				PR.AA-04: Identity assertions are protected, conveyed, and verified	
				PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties (formerly PR.AC-01, PR.AC-03, PR.AC-04)	

Function	Status	Category	Status	Subcategory	Status
				PR.AA-06: Physical access to assets is managed, monitored, and enforced commensurate with risk (formerly PR.AC-02, PR.PT-04)	
		Protect: Awareness and Training (PR.AT)		**PR.AT-01:** Personnel are provided awareness and training so they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind (formerly PR.AT-01, PR.AT-03, RS.CO-01)	
				PR.AT-02: Individuals in specialized roles are provided awareness and training so they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind (formerly PR.AT-02, PR.AT-03, PR.AT-04, PR.AT-05)	
		Protect: Data Security (PR.DS)		**PR.DS-01:** The confidentiality, integrity, and availability of data-at-rest are protected (formerly PR.DS-01, PR-DS.05, PR.DS-06, PR.PT-02)	
				PR.DS-02: The confidentiality, integrity, and availability of data-in-transit are protected (formerly PR.DS- 02, PR.DS-05)	
				PR.DS-10: The confidentiality, integrity, and availability of data-in-use are protected (formerly PR.DS-05)	
				PR.DS-11: Backups of data are created, protected, maintained, and tested (formerly PR.IP-04)	
		Protect: Platform Security (PR.PS)		**PR.PS-01:** Configuration management practices are established and applied (formerly PR.IP-01, PR.IP-03, PR.PT-02, PR.PT-03)	
				PR.PS-02: Software is maintained, replaced, and removed commensurate with risk (formerly PR.IP-12, PR.MA-02)	
				PR.PS-03: Hardware is maintained, replaced, and removed commensurate with risk (formerly PR.MA-01)	
				PR.PS-04: Log records are generated and made available for continuous monitoring (formerly PR.PT-01)	
				PR.PS-05: Installation and execution of unauthorized software are prevented	
				PR.PS-06: Secure software development practices are integrated and their performance is monitored throughout the software development life cycle	

Function	Status	Category	Status	Subcategory	Status
		Protect: Technology Infrastructure Resilience (PR.IR)		**PR.IR-01:** Networks and environments are protected from unauthorized logical access and usage (formerly PR.AC-03, PR.AC-05, PR.DS-07, PR.PT-04)	
				PR.IR-02: The organization's technology assets are protected from environmental threats (formerly PR.IP- 05)	
				PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations (formerly PR.PT-05)	
				PR.IR-04: Adequate resource capacity to ensure availability is maintained (formerly PR.DS-04)	
DETECT(DE)		**Detect: Continuous Monitoring (DE.CM)**		**DE.CM-01:** Networks and network services are monitored to find potentially adverse events (formerly DE.CM-01, DE.CM-04, DE.CM-05, DE.CM-07)	
				DE.CM-02: The physical environment is monitored to find potentially adverse events	
				DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events (formerly DE.CM-03, DE.CM-07)	
				DE.CM-06: External service provider activities and services are monitored to find potentially adverse events (formerly DE.CM-06, DE.CM-07)	
				DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events (formerly PR.DS-06, PR.DS-08, DE.CM-04, DE.CM-05, DE.CM-07)	
		Detect: Adverse Event Analysis (DE.AE) (formerly DE.AE, DE.DP-02)		**DE.AE-02:** Potentially adverse events are analyzed to better understand associated activities	
				DE.AE-03: Information is correlated from multiple sources	
				DE.AE-04: The estimated impact and scope of adverse events are determined	

Function	Status	Category	Status	Subcategory	Status
				DE.AE-06: Information on adverse events is provided to authorized staff and tools (formerly DE.DP-04)	
				DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	
				DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria (formerly DE.AE- 05)	
RESPOND(RS)		**Respond: Incident Management (RS.MA)** (formerly RS.RP)		**RS.MA-01:** The incident response plan is executed in coordination with relevant third parties once an incident is declared (formerly RS.RP-01, RS.CO-04)	
				RS.MA-02: Incident reports are triaged and validated (formerly RS.AN-01, RS.AN-02)	
				RS.MA-03: Incidents are categorized and prioritized (formerly RS.AN-04, RS.AN-02)	
				RS.MA-04: Incidents are escalated or elevated as needed (formerly RS.AN-02, RS.CO-04)	
				RS.MA-05: The criteria for initiating incident recovery are applied	
		Respond: Incident Analysis (RS.AN)		**RS.AN-03:** Analysis is performed to establish what has taken place during an incident and the root cause of the incident	
				RS.AN-06: Actions performed during an investigation are recorded and the records' integrity and provenance are preserved (formerly part of RS.AN-03)	
				RS.AN-07: Incident data and metadata are collected, and their integrity and provenance are preserved	
				RS.AN-08: An incident's magnitude is estimated and validated	
		Respond: Incident Response Reporting and Communication (RS.CO)		**RS.CO-02:** Internal and external stakeholders are notified of incidents	
				RS.CO-03: Information is shared with designated internal and external stakeholders (formerly RS.CO-03, RS.CO-05)	

Function	Status	Category	Status	Subcategory	Status
		Respond: Incident Mitigation (RS.MI)		**RS.MI-01:** Incidents are contained	
				RS.MI-02: Incidents are eradicated	
RECOVER (RC)		**Recover: Incident Recovery Plan Execution (RC.RP)**		**RC.RP-01:** The recovery portion of the incident response plan is executed once initiated from the incident response process	
				RC.RP-02: Recovery actions are selected, scoped, prioritized, and performed	
				RC.RP-03: The integrity of backups and other restoration assets is verified before using them for restoration	
				RC.RP-04: Critical mission functions and cybersecurity risk management are considered to establish post- incident operational norms	
				RC.RP-05: The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed	
				RC.RP-06: The end of incident recovery is declared based on criteria, and incident-related documentation is completed	
		Recover: Incident Recovery Communication (RC.CO)		**RC.CO-03:** Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders **RC.CO-04:** Public updates on incident recovery are shared using approved methods and messaging	

Figure 4. HITRUST Scorecard for the NIST Cybersecurity Framework

Appendix D – Bibliography

Bennekers, V. (Ed.) (2022). HITRUST Assessment Handbook. Available from https://hitrustalliance.net/manual/.

Blum, D. (2020). Rational Cybersecurity for Business: The Security Leader's Guide to Business Alignment. Silver Springs, MD: Apress. Available from https://learning.oreilly.com/library/view/rational-cybersecurity-for/9781484259528/html/Cover.xhtml.

Cascio, J. (2009, 28 Sep). The Next Big Thing: Resilience. Foreign Policy. Available from https://foreignpolicy.com/2009/09/28/the-next-big-thing-resilience/.

Cichonski, P., Millar, T., Grance, T., and Karen Scarfone, K. (2012, Aug). Computer Security Incident Handling Guide (NIST SP 800-61 r2). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Cline, B. (2014, Jun). 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.

Cline, B. (2017, Sep). Leveraging a Control-Based Framework to Simplify the Risk Analysis Process. ISSA Journal 15(9). Available from https://mydigitalpublication.com/publication/index.php?i=436950&m=0&l=&p=39&pre=.

Cline, B. (2021, Feb). HITRUST and HIPAA Safe Harbor: How the HITRUST Approach Meets the Requirements of Having Recognized Security Practices in Place. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/HITRUST-and-HIPAA-Safe-Harbor.pdf.

Cline, B. (2022a, Jul). HITRUST Approach to Quasi-Quantitative Residual Risk Analysis: Quantifying Risk in a Qualitative World. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/HITRUST-Approach-to-Quasi-Quantitative-Residual-Risk-Analysis-QQRRA.pdf.

Cline, B. (2022b, Jul). HITRUST TPRM Qualification Process: Methodology Guide: A proven six-step approach leveraging the HITRUST CSF framework and HITRUST Assurance Program to qualify a third party for a business relationship. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/HITRUST-Third-Party-Risk-Management-Methodology.pdf.

Cline, B. (2022, Oct). HITRUST TPRM Implementation Handbook: How organizations and TPRM software solution providers can ensure due diligence and due care when leveraging the six-step HITRUST TPRM Methodology (Ver. 1). Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/HITRUST-TPRM-Implementation-Handbook.pdf.

Cline, B. (2023a). HITRUST Risk Management Handbook: HITRUST CSF Control Maturity Model. HITRUST. Available from https://www.manula.com/manuals/hitrust/risk-management-handbook-exposure-draft/1/en/topic/hitrust-csf-control-maturity-model.

Cline, B. (2023b). HITRUST Risk Management Handbook: Step 3 – Implement and Manage Controls. HITRUST. Available from https://www.manula.com/manuals/hitrust/risk-management-handbook-exposure-draft/1/en/topic/hitrust-step-3-implement-and-manage-controls.

Cline, B. and Booker, R. (2023, Mar 8). Risk Analysis, Control Selection and Assurance with the Cybersecurity Framework Implementation Guide. HITRUST. Available from https://hitrustalliance.net/risk-analysis-control-selection-and-assurance-with-the-cybersecurity-framework-implementation-guide/.

CMS (2015). Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges, MARS-E Document Suite, Version 2.0. Baltimore, MD: Author. Available from https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf.

CMS (2017). CMS Acceptable Risk Safeguards (ARS) (CMS_CIO-STD-SEC01-3.0). Baltimore, MD: Author. Available from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-30-Publication.html.

DOE (2015, Jan). Energy Sector Cybersecurity Framework Implementation Guidance. Washington, DC: Author. Available from https://www.energy.gov/ceser/articles/energy-sector-cybersecurity-framework-implementation-guidance.

Exec. Order No. 13636, 3 Fed. Reg. 217 – 223 (2014). Available from https://www.govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf.

FedRAMP (2023). Understanding Baselines and Impact Levels for FedRAMP® Authorizations. Available from https://www.fedramp.gov/baselines/.

Fein, A., McMurrough, M., Cassidy, S., Harden, M., and Karbassi, S. (2023, Mar 6). White House Releases National Cybersecurity Strategy. Inside Privacy: Updates on developments in data privacy and cybersecurity. Available from https://www.insideprivacy.com/cybersecurity-2/white-house-releases-national-cybersecurity-strategy/.

Freund, J., and Jones, J. (2015). Measuring and Managing Information Risk: A FAIR Approach. Oxford: Elsevier, Inc.

HITRUST (2015, Nov 3). Health Industry Implementation of the NIST Cybersecurity Framework: A Collaborative Presentation by HHS, NIST, HITRUST, Deloitte and Seattle Children's Hospital (Webinar).

HITRUST (2019, Oct). HITRUST CSF® Assurance Program Requirements. Frisco, TX: Author. Available from https://hitrustalliance.net/content/uploads/CSF-Assurance-Program-Requirements.pdf.

HITRUST (2021). Building an Effective Third-Party Risk Management Program (Datasheet). Available from https://hitrustalliance.net/content/uploads/HITRUST-TPRM-Program-Datasheet.pdf.

HITRUST (2022, Feb). The Assurance Intelligence Engine™: How HITRUST Uses Automated Verification and Validation to Improve Rely-ability. Frisco, TX: Author. Available from https://hitrustalliance.net/content/uploads/The-Assurance-Intelligence-Engine.pdf.

HITRUST (2022a). HITRUST Shared Responsibility and Inheritance Program: Optimal Managed Risk Solutions for Sharing Information Security Control Assurances (Datasheet). Available from https://hitrustalliance.net/content/uploads/HITRUST-Shared-Responsibility-and-Inheritance-Program.pdf.

HITRUST (2022b). HITRUST Academy (Datasheet). Available from https://hitrustalliance.net/content/uploads/HITRUST-Academy-Overview.pdf.

HITRUST (2023a). HITRUST Approach. Available from https://hitrustalliance.net/the-hitrust-approach/.

HITRUST (2023b). HITRUST CSF Framework. Available from https://hitrustalliance.net/product-tool/hitrust-csf/.

HITRUST (2023c). HITRUST Threat Catalogue. Available from https://hitrustalliance.net/hitrust-threat-catalogue/.

HITRUST (2023d). HITRUST Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/.

HITRUST (2023e). Expanded HITRUST Assessment Portfolio. Available from https://hitrustalliance.net/expanded-hitrust-assessment-portfolio/.

HITRUST (2023f). MyCSF: Best in Class Information Risk Management Platform for Assessing and Reporting Information Risk and Compliance. Frisco, TX: Author. Available from https://hitrustalliance.net/content/uploads/HITRUST-MyCSF-Overview.pdf.

HITRUST (2023g). Third-Party Risk Management. Available from https://hitrustalliance.net/business/third-party-risk-management/.

HITRUST (2023h). HITRUST Shared Responsibility and Inheritance Program. Available from https://hitrustalliance.net/hitrust-srm-inheritance-program/.

HITRUST (2023i). HITRUST Results Distribution System. Available from https://hitrustalliance.net/results-distribution-system/.

HITRUST (2023j). HITRUST Certification of the NIST Cybersecurity Framework. Available from https://hitrustalliance.net/certification/nist-cybersecurity-framework-certification/.

HITRUST (2023k). HITRUST Risk-based, 2-Year (r2) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-risk-based-2-year-r2-validated-assessment/.

HPH SCC (2023). Home: Welcome to the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG). Available from https://healthsectorcouncil.org/.

HSCC CWG (2023, Mar). HPH Sector Cybersecurity Framework Implementation Guide, Version 2. Wash., DC: Author. Available from https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx.

Intraprise Health (2023). Security is a necessity, NOT a luxury. Available from https://intraprisehealth.com/security-is-a-necessity-not-a-luxury/.

IRS (2021, Nov). Tax Information Security Guidelines for Federal, State and Local Agencies (IRS Pub 1075, Revision 2021-11). Washington, DC: Author. Available from https://www.irs.gov/pub/irs-pdf/p1075.pdf.

Joint HPH CWG (2016, May). Healthcare Sector Cybersecurity Framework Implementation Guide, Version 1.1. Wash., DC: Author. Available from https://www.cisa.gov/sites/default/files/publications/HPH_Framework_Implementation_Guidance.pdf.

Joint Task Force, JTF (2020, Sep). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53), Revision 5. Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

Joint Task Force, JTF (2020, Oct). Control Baselines for Information Systems and Organizations (NIST SP 800-53B). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

Joint Task Force Transformation Initiative, JTF TI (2012, Sep). Guide for Conducting Risk Assessments (NIST SP 800-30 r1). Gaithersburg, MD: Author, p. H-3. Available from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

JTF TI (2013). Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 80-53 r4). Gaithersburg, MD: NIST, pp. D-1 – D-8. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Jordan, D. S. (1903, Apr). American University Tendencies, University Chronicle, University of California. [Stenographic report of an address delivered by David Starr Jordan, President of Stanford University, at the Charter Day exercises, March 23, 1903.] As cited in Quote Catalog (n.d.). David Starr Jordan. Available from https://quotecatalog.com/quote/david-starr-jordan-wisdom-is-knowi-P7vV6b7.

Kuhn, J. (1970). The Structure of Scientific Revolutions (2nd ed.). Chicago: University of Chicago Press. Available from https://www.lri.fr/~mbl/Stanford/CS477/papers/Kuhn-SSR-2ndEd.pdf.

Miller, L., and Gregory, P. (2012). CISSP for Dummies (4th ed.). New York: Wiley.

NIST (2004, Feb). Standards for Security Categorization of Federal Information and Information Systems (FIPS Pub 199). Gaithersburg, MD: Author. Available from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

NIST (2014, 12 Feb). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. Gaithersburg, MD: Author.

NIST (2015, Sep 30). Cybersecurity Framework FAQs Framework Components. Available from https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components#levels.

NIST (2018, 16 Apr). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Author. Available from https://doi.org/10.6028/NIST.CSWP.04162018.

NIST (2019, 12 Feb). NIST Marks Fifth Anniversary of Popular Cybersecurity Framework. Gaithersburg, MD: Author. Available from https://www.nist.gov/news-events/news/2019/02/nist-marks-fifth-anniversary-popular-cybersecurity-framework.

NIST (2023a). About NIST. Available from https://www.nist.gov/about-nist.

NIST (2023b). National Online Informative References Program. Available from https://csrc.nist.gov/projects/olir.

NIST (2023c). Informative References: What are they, and how are they used? Available from https://www.nist.gov/cyberframework/online-learning/informative-references.

NIST (2023d). Cybersecurity Framework Components: Framework Profiles. Available from https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components.

NIST (2023e). Glossary: Cyber Resiliency. Available from https://csrc.nist.gov/glossary/term/cyber_resiliency.

NIST (2023g). NIST Risk Management Framework. Available from https://csrc.nist.gov/projects/risk-management.

NIST (2024, 26 Feb). The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: Author. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

Nutkis, D., Mehta, R., and Grillo, R. (2016, Sep). The Healthcare Cyber Shift: From Prevention to Threat Detection and Response. Frisco, TX: HITRUST. Available from https://gtclawgroup.com/wp-content/uploads/2016/09/HealthcareCyberShift.pdf.

OASD (2021b). Government Coordinating Council. Available from https://www.phe.gov/Preparedness/planning/cip/HPH/Pages/Sector-Coordinating-Council.aspx.

Office of the Assistant Secretary for Preparedness and Response, OASD (2021a). Sector Coordinating Council. Available from https://www.phe.gov/Preparedness/planning/cip/HPH/Pages/Sector-Coordinating-Council.aspx.

Oxford Advanced Learner's Dictionary (2023). Resilience. Available from https://www.oxfordlearnersdictionaries.com/us/definition/english/resilience.

Random House Unabridged Dictionary (2023). Resilience. Available from https://www.dictionary.com/browse/resilient.

Rehabilitation Act, 29 U.S.C. § 798. Section 508 (1973). Available from https://www.govinfo.gov/app/details/COMPS-799.

Richards, D., Oliphant, A., and Le Grand, C. (2005, Mar). Global Technology Audit Guide: Information Technology Controls (GTAG 1). Altamonte

Springs, FL: The Institute of Internal Auditors. Available from https://pdf4pro.com/cdn/gtag-1-information-technology-controls-26aa03.pdf.

The Cybersecurity Enhancement Act, Pub. L. No. 113-274 (2014). Available from https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

The White House (2013, Feb 12). Presidential Policy Directive—Critical Infrastructure Security and Resilience (PPD-21). Washington, DC: Author. Available from https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf.

The White House (2023, 1 Mar). National Cybersecurity Strategy. Wash., DC: Author. Available from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Twain, M. (2901). Note to the Young People's Society, Greenpoint Presbyterian Church. Cited in Twain Quotes (n.d.). Directory of Mark Twain's maxims, quotations, and various opinions: Right. Available from http://www.twainquotes.com/Right.html.

Williams, C., Donaldson, S., and Siegal, S. (2020). Building an Effective Security Program. Boston: De Gruter.

Appendix E – Endnotes

[1] Jordan, D. S. (1903, Apr). American University Tendencies, University Chronicle, University of California, p. 4. [Stenographic report of an address delivered by David Starr Jordan, President of Stanford University, at the Charter Day exercises, March 23, 1903.] As cited in Quote Catalog (n.d.). David Starr Jordan. Available from https://quotecatalog.com/quote/david-starr-jordan-wisdom-is-knowi-P7vV6b7.

[2] Cline, B. (2014, Jun). 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.

[3] NIST (2023a). About NIST. Available from https://www.nist.gov/about-nist.

[4] NIST (2014, Feb 12). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0. Gaithersburg, MD: Author.

[5] The White House (2013, Feb 12). Presidential Policy Directive—Critical Infrastructure Security and Resilience (PPD-21). Washington, DC: Author pp. 2 – 4. Available from https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf.

[6] Office of the Assistant Secretary for Preparedness and Response, OASD (2021a). Sector Coordinating Council. Available from https://www.phe.gov/Preparedness/planning/cip/HPH/Pages/Sector-Coordinating-Council.aspx.

[7] OASD (2021b). Government Coordinating Council. Available from https://www.phe.gov/Preparedness/planning/cip/HPH/Pages/Sector-Coordinating-Council.aspx.

[8] Joint HPH CWG (2016, May). Healthcare Sector Cybersecurity Framework Implementation Guide, Version 1.1. Wash., DC: Author. Available from https://www.cisa.gov/sites/default/files/publications/HPH_Framework_Implementation_Guidance.pdf.

[9] Rehabilitation Act, 29 U.S.C. § 798. Section 508 (1973). Available from https://www.govinfo.gov/app/details/COMPS-799.

[10] HITRUST (2023a). HITRUST Approach. Available from https://hitrustalliance.net/the-hitrust-approach/.

[11] HSCC CWG (2023, Mar). HPH Sector Cybersecurity Framework Implementation Guide, Version 2. Wash., DC: Author. Available from https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx.

[12] HPH SCC (2023). Home: Welcome to the Healthcare and Public Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG). Available from https://healthsectorcouncil.org/.

[13] NIST (2018, Apr 16). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Author. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[14] NIST (2023b). National Online Informative References Program. Available from https://csrc.nist.gov/projects/olir.

[15] NIST (2023c). Informative References: What are they, and how are they used? Available from https://www.nist.gov/cyberframework/online-learning/informative-references.

[16] Joint Task Force, JTF (2020, Sep). Security and Privacy Controls for Information Systems and Organizations (NIST SP 800-53), Revision 5. Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[17] HITRUST (2023b). HITRUST CSF Framework. Available from https://hitrustalliance.net/product-tool/hitrust-csf/.

[18] Freund, J. and Jones, J. (2015). Measuring and Managing Information Risk: A FAIR Approach. Oxford: Elsevier, Inc.

[19] Cline, B. (2017, Sep). Leveraging a Control-Based Framework to Simplify the Risk Analysis Process. ISSA Journal 15(9), pp. 39 – 42. Available from https://mydigitalpublication.com/publication/index.php?i=436950&m=0&l=&p=39&pre=.

[20] NIST (2023d). Cybersecurity Framework Components: Framework Profiles. Available from https://www.nist.gov/cyberframework/online-learning/cybersecurity-framework-components.

[21] Cline, B. and Booker, R. (2023, Mar 8). Risk Analysis, Control Selection and Assurance with the Cybersecurity Framework Implementation Guide. HITRUST. Available from https://hitrustalliance.net/risk-analysis-control-selection-and-assurance-with-the-cybersecurity-framework-implementation-guide/.

[22] NIST (2018, Apr 16), p. 2.

[23] Cline, B. (2021, Feb). HITRUST and HIPAA Safe Harbor: How the HITRUST Approach Meets the Requirements of Having Recognized Security Practices in Place. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/HITRUST-and-HIPAA-Safe-Harbor.pdf.

[24] The White House (2023, 1 Mar). National Cybersecurity Strategy. Wash., DC: Author, p. 8. Available from https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[25] Fein, A., McMurrough, M., Cassidy, S., Harden, M., and Karbassi, S. (2023, Mar 6). White House Releases National Cybersecurity Strategy. Inside Privacy: Updates on developments in data privacy and cybersecurity. Available from https://www.insideprivacy.com/cybersecurity-2/white-house-releases-national-cybersecurity-strategy/.

[26] The White House (2023, 1 Mar), p. 2.

[27] Nutkis, D., Mehta, R., and Grillo, R. (2016, Sep). The Healthcare Cyber Shift: From Prevention to Threat Detection and Response. Frisco, TX: HITRUST, p. 2. Available from https://gtclawgroup.com/wp-content/uploads/2016/09/HealthcareCyberShift.pdf.

[28] Kuhn, J. (1970). The Structure of Scientific Revolutions (2nd ed.). Chicago: University of Chicago Press, p. 52. Available from https://www.lri.fr/~mbl/Stanford/CS477/papers/Kuhn-SSR-2ndEd.pdf.

[29] Nutkis, D., Mehta, R., and Grillo, R. (2016, Sep), p. 3.

[30] The White House (2013, Feb 12).

[31] Exec. Order No. 13636, 3 Fed. Reg. 217 – 223 (2014). Available from https://www.govinfo.gov/content/pkg/CFR-2014-title3-vol1/pdf/CFR-2014-title3-vol1-eo13636.pdf.

[32] The Cybersecurity Enhancement Act, Pub. L. No. 113-274 (2014). Available from https://www.congress.gov/bill/113th-congress/senate-bill/1353/text.

[33] Exec. Order No. 13636, 3 Fed. Reg. 217 – 223 (2014), p. 219.

[34] The White House (2023, 1 Mar), p. 8.

[35] Ibid.

[36] Ibid., p. 4.

[37] Ibid., pp. 19 – 21.

[38] Ibid., p. 4.

[39] Ibid., p. 5.

[40] Ibid., p. 8.

[41] Cascio, J. (2009, 28 Sep). The Next Big Thing: Resilience. Foreign Policy. Available from https://foreignpolicy.com/2009/09/28/the-next-big-thing-resilience/.

[42] Random House Unabridged Dictionary (2023). Resilience. Available from https://www.dictionary.com/browse/resilient.

[43] Oxford Advanced Learner's Dictionary (2023). Resilience. Available from https://www.oxfordlearnersdictionaries.com/us/definition/english/resilience.

[44] NIST (2023e). Glossary: Cyber Resiliency. Available from https://csrc.nist.gov/glossary/term/cyber_resiliency.

[45] Ibid.

[46] Cline, B. (2022a, Jul). HITRUST Approach to Quasi-Quantitative Residual Risk Analysis: Quantifying Risk in a Qualitative World. Frisco, TX: HITRUST, pp. 20-22. Available from https://hitrustalliance.net/content/uploads/HITRUST-Approach-to-Quasi-Quantitative-Residual-Risk-Analysis-QQRRA.pdf.

[47] Ibid.

[48] Ibid.

[49] Adapted from Cline, B. (2022a, Jul), p. 23.

[50] Miller, L., and Gregory, P. (2012). CISSP for Dummies (4th ed.). New York: Wiley.

[51] Freund, J. and Jones, J. (2015).

[52] Richards, D., Oliphant, A., and Le Grand, C. (2005, Mar). Global Technology Audit Guide: Information Technology Controls (GTAG 1). Altamonte

Springs, FL: The Institute of Internal Auditors. Available from https://pdf4pro.com/cdn/gtag-1-information-technology-controls-26aa03.pdf, p. 3.

[53] Freund, J. and Jones, J. (2015).

[54] Richards, D., Oliphant, A., and Le Grand, C. (2005, Mar), p. 4.

[55] Ibid.

[56] Williams, C., Donaldson, S., and Siegal, S. (2020). Building an Effective Security Program. Boston: De Gruter.

[57] Ibid.

[58] Kreitner, R. (1995). Management (6th ed.). New York: Houghton Mifflin College Division, p. 4.

[59] Cline, B. (2022, Jul), p. 22.

[60] NIST (2019, 12 Feb). NIST Marks Fifth Anniversary of Popular Cybersecurity Framework. Gaithersburg, MD: Author. Available from https://www.nist.gov/news-events/news/2019/02/nist-marks-fifth-anniversary-popular-cybersecurity-framework.

[61] NIST (2018, 16 Apr). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Author, p. 2. Available from https://doi.org/10.6028/NIST.CSWP.04162018.

[62] HITRUST (2015, Nov 3). Health Industry Implementation of the NIST Cybersecurity Framework: A Collaborative Presentation by HHS, NIST, HITRUST, Deloitte and Seattle Children's Hospital (Webinar), p10 [updated from the original].

[63] NIST (2024, 26 Feb). The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: Author. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[64] Ibid., p. 3.

[65] Ibid., pp. 3 – 4.

[66] Ibid., p. 4.

[67] Ibid.

[68] Ibid.

[69] Ibid., p. 9.

[70] Ibid.

[71] Ibid., p. 6.

[72] Ibid., p. 7.

[73] Ibid, p. 24.

[74] Ibid., pp. 24 – 25.

[75] NIST (2015, Sep 30). Cybersecurity Framework FAQs Framework Components. Available from https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-components#levels.

[76] NIST (2024, Feb 26), p. 7.

[77] Ibid., p. 8.

[78] Ibid., p. 3.

[79] Ibid., pp. 3 – 4.

[80] Cline, B. (2022a, Jul), pp. 21 – 22.

[81] Blum, D. (2020). Rational Cybersecurity for Business: The Security Leader's Guide to Business Alignment. Silver Springs, MD: Apress., Figure 1. Available from https://learning.oreilly.com/library/view/rational-cybersecurity-for/9781484259528/html/Cover.xhtml.

[82] Intraprise Health (2023). Security is a necessity, NOT a luxury. Available from https://intraprisehealth.com/security-is-a-necessity-not-a-luxury/.

[83] HITRUST (2023a).

[84] Cline, B. (2017, Sep).

[85] NIST (2023g). NIST Risk Management Framework. Available from https://csrc.nist.gov/projects/risk-management.

[86] NIST (2004, Feb). Standards for Security Categorization of Federal Information and Information Systems (FIPS Pub 199). Gaithersburg, MD: Author, p. 2. Available from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[87] Joint Task Force, JTF (2020, Oct). Control Baselines for Information Systems and Organizations (NIST SP 800-53B). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf.

[88] Cline, B. (2017, Sep), p. 41.

[89] CMS (2017). CMS Acceptable Risk Safeguards (ARS) (CMS_CIO-STD-SEC01-3.0). Baltimore, MD: Author. Available from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-30-Publication.html.

[90] CMS (2015). Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges, MARS-E Document Suite, Version 2.0. Baltimore, MD: Author. Available from https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf.

[91] IRS (2021, Nov). Tax Information Security Guidelines for Federal, State and Local Agencies (IRS Pub 1075, Revision 2021-11). Washington, DC: Author. Available from https://www.irs.gov/pub/irs-pdf/p1075.pdf.

[92] FedRAMP (2023). Understanding Baselines and Impact Levels for FedRAMP® Authorizations. Available from https://www.fedramp.gov/baselines/.

[93] Cline, B. (2022b, Jul). HITRUST TPRM Qualification Process: Methodology Guide: A proven six-step approach leveraging the HITRUST CSF framework and HITRUST Assurance Program to qualify a third party for a business relationship. Frisco, TX: HITRUST, pp. 16 – 17. Available from https://hitrustalliance.net/content/uploads/HITRUST-Third-Party-Risk-Management-Methodology.pdf.

[94] HITRUST (2023c). HITRUST Threat Catalogue. Available from https://hitrustalliance.net/hitrust-threat-catalogue/.

[95] HITRUST (2023d). HITRUST Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/.

[96] Cline, B. (2022a, Jul), pp. 11-12, 29.

[97] HITRUST (2023e). Expanded HITRUST Assessment Portfolio. Available from https://hitrustalliance.net/expanded-hitrust-assessment-portfolio/.

[98] Cline, B. (2022b, Jul), pp. 21 – 26.

[99] Bennekers, V. (Ed.) (2022). HITRUST Assessment Handbook. Available from https://hitrustalliance.net/manual/.

[100] HITRUST (2019, Oct). HITRUST CSF® Assurance Program Requirements. Frisco, TX: Author, pp. 7 – 8. Available from https://hitrustalliance.net/content/uploads/CSF-Assurance-Program-Requirements.pdf.

[101] Cline, B. (2023a). HITRUST Risk Management Handbook: HITRUST CSF Control Maturity Model. HITRUST. Available from https://hitrustalliance.net/manual-risk-management/1.0/en/topic/executive-summary.

[102] HITRUST (2022, Feb). The Assurance Intelligence Engine™: How HITRUST Uses Automated Verification and Validation to Improve Rely-ability. Frisco, TX: Author, pp. 8 – 9. Available from https://hitrustalliance.net/content/uploads/The-Assurance-Intelligence-Engine.pdf.

[103] Cline, B. (2022, Oct). HITRUST TPRM Implementation Handbook: How organizations and TPRM software solution providers can ensure due diligence and due care when leveraging the six-step HITRUST TPRM Methodology (Ver. 1). Frisco, TX: HITRUST. Available from https://hitrustalliance.net/content/uploads/HITRUST-TPRM-Implementation-Handbook.pdf.

[104] HITRUST (2019, Oct), p. 6.

[105] HITRUST (2023f). MyCSF: Best in Class Information Risk Management Platform for Assessing and Reporting Information Risk and Compliance. Frisco, TX: Author. Available from https://hitrustalliance.net/content/uploads/HITRUST-MyCSF-Overview.pdf.

[106] HITRUST (2023g). Third-Party Risk Management. Available from https://hitrustalliance.net/business/third-party-risk-management/.

[107] HITRUST (2021). Building an Effective Third-Party Risk Management Program (Datasheet). Available from https://hitrustalliance.net/content/uploads/HITRUST-TPRM-Program-Datasheet.pdf.

[108] HITRUST (2023h). HITRUST Shared Responsibility and Inheritance Program. Available from https://hitrustalliance.net/hitrust-srm-inheritance-program/.

[109] HITRUST (2022a). HITRUST Shared Responsibility and Inheritance Program: Optimal Managed Risk Solutions for Sharing Information Security Control Assurances (Datasheet). Available from https://hitrustalliance.net/content/uploads/HITRUST-Shared-Responsibility-and-Inheritance-Program.pdf.

[110] HITRUST (2023i). HITRUST Results Distribution System. Available from https://hitrustalliance.net/results-distribution-system/.

[111] HITRUST (2022b). HITRUST Academy (Datasheet). Available from https://hitrustalliance.net/content/uploads/HITRUST-Academy-Overview.pdf.

[112] Twain, M. (2901). Note to the Young People's Society, Greenpoint Presbyterian Church. Cited in Twain Quotes (n.d.). Directory of Mark Twain's maxims, quotations, and various opinions: Right. Available from http://www.twainquotes.com/Right.html.

[113] Cichonski, P., Millar, T., Grance, T., and Karen Scarfone, K. (2012, Aug). Computer Security Incident Handling Guide (NIST SP 800-61 r2). Gaithersburg, MD: NIST, p. 21. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

[114] NIST (2024, Feb 26), pp. 6 – 7.

[115] NIST (2018, Aug 16), pp. 14 – 15.

[116] HSCC CWG (2023, Mar), p. 8.

[117] NIST (2024, Feb 26), p. 6.

[118] NIST (2018, Aug 16), p. 14.

[119] Adapted from Department of Energy (2015, Jan). Energy Sector Cybersecurity Framework Implementation Guidance. Washington, DC: Author. Available from https://www.energy.gov/ceser/articles/energy-sector-cybersecurity-framework-implementation-guidance.

[120] For example, see The White House (2023, 1 Mar).

[121] Cline, B. (2023b). HITRUST Risk Management Handbook: Step 3 – Implement and Manage Controls. HITRUST. Available from https://hitrustalliance.net/manual-risk-management/1.0/en/topic/hitrust-step-3-implement-and-manage-controls.

[122] Cline, B. (2023c). Risk Management Handbook: Appendix A1 – Alternate Controls. HITRUST. Available from https://hitrustalliance.net/manual-risk-management/1.0/en/topic/a-1-alternate-controls.

[123] HITRUST (2023e).

[124] HITRUST (2023k). HITRUST Risk-based, 2-Year (r2) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-risk-based-2-year-r2-validated-assessment/.

[125] HITRUST (2023j). HITRUST Certification of the NIST Cybersecurity Framework. Available from https://hitrustalliance.net/certification/nist-cybersecurity-framework-certification/.

[126] Cline, B. (2022b, Jul), pp. 16 – 17.

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

[128] Joint Task Force Transformation Initiative, JTF TI (2012, Sep). Guide for Conducting Risk Assessments (NIST SP 800-30 r1). Gaithersburg, MD: Author, p. H-3. Available from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.