HITRUST®

HITRUST Third-Party Risk Management (TPRM) Methodology: The Qualification Process

A streamlined approach to qualifying a third party for a business relationship leveraging the HITRUST CSF and CSF Assurance Program

October 2019

Executive Summary

HITRUST®, since 2007, has been championing and delivering solutions to address the lack of a common understanding around the security and privacy controls needed to safeguard sensitive information and individual privacy. These solutions include:

1. An industry accepted information security and privacy control framework, the HITRUST CSF®, that incorporates multiple regulatory requirements and best practice standards and frameworks;
2. A standard, open and transparent assessment process to provide accurate, consistent and repeatable assurances around the level of protection provided by an organization; and
3. An industry recognized certification of an organization's conformity to the protection requirements specified in the HITRUST CSF through the HITRUST CSF Assurance™ Program.

However, there is currently no common or consistent approach to determining what information risk assurances should be provided and maintained when an organization shares sensitive information with a third party. This creates inefficiencies when organizations seek greater assurances from their third parties than are warranted (based on risk or regulatory compliance requirements) or when organizations do not seek enough assurances and expose themselves to more risk than intended (based on their tolerance or capacity to accept risk).

The HITRUST Third-Party Risk Management (TPRM) Qualification Methodology provides such an approach.

This whitepaper focuses on the HITRUST TPRM Qualification Methodology—a process organizations undertake to qualify or re-qualify third parties for a specific business relationship by obtaining assurances appropriate to the information security, privacy and compliance risk[1] they inherently pose to the organization.

More specifically, we discuss:

- The information needed to help organizations triage third parties based on the inherent risk they pose,
- A standardized approach to triaging third parties based on specific inherent risk factors and selecting an assessment that provides a level of assurance appropriate to the risk,
- The various risk assessments available, including a targeted, 'pre-qualifying' HITRUST CSF Rapid Assessment that addresses high-risk, high-interest and foundational security controls, and how they can be leveraged in an iterative assurance process,
- A HITRUST CSF Trust Score™ that helps improve the reliability of self-assessments used in the iterative assurance process and supports an organization's evaluation of the overall trustworthiness of a third party,
- Gap analysis based on a comparison of a third-party's current and target security profiles, and the creation and prioritization of corrective action plans (CAPs),
- The evaluation and reporting of risk based on control maturity and relative impact of a control failure, and
- Formal risk acceptance by management based on the risk target(s) provided by the third-party's target profile and the residual risk indicated by its current security profile.

The HITRUST TPRM Qualification Methodology is a potential 'game-changer' for any organization that wants to address the inconsistencies, inefficiencies, ineffectiveness and high costs of their current approach to TPRM and third-party assurance and provides a 'win-win' for organizations and third parties alike.

Table of Contents

Table of Contents

List of Figures

Table of Contents

List of Tables

Introduction

HITRUST champions and delivers solutions to address the lack of a common understanding around the security and privacy controls needed to demonstrate an appropriate level of due diligence[2] and due care[3] for the protection of sensitive information,[4,5] such as personal data,[6] as well as a common mechanism for providing assurances[7] for both internal and external stakeholders around the state of an organization's information risk[8] management[9] and compliance[10] program.

While HITRUST offers multiple means of providing industry various levels of assurance—such as with a HITRUST CSF Readiness Assessment or Validated Assessment against some or all of the HITRUST CSF control requirements applicable to an organization—there is currently no common methodology or approach to identifying the means and rigor with which such assurances should be provided and maintained.

This document outlines HITRUST's TPRM Qualification Methodology, which provides a common approach that can be used across industries for efficient and effective third-party risk management.

Third-Party Risk Management

Third parties,[11] such as vendors, suppliers and business partners, can introduce significant business risk to an organization simply due to the type and amount of sensitive information shared and how they process[12] and potentially share this information amongst themselves.

1. Data breaches are increasingly being attributed to security failures in an organization's supply chain.[13]
2. The 'flow down' of contractual requirements to downstream organizations in the supply chain is necessary but insufficient for adequate due care or diligence.[14]
3. The provision of satisfactory assurances through audit or assessment can often be a legal or regulatory requirement, depending on the type and nature of the data.[15]
4. An organization's brand and reputation may still be affected by a breach in its supply chain.[16]
5. Organizations may still be held accountable by customers and upstream partners for the failure of downstream third parties to protect the data they receive.[17]

Many organizations subsequently go to great lengths to manage their third-party risk, often through a formal management process such as the generic model shown in Figure 1 below.

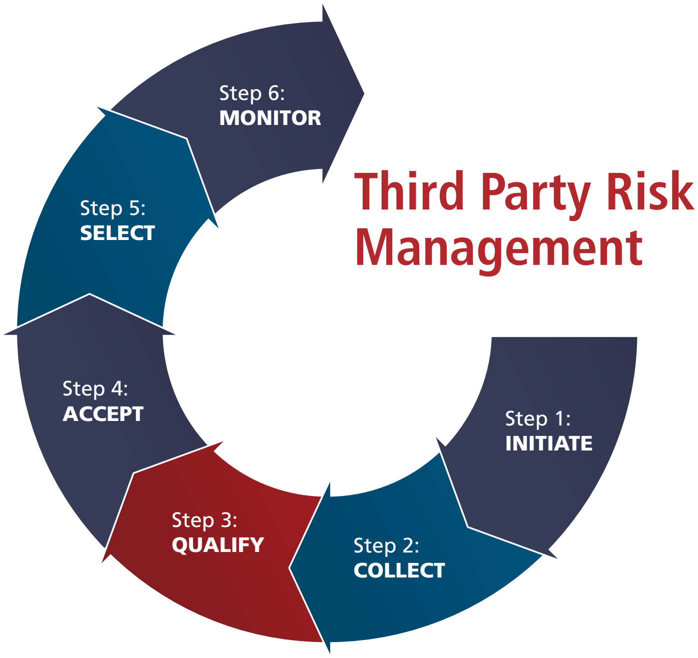


Figure 1. Generic Third-Party Risk Management Process Model

While the actual implementation of TPRM varies from one organization to another, they will typically address each step of the process in some way.

- Step 1 – **Initiate**. Prior to contract award or as part of a routine or special reassessment (e.g., annually or after a material change in the relationship, respectively), formally initiate the TPRM process and, if necessary, request information from internal departments or external stakeholders.
- Step 2 – **Collect**. Gather proposals, contracts and other documentation about the third party and the products, services, etc., the third party provides or will provide, including documentation received from the third party (e.g., a short questionnaire about their business practices) and then route to the SMEs within the organization for review.
- Step 3 – **Qualify**. Evaluate the information about the third party and the products, services, etc., the third party provides or will provide and assess the level of risk they pose to the organization.
- Step 4 – **Accept**. Formally accept or decline to accept the level of risk posed to the organization should they enter or continue a formal relationship (i.e., for the products, services, etc., provided). Note that failure to accept the risk should result in dropping the third party from consideration in a competitive bid or canceling/modifying the contract or other agreement if a current relationship exists.
- Step 5 – **Select**. If entering into a new relationship via competitive selection, select the appropriate third party, execute all necessary legal contracts, and complete other onboarding activities; if an existing relationship, make any changes needed in legal contracts or other documentation to reflect any changes in the third-party relationship (e.g., the amount of data the third party receives or how it is processed).
- Step 6 – **Monitor**. Continuously monitor the third party for changes in potential business risk, including information security, privacy and compliance risk.

The organization should re-enter Step 1– Initiate to review existing third-party relationships and determine if there have been any material changes in the relationship, e.g., in the amount of data to which they have access or how they process the information. The Initiate stage may be entered periodically (e.g., annually) or aperiodically when a specific condition or trigger is encountered (e.g., the third party reports a breach).

This paper focuses on a subset, specific of TPRM Step 3 – Qualify, which is the process an organization uses to vet or 'qualify' a third party's information security and privacy risk and compliance programs and determines if the risk associated with the business relationship falls within acceptable levels; incorporates HITRUST's prior discussion of the Risk Triage Methodology (RTM); and will continue to expand discussion of third-party assurance to include the entire qualification process—and eventually the entire TPRM process—over time.

The TPRM Qualification Process

Step 3 of the TPRM process outlined above—Qualify—is dedicated to qualifying a third party for a business relationship by evaluating information about a third party and the products, services, etc., it provides or will provide an organization as well as assessing the level of risk it poses to the organization given the information it processes or will process. The result is a level of assurance—essentially a measure of confidence or trust—that a third party will provide an appropriate level of due diligence and due care for the protection of sensitive information and individual privacy. Such assurances can take many forms, such as an attestation of conformity, or some type of conformity assessment, such as a controls gap assessment against a security standard.

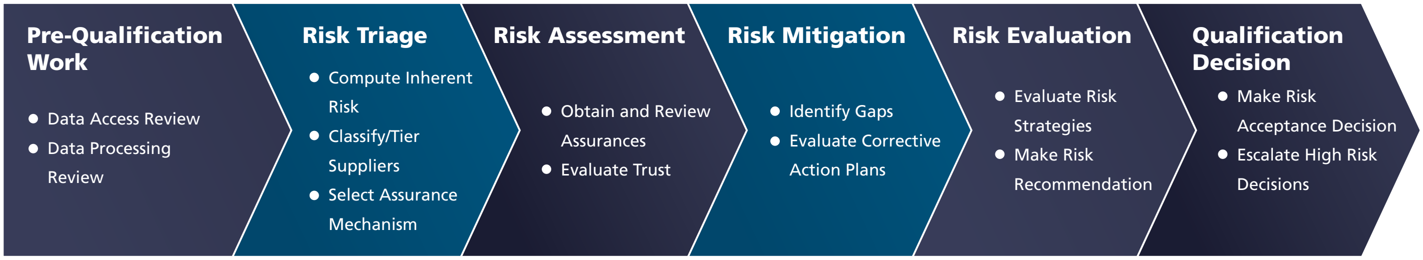


Figure 2. Generic Third-Party Qualification Process

The qualification process depicted in Figure 2 above consists of six basic steps:

1. Pre-Qualification Work (PQW) – Data access is reviewed based on the information gathered in the prior step in the TPRM process model;
2. Risk Triage (RT) – The third party is classified or tiered according to the level of inherent risk it presents based on specific risk factors;
3. Risk Assessment (RA) – Assurances around the level of residual risk the third party poses to the organization based on an attestation or assessment of conformity to an organization-defined security and privacy standard are obtained and reviewed;
4. Risk Mitigation (RM) – Any gaps in conformity are evaluated along with the third party's corrective action plans (CAPs) to address those gaps, if any;
5. Risk Acceptance (RA) – The remaining or residual risk is evaluated; and
6. Qualification Decision (QD) – Management determines if the organization is willing to accept that risk based on its general risk appetite[18] and specific risk tolerances."[19]

Qualify Step 1 – Pre-Qualification Work

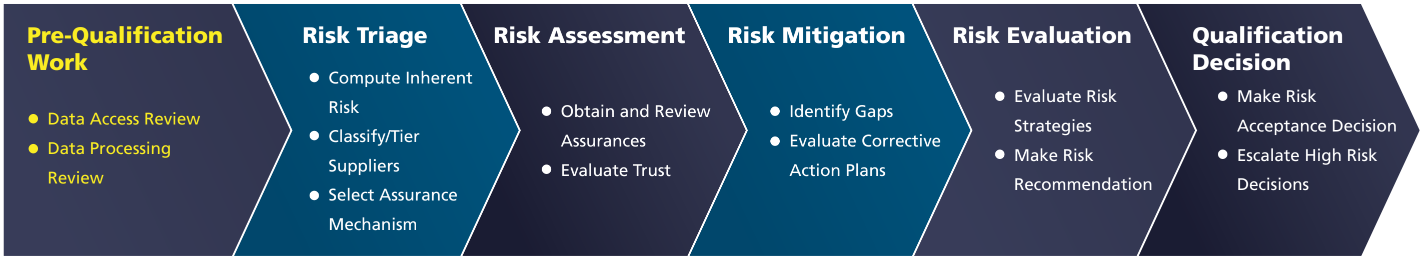


Figure 3. Qualify Step 1 – Pre-Qualification Work

PQW builds upon the TPRM Collection Process (TPRM Step 2 – Collect) as shown previously in Figure 1, during which the organization gathers and reviews proposals, contracts and other documentation about the third party and the products, services, etc., the third party provides or will provide, including documentation received from the third party (e.g., a short questionnaire about their business practices). However, the PQW is focused on identifying the organization's information that is or will be provided to—and processed by—a third party and is subsequently supported by two types of reviews: one focused on data access and the other focused on how the data will be processed.

Types of Review

Data Access Review

The data access review is focused on identifying the type of information that is or will be accessed and how it will or may be accessed. Sources that can help answer these questions include but are not limited to:

- Data Inventories
- Process Flows
- Contracting & Procurement Records
- Subject Matter Expert (SME) Interviews
- Access Reviews
- Third-party Questionnaires

Data Process Review

The data process review is focused on identifying how information is or may be processed by the third party. Sources that can help answer these questions include but are not limited to:

- Process Flows
- Contracting & Procurement Records
- SME Interviews
- Third-party Questionnaires

Sources of Information

While there are various sources of information that may be available to an organization to perform these reviews, the goal is to leverage as much information as needed to address each of the risk factors used in the next step in the TPRM Qualification Process (TPRM Step 3 – Qualify). For more information on these factors, refer to Qualify Step 2 – Risk Triage and/or Appendix A – Risk Triage Inherent Risk Factor Ratings.

Potential sources of information identified above are described in more detail below.

Data Inventory

One of the first steps when qualifying a third party for a business relationship is to determine the specific information for which it has or will be provided access. Subsequently, any hope of providing an accurate accounting of a third party's information access rests on an accurate data inventory.

A data inventory is defined as "a list of datasets[20] with meta data[21] that describes their contents, source, licensing and other useful information … that can help users understand why data has been collected, what it contains, how it is managed and the ways it will be made available for others to use."[22,23] The types of meta data collected about a dataset may include but are not limited to:

- Data owner (e.g., a specific business unit manager)
- Data custodian (e.g., a specific employee)
- Data type (e.g., personal data)
- Data sensitivity (e.g., high/medium/low)
- Data location (e.g., system name)
- Data subjects (e.g., employees)
- Data source (e.g., data subject; employment check)
- Data scope (e.g., all employee data)
- Data format (e.g., electronic, '.dbs' format)
- Data purpose (e.g., human resources management)
- Data processors (e.g., company A, company B)

Process Flows

Although a data inventory provides needed information on the type of data to which a third-party may be given access, it may not address how that access may be obtained nor how the information may be processed. Process flows, including data flows and workflows, can help provide the additional context needed to answer these questions.

A data flow diagram (DFD) can be helpful as it shows how information is processed in one or more information systems[24] and can help one understand the business processes the system(s) support. "When it comes to conveying how … data flows through systems (and how that data is transformed in the process), [DFDs] are the method of choice over technical descriptions for three principal reasons:

1. DFDs are easier to understand by technical and nontechnical audiences,

2. DFDs can provide a high-level system overview, complete with boundaries and connections to other systems, and

3. DFDs can provide a detailed representation of system components."[25]

While there are several types of DFDs, a good DFD will also show how information is accessed and by whom, as can be seen in Figure 4[26] below.

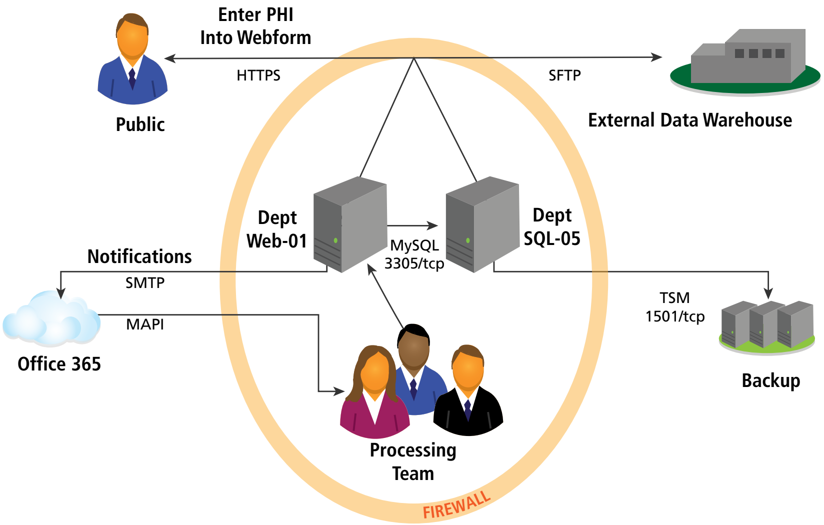


Figure 4. Example of a DFD Showing Data Access

Workflows[27] are also useful as they provide a graphical visualization of the actual work performed by the organization in support of a specific product or service, and they may also include information on who may potentially have access to the information used in the process as shown in Figure 5[28] below for logistics management.

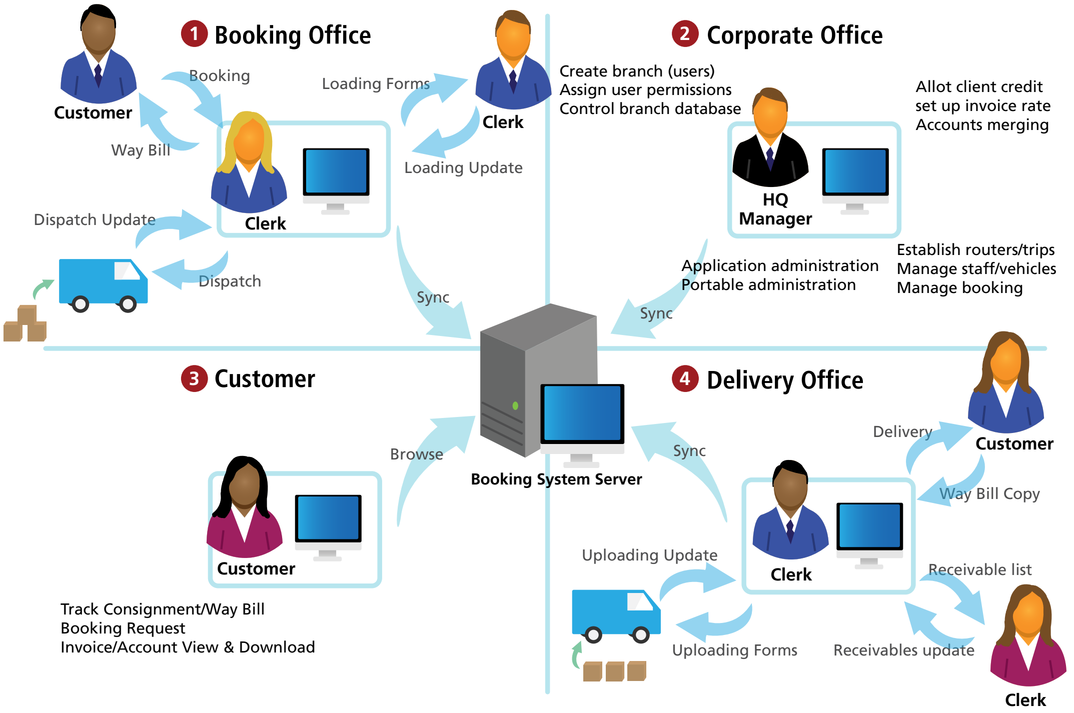


Figure 5. Example Workflow Diagram Showing Data Access

Contracting & Procurement Records

Both requests for proposal (RFPs) and third-party responses to RFPs can provide information about proposed business relationships, while contracts and other agreements such as data use or processing agreements can provide information about existing business relationships. These documents may also provide a good source of DFDs and workflow diagrams specific to the existing or proposed business relationship under review.

This is especially true if the proposals require the information needed by the data access review in the third party's response and if the contracts and other agreements also require the production of this information. For example, the HITRUST CSF requires third-party agreements to provide a description of the product or service to be provided, and a description of the information to be made available along with its level of sensitivity.

SME Interviews

Documentation often tends to become stale over time. Interviews with relevant SMEs in the information technology (IT) department and relevant business units can help ensure the information obtained from existing documentation is both current and relevant to an existing or proposed third-party relationship. Examples of the types of SMEs one should consider interviewing are network, system and application administrators; system and business analysts; system and enterprise architects; and managers from relevant business units, contracting and procurement, among others. The interviews should focus on verifying relevant information obtained from other sources and addressing the risk factors used in support of the Risk Triage Process (Qualify Step 2 – Risk Triage).

Access Reviews

Access reviews are conducted periodically by management to ensure user access rights and privileges are appropriate to a user's current job role and 'need-to-know.' For existing business processes that are not yet outsourced, these reviews will help indicate what data is accessed and how it is accessed for specific job functions/tasks, which can be used to make inferences about how a potential third party might do the same. For existing business processes that are currently outsourced but for which a new third party may become involved, it can provide specific information about the new third party's access needs.

Third-party Questionnaires

Third-party questionnaires should be used sparingly and focus specifically on obtaining information regarding the risk factors used in the TPRM Risk Triage Process (Qualify Step 2 – Risk Triage) that is not available from other sources. HITRUST provides an Inherent Risk Questionnaire (IRQ) that specifically addresses the inherent risk factors used in the next step of the HITRUST TPRM Qualification Process, Qualify Step 2 – Risk Triage. For example, the IRQ asks about a third-party's intent to outsource to a subcontractor or utilize cloud services and, if so, the type of outsourcing or cloud services it would use to deliver the product or services they provide or would provide to the organization.

Summary

The intent of PQW is to provide the information needed to address the risk factors used in the Risk Triage Process (Qualify Step 2 – Risk Triage). Subsequently, the organization must ensure TPRM Collection Process (TPRM Step 2 – Collect) addresses, at a minimum, these specific factors.

Relevant sources of information are many and varied and include, but are not limited to, data inventories, process flows, contracting and procurement records, SME interviews, user access reviews and third-party questionnaires.

Once the requisite information about a third party is obtained and reviewed by the appropriate SMEs for completeness and accuracy in the TPRM Collection Process (TPRM Step 2 – Collect), it is then made available to the TPRM team for review.

Qualify Step 2 – Risk Triage

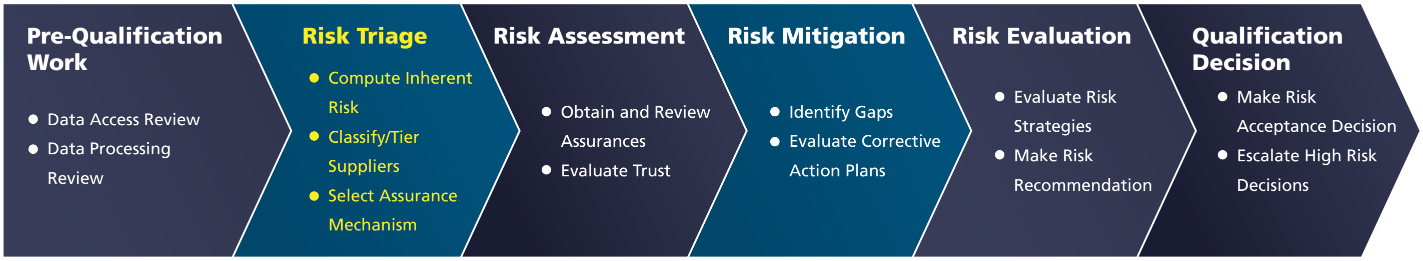

Pre-Qualification Work
● Data Access Review
● Data Processing Review
Risk Triage
● Compute Inherent Risk
● Classify/Tier Suppliers
● Select Assurance Mechanism
Risk Assessment
● Obtain and Review Assurances
● Evaluate Trust
Risk Mitigation
● Identify Gaps
● Evaluate Corrective Action Plans
Risk Evaluation
● Evaluate Risk Strategies
● Make Risk Recommendation
Qualification Decision
● Make Risk Acceptance Decision
● Escalate High Risk Decisions

Figure 6. Qualify Step 2 – Risk Triage

In general, we understand triage to mean "the assigning of priority order to projects on the basis of where funds and other resources can be best used, are most needed, or are most likely to achieve success."[29] In the context of managing risk from third parties, we interpret risk triage as the assignment of priority order and/or specific types of assurance mechanisms based on inherent risk[30] to ensure the organization's risk appetite and/or specific risk tolerances for sharing sensitive information with third parties are adequately addressed.

We must necessarily triage third parties based on the inherit risk posed to the organization by simply sharing information, as the extent to which these third parties can adequately protect this information would not be known until the appropriate assurance mechanism is selected and adequate assurances are obtained.

More specifically, this level of inherent risk must be determined based on a limited amount of readily available information if the process is to be efficient as well as effective. By this we mean information that we already know or can easily become known, such as researching public information or simply requesting information directly from the third-party. However, the latter is not meant to imply an attempt to gain information about the state of key controls using an extensive or otherwise exhaustive data protection questionnaire or similar approach, as the selection of a specific assurance mechanism is the end goal of the risk triage process.

Risk triage involves classifying or tiering a third party according to the level of risk it presents in a proposed or existing business relationship, and includes:

(i) Inherent risk factors,

(ii) A scoring model based on those factors, and

(iii) Specific recommendations for the type and rigor of assurance based on those scores.

Risk Factors

The key to differentiating inherent risk between and amongst various third parties is to identify a set of common factors that will provide a reasonable and meaningful categorization of inherent risk.

> *Risk models define the risk factors to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk factors are also used extensively in risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts. Typical risk factors include threat, vulnerability, impact, likelihood, and* ***predisposing condition****.*[31]

A predisposing condition is one that "exists within an organization, … which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, [or] other organizations."[32] We interpret this to mean that a predisposing condition may influence the probable impact should an event occur; however, we also believe the same can be said for the likelihood an event will occur. For example—given the general lack of visibility and control an organization has in certain public cloud environments—data hosted in these environments may be more likely to be compromised than data hosted by the organization on its premises.

HITRUST, through the HITRUST CSF and CSF Assurance programs, already leverages this concept of predisposing conditions as risk factors to help categorize the relative risk within and between organizations, their architecture/technology, and their legislative, regulatory and contractual requirements to create a more tailored enumeration of HITRUST CSF controls for each type of entity as defined by their respective factors.

We take a similar approach with third-party risk triage and define three types of inherent risk factors for third-party risk triage: organizational, compliance and technical. However, one should note that the risk factors selected by HITRUST are not absolute. Organizations are free to adjust these inherent risk factors based on their risk appetite and tolerances[33] and/or select other inherent risk factors they believe provide reasonable estimators for likelihood and impact in the risk triage model.

Organizational Factors

Organizational factors are attributes of the data provided to a third party and are essentially related to the value of the data. Although these factors could influence likelihood due to threat actor motivation, we believe these attributes are more indicative of the probable impact in the event of a compromise, especially if the data is of one type or is otherwise of uniform value (e.g., ePHI[34] or cardholder data[35] in particular and PII[36] or personal data[37] in general). Our rationale is based on numerous sources that cite the cost of a data breach based on an average cost per individual record.[38]

Specific organizational factors addressed by the HITRUST Risk Triage Qualification Methodology include but are not necessarily limited to:

(i) The percentage of organizational data shared with a third party;

(ii) The total amount of data such as the number of individual records; and

(iii) The criticality of the business relationship to the organization.

Compliance Factors

Compliance factors are associated with fines and other penalties that a regulatory body could levy on an organization due to a breach caused by a third party, subsequently influencing the probable impact of a data compromise. Regulatory oversight, however, can have limited practical impact on the likelihood of a data breach, even in such highly regulated industries like healthcare,[39] and impact is subsequently not considered in the HITRUST model for these factors.

Specific compliance[40] factors for the organization addressed by the HITRUST Risk Triage Methodology include but are not necessarily limited to:

(i) The comprehensiveness and specificity of an applicable regulation or a mandatory standard's protection requirements;

(ii) The specific assurance requirements of applicable regulations and mandatory standards;

(iii) The penalties specified in the regulations/mandatory standards or otherwise seen in practice; and

(iv) The level of enforcement provided by the regulatory or standards bodies.

Technical Factors

Technical factors relate to how a third party accesses, processes, stores and disposes of the data provided by the organization and influence the likelihood data will be compromised; however, these are situational and do not address the controls specified for use in these situations. For example, the organization has less control as well as less visibility of the protections afforded its data when processed off-site, in the cloud or by a subcontractor rather than managed on premises by organization staff. Or an organization could be averse to the use of subcontractors to process sensitive data on behalf of the organization. While the location could influence the likelihood of a compromise, we note the processing location may have little, if any, influence on probable impact should a breach occur.

Specific technical factors addressed by the HITRUST Risk Triage Methodology, include but are not necessarily, limited to:

(i) The data processing environments used by a third party;

(ii) The type of cloud environment, if one is used by a third party;

(iii) The mechanism used by a third party to access the organization's data;

(iv) The location of data stored by a third party; and

(v) The use of subcontractors by a third party.

Triaging Risk

Table *1* below lists each of these factors, grouped by risk component and factor type, along with recommended values for each factor based on a five-point quasi-quantitative scale.

Table 1. Triage Risk Factors by Factor Type and Associated Ratings/Scores

Risk Component	Risk Factor Type	Risk Factor	Risk Factor Ratings					Risk Factor Type Score	Risk Comp. Score
			Very Low (0)	Low (1)	Medium (2)	High (3)	Very High (4)		
Impact	Organizational	IO1: Percentage of organizational data	≤ 20%	20 – 40%	40 – 60%	60 – 80%	> 80%	Simple Average	High Watermark
		IO2: Total amount of organizational data	N/A	≤ 1M Records	1M - 10M Records	10M - 60M Records	> 60M Records		
		IO3: Criticality of the business relationship	Minimal	Low	Moderate	High	Critical		
	Compliance[41]	IC1: Comprehensive-ness and specificity of requirements	None	General, Non-specific	General Framework-based Req'ts[42] [43]	Prescriptive Framework-based Req'ts [44]	N/A	Simple Average	
		IC2: Level of assurance required	None	Self-Assessment/ Attestation	Risk-based (Determined by the Org.)	Specific Reporting Format[45]	Specific Ctrl Requirement Framework[46]		
		IC3: Specified or observed lines and penalties	Insignificant	Minor	Moderate	Significant	Catastrophic		
		IC4: Level of enforcement	None	Inconsistent or Ad Hoc	Reactive	Proactive	Aggressive		
Likelihood	Technical	LT1: Data processing environment	On-premise	N/A	Hosted (IaaS)	Cloud (PaaS)	Cloud (SaaS)	Simple Average	
		LT2: Type of cloud environment, if used	N/A	N/A	Private	Hybrid	Public		
		LT3: Data access approach	Onsite (Supervised)	Onsite (Unsupervised)	Offsite (No Remote Access)	Remote Access (Individual)	Remote Access (Group)		
		LT4: Data Storage location	None	Onsite (Controlled)	Onsite (Uncontrolled)	Off Site (Single Location)	Offsite (Multiple Locations)		
		LT5: Use of subcontractors	None	N/A	One-level Subcontractor	N/A	Multiple or Not Specified		

For more information, see Appendix A – Risk Triage Inherent Risk Factor Ratings.

Computing Inherent Risk

As shown in Table *1* on the previous page, HITRUST recommends computing a simple average for each risk factor type: organizational, compliance, and technical. However, we recommend taking a high watermark approach for the impact score as both organizational and compliance risk are significant enough on their own to warrant a high-level of assurance. The likelihood score is trivial, as it is identical to the technical factor.

Although we recommend a simple average, organizations may wish to compute a weighted average for a factor type if one or more risk factors are of particular concern. For example, an organization may be (risk) averse to placing sensitive information in the public cloud and weight the type of cloud environment used by a third party more heavily.

EXAMPLE: Vendor A

An example of Factor Type and Risk Component Scores computed from the Risk Factor Ratings in the model is provided in Table *2*.

Table 2. Example Factor and Risk Component Calculations (Vendor A)

Risk Component	Risk Factor Type	Risk Factor	Risk Factor Rating	Risk Factor Type Score	Risk Comp. Score
Impact	Organizational	IO1: Percentage of organizational data	1	2.0	2.5
		IO2: Total amount of organizational data	2		
		IO3: Criticality of the business relationship	3		
	Compliance	IC1: Comprehensiveness and specificity of requirements	2	2.5	
		IC2: Level of assurance required	2		
		IC3: Specified or observed fines and penalties	3		
		IC4: Level of enforcement	3		
Likelihood	Technical	LT1: Data processing environment	4	1.8	
		LT2: Type of cloud environment, if used	2		
		LT3: Data access approach	0		
		LT4: Data storage location	1		
		LT5: Use of subcontractors	2		

Factor Ratings were selected from Table *1* and averages—the Factor Type Score—were computed for each Factor Type. The Organizational Factor Type Score, for example, was computed as (1 + 2 + 3)/3 = 2.0. The Risk Component Score for Impact is simply the high watermark (i.e., the highest) value of the Organizational and Compliance Risk Factor Type Scores of 2.0 and 2.5, respectively, which is 2.5. The Risk Component Score for Likelihood is simply the Technical Factor Type Score of 1.8. Now that the Risk Component Scores for Impact and Likelihood are computed, these values can be plotted on a heat map as shown in Figure 7 below.

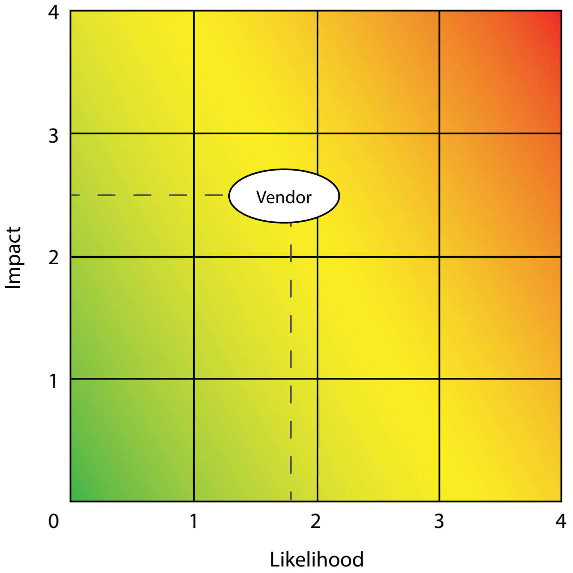


Figure 7. Example Heatmap (Vendor A)

The inherent risk posed by a third-party can also be calculated as follows:

$$Inherent\ Risk = ROUND(UP)\left[\frac{Likelihood\ x\ Impact}{4}\right]$$

By rounding up the raw risk score, one can then determine one of the five HITRUST-recommended assurance approaches, as shown in Table *3*.

Table 3. HITRUST-recommended Assurance Approaches[47]

Inherent Risk	Assurance Approach
0 – Very Low	HITRUST CSF Readiness Assessment[48] w/[49] No Minimum Score and CAPs[50] Not Required
1 – Low	HITRUST CSF Validated Assessment with No Minimum Score[51] and CAPs Allowed
2 – Moderate	HITRUST CSF Validated Assessment > 62 w/ CAPs Allowed
3 – High	HITRUST CSF Validated Assessment ≥ 71 w/ No CAPs Allowed
4 – Very High	HITRUST CSF Validated Assessment ≥ 87 w/ CAPs Allowed

EXAMPLE: Vendor A

$$
\begin{aligned}
\mathit{Inherent\ Risk} &= \mathit{ROUND(UP)}\left[\frac{\mathit{Likelihood\ x\ Impact}}{4}\right]\\
&= \mathit{ROUND(UP)}\left[\frac{1.8\ x\ 2.5}{4}\right]\\
&= \mathit{ROUND(UP)}\,[1.125]\\
&= 2
\end{aligned}
$$

In this example, Vendor A would be asked to obtain a HITRUST CSF validated assessment and obtain a minimum score of 62 (out of 100) with corrective action plans (CAPs). With a limited number of CAPs, the organization could become HITRUST CSF certified as well.

Summary

Risk triage involves classifying or tiering a third party according to the level of inherent risk it presents in a proposed or existing business relationship.

Table 4. Consolidated View of the HITRUST TPRM Risk Triage Approach

Risk Component	Risk Factor Type	Risk Factor	Risk Factor Rating	Risk Factor Type Score	Risk Comp. Score	Risk Score	Assessment Type (Based on Risk Score)
Impact	Organizational	IO1: Percentage of organizational data	0 – 4	Simple Average 0 – 4	High Watermark 0 – 4	Simple Average (Rounded UP to the Next Highest Integer) 0 – 4	0 – HITRUST CSF Readiness Assessment w/ No Minimum Score and CAPs Not Required 1 – HITRUST CSF Validated Assessment w/ No Minimum Score and CAPs Allowed 2 – HITRUST CSF Validated Assessment w/ a Consolidated Score > 62 and CAPs Allowed 3 – HITRUST CSF Validated Assessment w/ a Consolidated Score > 71 and No CAPs Allowed 4 – HITRUST CSF Validated Assessment w/ a Consolidated Score > 87 and CAPs Allowed
		IO2: Total amount of organizational data	0 – 4				
		IO3: Criticality of the business relationship	0 – 4				
	Compliance	IC1: Comprehensiveness and specificity of requirements	0 – 4	Simple Average 0 – 4			
		IC2: Level of assurance required	0 – 4				
		IC3: Specified or observed fines and penalties	0 – 4				
		IC4: Level of enforcement	0 – 4				
Likelihood	Technical	LT1: Data processing environment	0 – 4	Simple Average 0 – 4			
		LT2: Type of Cloud environment, if used	0 – 4				
		LT3: Data access approach	0 – 4				
		LT4: Data storage location	0 – 4				
		LT5: Use of subcontractors	0 – 4				

As shown in Table *4* above, the HITRUST risk triage approach provides:

1. Specific organizational, compliance and technical factors that help identify the type and amount of inherent risk the business relationship with the vendor poses;
2. A simple risk scoring model to help quantify the risk; and

3. Specific recommendations for the type and rigor of the assessment and the maturity of the organization's information protection.

By providing a common set of risk factors independent of the security and privacy controls that may or may not be implemented by a third party, an organization can readily assess inherent risk and determine a reasonable and appropriate mechanism for the assurances it needs at a reasonable cost. Broad adoption will also significantly reduce costs for any third party that needs to provide assurances to multiple customers or business partners.

Qualify Step 3 – Risk Assessment

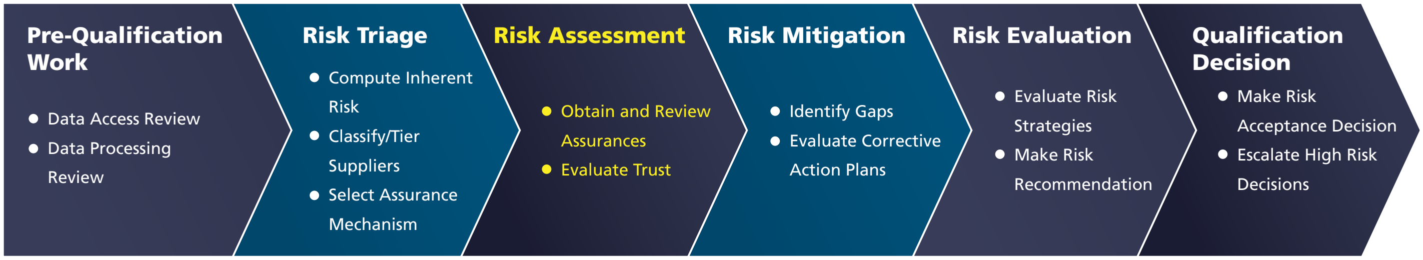

Pre-Qualification Work
● Data Access Review
● Data Processing Review
Risk Triage
● Compute Inherent Risk
● Classify/Tier Suppliers
● Select Assurance Mechanism
Risk Assessment
● Obtain and Review Assurances
● Evaluate Trust
Risk Mitigation
● Identify Gaps
● Evaluate Corrective Action Plans
Risk Evaluation
● Evaluate Risk Strategies
● Make Risk Recommendation
Qualification Decision
● Make Risk Acceptance Decision
● Escalate High Risk Decisions

Figure 8. Qualify Step 3 – Risk Assessment

After the appropriate assurance mechanism is selected in the Risk Triage Process (Qualify Step 2 – Risk Assessment), the organization notifies the third-party and establishes a timeline for compliance, assists and/or monitors the third party until the appropriate assurances are provided, and then reviews the assurances for accuracy and completeness.

Obtaining Assurance

The organization must notify the third party of the type and level of assurance required, which includes but is not necessarily limited to:

- HITRUST CSF Readiness Assessment with no minimum score and CAPs not required
- HITRUST CSF Validated Assessment with no minimum score and CAPs allowed
- HITRUST CSF Validated Assessment with a consolidated score > 62 and CAPs allowed
- HITRUST CSF Validated Assessment with a consolidated score > 71 and no CAPs allowed
- HITRUST CSF Validated Assessment with a consolidated score > 87 and CAPs allowed

Organizations are free to append requirements to the specified assurances (e.g., minimum scores for specific HITRUST CSF Categories, Objectives, Controls or Control Requirements)[52] to address organizational risk tolerances for specific activities (e.g., outsourcing) or areas of concern (e.g., access control).

Scope / Applicability

To ensure the assessment specified by the risk triage model provides the appropriate level of assurance, one of the first things the organization must do is work with the third party to ensure applicable organizational and system elements are included in the assessment. This includes specification of the physical and logical systems used by a third party that support the workflow(s) for the product(s) and/or service(s) being or to be provided the organization, as well as the logical interfaces to the systems included in the assessment scope. Note proper network segmentation will help ensure systems that are not part of the applicable workflow are excluded from the assessment scope.

HITRUST provides specific guidance[53] on how an assessment's scope should be documented via a Scope Overview, Scope Description and Scope Diagram.

Scope Overview

The Scope Overview is designed to communicate in summary form what system(s) and process(es) were assessed as well as the components they are made of and the market-facing products and/or service lines they support. It will also communicate if the environment was assessed as a whole and what portions of the environment may have been excluded if partially assessed. Exclusions are only acceptable when there is a clear delineation. An example might be a portal that allows organizations to present content: the portal might be included but the content could be excluded.

Table *5* below provides an example of a Scope Overview for the systems and associated services considered 'in scope', including exclusions from that scope.

Table 5. Example of a Scope Overview

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
Chinstrap Portal	UNIX Oracle DB v8.1 Java .Net VMWare v7.9	Penguin Nest		🟡	🔴	Content and the underlying applications that provide it for delivery through Penguin Nest by customers were not assessed as part of this report.
		Penguin Analytics	🟢			N/A
		South Pole Benefit Eligibility	🟢			N/A

Scope Description

The scope description is a verbose discussion of the system(s) and process(es) that were assessed for the report. It should be written with as much detail about the system(s) and process(es) as possible and include descriptions of the service offering(s) and/or product(s) that they support. Items to include in the scope description would include component parts, internal vs. external development, connectivity, interfaces, and high-level network or architecture diagram.

The following is an example of a Scope Description based on the prior example for the Scope Overview.

Systems

The system that was assessed for this report is Chinstrap Portal ("Portal"). The Portal is a platform that allows numerous applications and service offerings to be accessed via a single web-based interface via a browser. It does this for numerous customers and allows their customers to obtain information in a single location. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net, runs on a HP-UX platform, and is supported by an Oracle database. The solution leverages VMWare for scalability. The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility. Penguin Nest is an application that delivers content and applications from customer systems via the Portal. This assessment only includes the Portal code that comprises Penguin Nest interface. Applications and content delivered by customers via Penguin Nest were not assessed as they are owned and managed by customers. This exclusion includes the mechanisms for connectivity. Penguin Analytics is an application that delivers reporting and analytics capability to customers. It allows them to develop dashboards and reports and track KPIs with their information that is stored within the Portal. South Pole Benefits Eligibility allows our customers to provide benefit eligibility information so that users of the system have a single place to go to get the eligibility information from multiple customers.

Facilities

The Portal is hosted in both the South Pole and North Pole data centers. Both locations are in scope for this report as well as the corporate headquarters located in Antarctica. Branch location personnel are not involved in development or maintenance of the Portal, so this report excludes all branch offices.

Scope Diagram

The Scope Diagram is essentially a high-level DFD, as discussed earlier for PQW (Qualify Step 1 – Pre-Qualification Work), an example for which is provided Figure 9 in below.

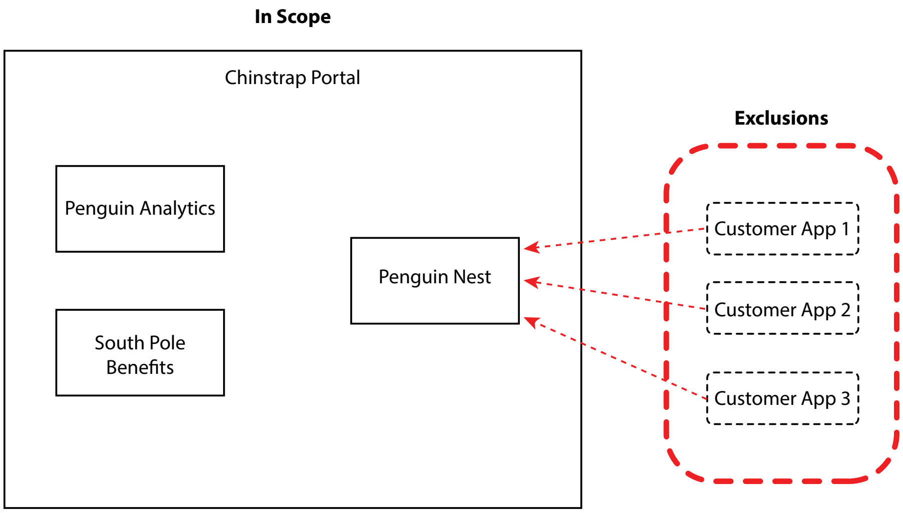


Figure 9. Example of a Scope Diagram

Note scoping a HITRUST CSF assessment is similar to the process used by U.S. government organizations establishing a security perimeter or authorization/accreditation boundary,[54] and those familiar with the process can apply the same principles when scoping a HITRUST CSF assessment.

Control Specifications

Once scoping is complete, organizations should then work with the third party to ensure an appropriate set of security and privacy controls is specified for the assessment. Fortunately, the process is relatively straightforward due to how the HITRUST CSF is built.

By leveraging the same control framework-based approach to risk analysis[55] used by U.S. government organizations and following the National Institute of Standards and Technology (NIST) tailoring[56] process, HITRUST integrated and harmonized multiple information security and privacy regulations, standards and best practice frameworks—referred to as authoritative sources—to create the CSF as an industry-level overlay[57] of the NIST moderate-level initial security control baseline,[58] as shown in Figure 10 below.

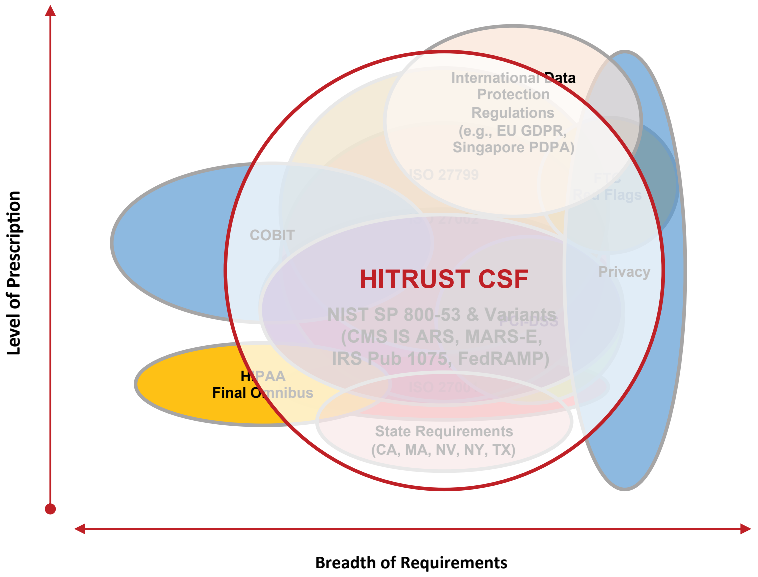

Level of Prescription
International Data Protection Regulations (e.g., EU GDPR, Singapore PDPA)
ISO 27799
FTC Red Flags
ISO 27002
COBIT
HITRUST CSF
Privacy
NIST SP 800-53 & Variants (CMS IS ARS, MARS-E, IRS Pub 1075, FedRAMP)
PCI-DSS
HIPAA Final Omnibus
ISO 27001
State Requirements (CA, MA, NV, NY, TX)
Breadth of Requirements

Figure 10. The HITRUST CSF – A Highly Tailored, Industry-level Control Framework Overlay

The control requirements in the overlay were then organized along the lines of the security control clauses contained in ISO/IEC 27001 – Appendix A with slight modifications, such as the addition of three new families of controls: CSF Control Category 0 – Information Security Management Program, CSF Control Category 3 – Risk Management Program, and CSF Control Category 13 – Privacy Practices. A high-level depiction of the HITRUST CSF Control Categories and Supporting Control Objectives is provided in Figure 11.

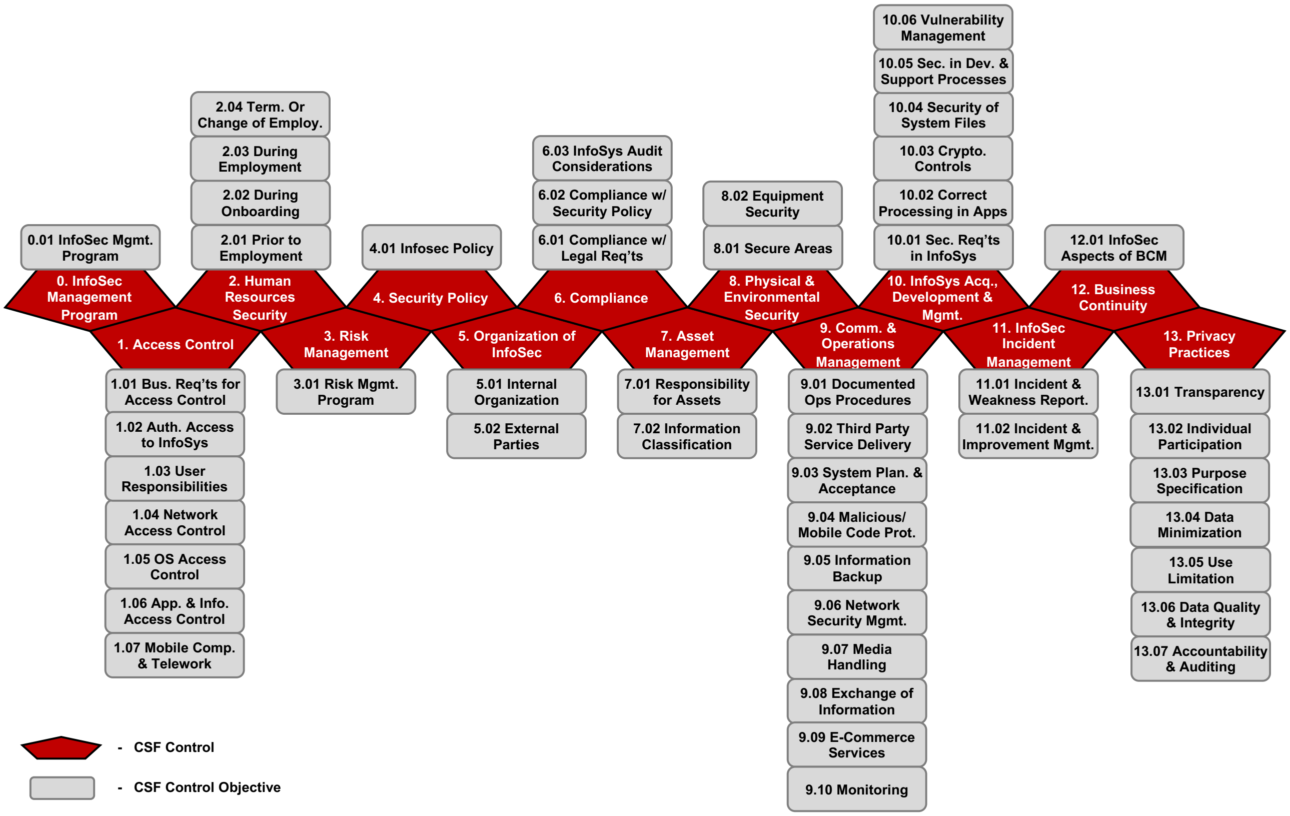

0.01 InfoSec Mgmt. Program
0. InfoSec Management Program
1. Access Control
1.01 Bus. Req'ts for Access Control
1.02 Auth. Access to InfoSys
1.03 User Responsibilities
1.04 Network Access Control
1.05 OS Access Control
1.06 App. & Info. Access Control
1.07 Mobile Comp. & Telework
2.04 Term. Or Change of Employ.
2.03 During Employment
2.02 During Onboarding
2.01 Prior to Employment
2. Human Resources Security
3. Risk Management
3.01 Risk Mgmt. Program
4.01 Infosec Policy
4. Security Policy
5. Organization of InfoSec
5.01 Internal Organization
5.02 External Parties
6.03 InfoSys Audit Considerations
6.02 Compliance w/ Security Policy
6.01 Compliance w/ Legal Req'ts
6. Compliance
7. Asset Management
7.01 Responsibility for Assets
7.02 Information Classification
8.02 Equipment Security
8.01 Secure Areas
8. Physical & Environmental Security
9. Comm. & Operations Management
9.01 Documented Ops Procedures
9.02 Third Party Service Delivery
9.03 System Plan. & Acceptance
9.04 Malicious/ Mobile Code Prot.
9.05 Information Backup
9.06 Network Security Mgmt.
9.07 Media Handling
9.08 Exchange of Information
9.09 E-Commerce Services
9.10 Monitoring
10.06 Vulnerability Management
10.05 Sec. in Dev. & Support Processes
10.04 Security of System Files
10.03 Crypto. Controls
10.02 Correct Processing in Apps
10.01 Sec. Req'ts in InfoSys
10. InfoSys Acq., Development & Mgmt.
11. InfoSec Incident Management
11.01 Incident & Weakness Report.
11.02 Incident & Improvement Mgmt.
12.01 InfoSec Aspects of BCM
12. Business Continuity
13. Privacy Practices
13.01 Transparency
13.02 Individual Participation
13.03 Purpose Specification
13.04 Data Minimization
13.05 Use Limitation
13.06 Data Quality & Integrity
13.07 Accountability & Auditing
- CSF Control
- CSF Control Objective

Figure 11. HITRUST CSF Control Categories and Objectives

The HITRUST CSF is also structured in such a way that specific control requirements can be applied to a specific scope based relevant organizational, system (technical) and regulatory (compliance) risk factors as shown in Figure 12.

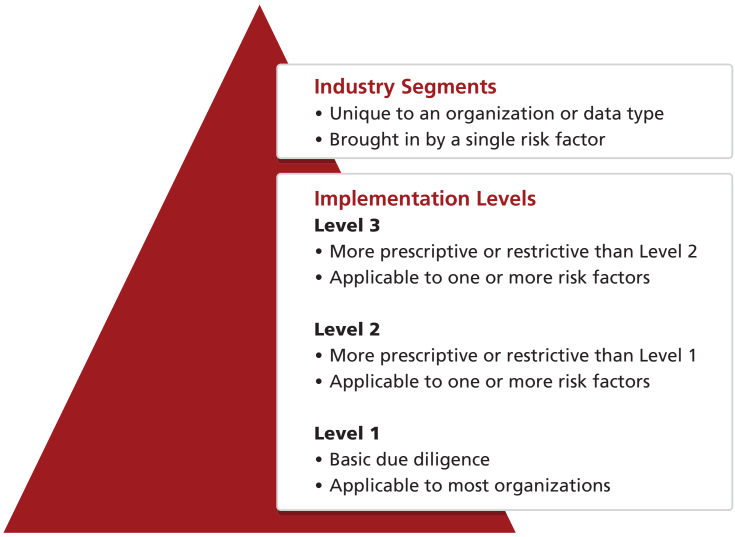

Industry Segments
• Unique to an organization or data type
• Brought in by a single risk factor
Implementation Levels
Level 3
• More prescriptive or restrictive than Level 2
• Applicable to one or more risk factors
Level 2
• More prescriptive or restrictive than Level 1
• Applicable to one or more risk factors
Level 1
• Basic due diligence
• Applicable to most organizations

Figure 12. Layered Structure of a HITRUST CSF Control

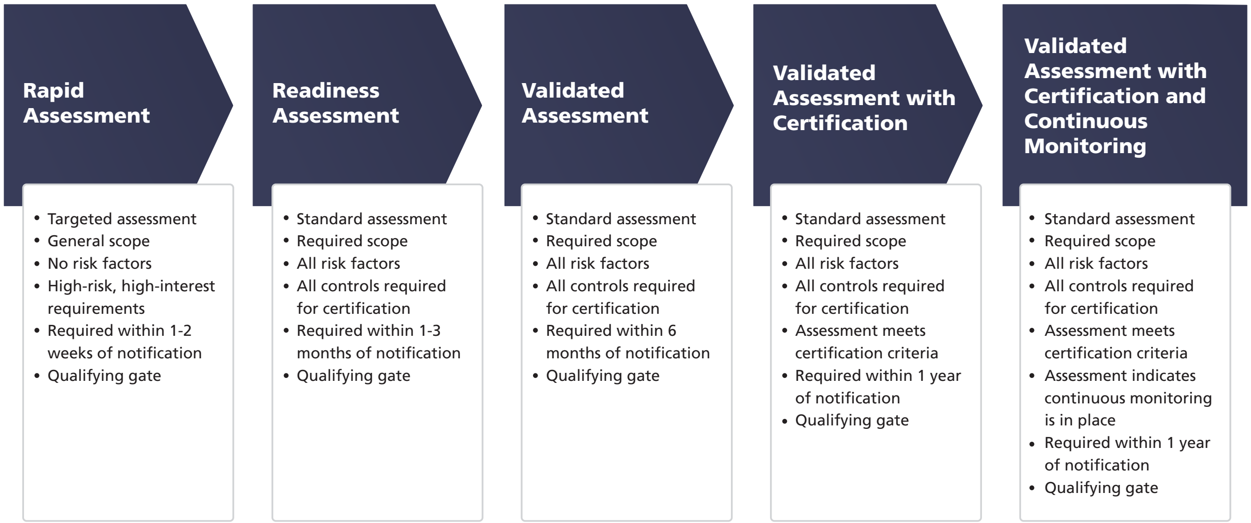
Each HITRUST CSF control contains up to three implementation levels. Each level may address one or more risk factors and contain multiple prescriptive control requirements that are considered generally applicable to organizations with those risk factors. Each control may also contain one or more industry segments, which are currently brought in by a single regulatory risk factor, i.e., a specific law, regulation or framework. Each segment provides additional prescription to cover control requirements that are generally unique to the organization and/or data type that is addressed by the risk factor but was not included previously in a standard implementation level.

Once the control requirements are specified based on the risk factors applicable to the relevant scope, all elements of the requisite assurance are addressed: the rigor of the control requirements to provide an acceptable level of due diligence and due care, the rigor of the control implementation to ensure an acceptable level of residual risk, and the rigor of the assessment to ensure an acceptable level of confidence in the assurances provided.

Assessment Process

Once the desired assessment is scoped and the HITRUST CSF controls are tailored appropriately, the third party is responsible for conducting the assessment and providing the HITRUST CSF assessment report to the organization.[59] The organization is responsible for providing oversight by monitoring progress and, if needed, periodically evaluating the third party's progress and making risk-based decisions about continuing or discontinuing the assessment process.

A generic process for third parties to obtain a CSF assessment that meets the organization's assurance requirements is provided in Figure 13 below.



Rapid Assessment

- Targeted assessment
- General scope
- No risk factors
- High-risk, high-interest requirements
- Required within 1-2 weeks of notification
- Qualifying gate

Readiness Assessment

- Standard assessment
- Required scope
- All risk factors
- All controls required for certification
- Required within 1-3 months of notification
- Qualifying gate

Validated Assessment

- Standard assessment
- Required scope
- All risk factors
- All controls required for certification
- Required within 6 months of notification
- Qualifying gate

Validated Assessment with Certification

- Standard assessment
- Required scope
- All risk factors
- All controls required for certification
- Assessment meets certification criteria
- Required within 1 year of notification
- Qualifying gate

Validated Assessment with Certification and Continuous Monitoring

- Standard assessment
- Required scope
- All risk factors
- All controls required for certification
- Assessment meets certification criteria
- Assessment indicates continuous monitoring is in place
- Required within 1 year of notification
- Qualifying gate

Figure 13. Notional Qualifying Assessment Process

If the third party has a HITRUST CSF assessment, the organization must review the assessment report in its entirety to verify:

- The assessment type is valid, e.g., a self-assessment does not satisfy the requirement for a HITRUST CSF Validated Assessment,
- The assessment scope covers the scope required for the product(s) and/or services(s) provided or will be provided, i.e., no part of the organization and/or no system that must be addressed by the assessment are excluded,

- The assessment includes all the risk factors needed to properly tailor the HITRUST CSF controls for the required scope, e.g., the assessment could list more factors if the required factors are included,
- The assessment scores meet the required minimum(s), e.g., the average maturity score is 75 for a third party with high inherent risk, and
- The assessment meets the criteria for CAPs, i.e., CAPs are not needed to address any gaps in control implementation when CAPs are not allowed.

If the assessment is acceptable, the 'gate' for a qualifying assessment has been reached and the organization may proceed to the Risk Mitigation Process (Qualify Step 4 – Risk Mitigation).

If the assessment provided by the third party does not satisfy any one of these requirements, the organization will need to work with the third party to ensure additional assessment is performed to address the deficiency(ies) outlined above. The process will be almost identical to that undertaken by third parties that do not have a CSF assessment.

Those third parties without an appropriate CSF assessment will enter the Qualifying Assessment Process where needed. For example, an organization that is required to provide a HITRUST CSF Validated Assessment that meets HITRUST CSF certification requirements but only has a HITRUST CSF Readiness Assessment will begin the process of obtaining a HITRUST CSF Validated Assessment. Whether the third party must submit an additional assessment will depend on how well the third party scores on the initial HITRUST CSF Validated Assessment. Third parties with robust information security and privacy programs may very well submit an assessment that meets the criteria for certification; however, it's also possible for a third party to submit multiple HITRUST CSF Validated Assessments if the initial assessment does not meet the scoring requirements even if certified, e.g., when certification with a robust continuous monitoring program is required.

Requesting Additional Information

At any point during the Qualifying Assessment Process, the organization may need to reach out to the third party and request additional information, e.g., about the state of the assessment or specific questions about what an assessment report may or may not address, and are typically required to address concerns with:

- Accuracy, e.g., concerns about whether the observations and supporting artifacts in a report do not appear to justify the control maturity scores,
- Completeness, e.g., questions as to whether the entire scope or all elements of the controls are adequately addressed in the report, and
- Granularity, e.g., do the artifacts provide the necessary details around all aspects of the control requirements.

Note most of these concerns arise when relying on a HITRUST CSF Rapid or Readiness Assessment, as HITRUST CSF Validated Assessments are conducted by qualified HITRUST CSF Assessors and undergo a quality review by HITRUST before the report is issued.

Improving Trust

Control Maturity

Control maturity is one of the best ways to determine an organization's security posture, especially when assessed against a comprehensive framework of prescriptive privacy and security controls. HITRUST's approach is similar to the Carnegie Melon Software

Engineering Institute's (CM-SEI's) Capability Maturity Model Integrated (CMMI) for process improvement[60] but modified along the lines of NIST's Program Review for Information Security Management Assistance (PRISMA) approach to maturity[61] to better fit assessments of information security and privacy risk and compliance programs.

The HITRUST CSF control maturity model's first three levels provide rough equivalence with traditional compliance-based assessments. First, control requirements must be clearly understood at all levels of the organization through documented policies or standards that are communicated with all stakeholders. Second, procedures must be in place to support the actual implementation of required controls. And third, the controls must be fully implemented and tested as required to ensure they operate as intended. These three maturity levels address the concept of design effectiveness.

The model's last two maturity levels differ from the CMMI approach by integrating the concept of "you can't manage what you don't measure" and address operational effectiveness by specifying metrics and evaluating an organization's response to potential deficiencies indicated by these metrics.[62]

Since control maturity provides a mathematical estimator for the likelihood a control will fail, more mature organizations subsequently pose less risk that those that are less mature. Further, HITRUST's CSF control maturity model provides a valid way of forecasting future effectiveness—and subsequently risk—based on the 'measured' and 'managed' levels of maturity, i.e., the continuous monitoring of the organization's control environment. The result is a higher level of assurance than what can be provided by traditional assessment models centered solely on current effectiveness of implementation.

Levels of Assurance

As discussed earlier, there are five types of assessments used to help qualify a third party for a business relationship with an organization. We list them here by increasing level of assurance with a short description of the characteristics that help determine their assurance level:

- HITRUST CSF Rapid Assessment – A limited set of control requirements and assessment by the third party using a simplified version[63] of the HITRUST CSF control maturity model (see Appendix B). Note HITRUST highly recommends providing the Rapid Assessment concurrently with any questionnaire(s) the organization may send a third party, as discussed previously in Qualify Step 1 – Pre-Qualification Work.
- HITRUST CSF Readiness Assessment – Full set of control requirements tailored to the required scope and assessment by the third party using the standard version of the HITRUST CSF control maturity model.
- HITRUST CSF Validated Assessment – Full set of control requirements tailored to the required scope and assessment by an independent HITRUST CSF assessor using the standard version of the HITRUST CSF control maturity model.[64]
- HITRUST CSF Validated Assessment with Certification – Full set of control requirements tailored to the required scope, assessment by an independent HITRUST CSF assessor using the standard version of the HITRUST CSF control maturity model, and assessment scores meet HITRUST CSF certification criteria.
- HITRUST CSF Validated Assessment with Certification and Continuous Monitoring - Full set of control requirements tailored to the required scope, assessment by an independent HITRUST CSF assessor using the standard version of the HITRUST CSF control maturity model, assessment scores meet HITRUST CSF certification criteria, and the aggregated maturity score—currently 87 or more—reflects program management based on the use of metrics.[65]

This concept of increasing levels of assurance is depicted graphically in Figure 14:

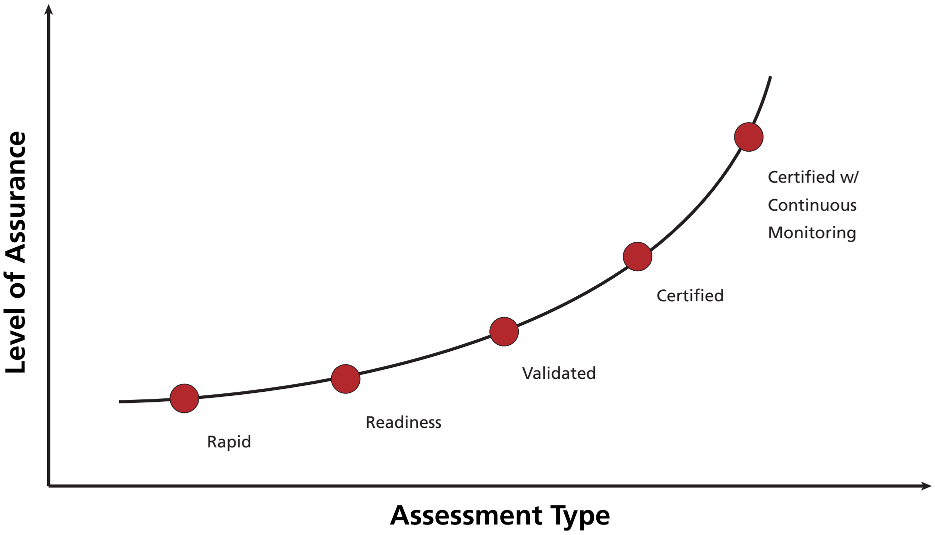


Figure 14. Relative Assurance Based on Assessment Type

Assurance is improved by each succeeding type of assessment based on the completeness of the control requirements specified, whether it's conducted by a third party or an independent HITRUST CSF assessor, the rigor of the assessment and scoring approach, and the maturity of program implementation as reflected by the scores.

The HITRUST Trust Score

As discussed in the Risk Triage Process (Qualify Step 2 – Risk Triage), each type of assessment provides a level of assurance appropriate for the inherent risk presented by a third party for the business relationship. While this works well if the assessment received by the organization is the one specified in risk triage, it can be problematic if it is not. And it can be particularly problematic if say, for example, it's a HITRUST CSF Readiness Assessment for a third party that's required to be HITRUST CSF certified. This is primarily due to the lower level of assurance, i.e., trust, that can be placed in the self-assessment and the amount of time that may be required for the third party to become certified.

Self-assessments are historically less trustworthy than assessments conducted by a third party, such as HITRUST CSF Validated Assessments, because the scores are almost always inflated due to a lack of understanding of the requirements and how they should be assessed or even due to intentional misrepresentation. However, it has been shown that self-assessments can be more accurate—and subsequently more trustworthy—when proceeded by appropriate guidance or facilitated by a subject matter expert. It is for this reason that HITRUST generally requires a facilitated HITRUST CSF Readiness Assessment for TPRM.

To further increase the level of trust provided by a HITRUST CSF Readiness Assessment used to help qualify a third party for a relatively risky business relationship, HITRUST also incorporates a trust score to support third-party qualification by comparing the results of a HITRUST CSF Readiness Assessment with the results of any HITRUST CSF Validated Assessment(s) generated later in the process. If a third party provides a valid, reliable ('rely-able') HITRUST CSF Readiness Assessment and later provides a HITRUST CSF Validated Assessment, one would expect the control maturity scores to remain relatively 'flat' if not improve over time. However, control maturity scores that decrease over time would indicate the original HITRUST CSF Readiness Assessment was not 'rely-able.' Differences in the 'right' direction would result in higher trust scores and those in the 'wrong' direction would result in lower trust scores.

HITRUST subsequently proposes a Trust Score based on a standard z score for the difference of means between the HITRUST CSF maturity scores for the HITRUST CSF Readiness Assessment and the HITRUST CSF Validated Assessment.

If $\overline{x}_{\Delta_i}$ is the difference in HITRUST CSF maturity scores between a HITRUST CSF Rapid Assessment and a HITRUST CSF Validated Assessment and μ and σ are the population mean and standard deviation of the differences, respectively, then

$$z = \frac{\overline{x}_{\Delta_i} - \mu_\Delta}{\sigma_\Delta}$$

Since we may safely assume that the population mean of the differences, μ_Δ, should be zero, we are only required to use the sample standard deviation of the means, s_{Δ_i} , as an estimate of the population standard deviation, σ_Δ. The standard z score for the difference of means may then be written as

$$z = \frac{\overline{x}_{\Delta_i} - 0}{s_{\Delta_i}} = \frac{\overline{x}_{\Delta_i}}{s_{\Delta_i}}.$$

Figure 15 below depicts the bell curve for a standard z score.

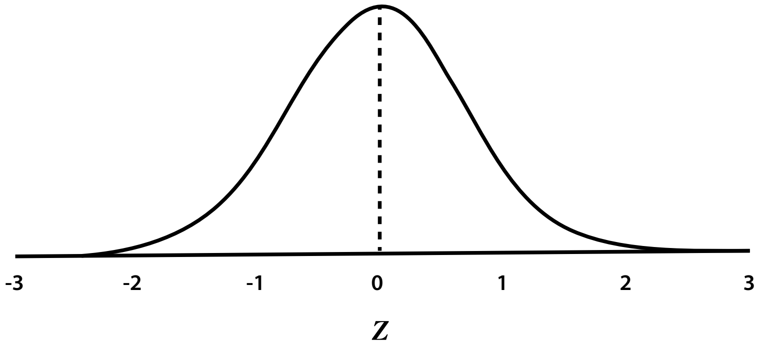


Figure 15. Bell Curve for Standard Z Score

Differences between the means will be computed by subtracting the HITRUST CSF control maturity scores for the HITRUST CSF Rapid Assessment from the corresponding maturity scores in the HITRUST CSF Validated Assessment. Overestimation of the control maturity scores in the HITRUST CSF Rapid Assessment will result in negative values for the differences, and consistent overestimation will likely result in a negative mean of the differences, $\overline{x}_{\Delta_i}$ i.

The HITRUST Trust Score will subsequently focus on the negative portion of the bell curve, establish a Trust Score of zero (0) for z scores less than -3 standard deviations from the mean, and establish a maximum Trust Score of ten (10) for z scores greater than or equal to zero. The latter condition indicates organizations with consistent HITRUST CSF Rapid Assessment and HITRUST CSF Validated Assessment results as well as those that underestimate their maturity on a self-assessment are equally trustworthy. Modifications to the bell curve resulting from these conditions are reflected in Figure 16.

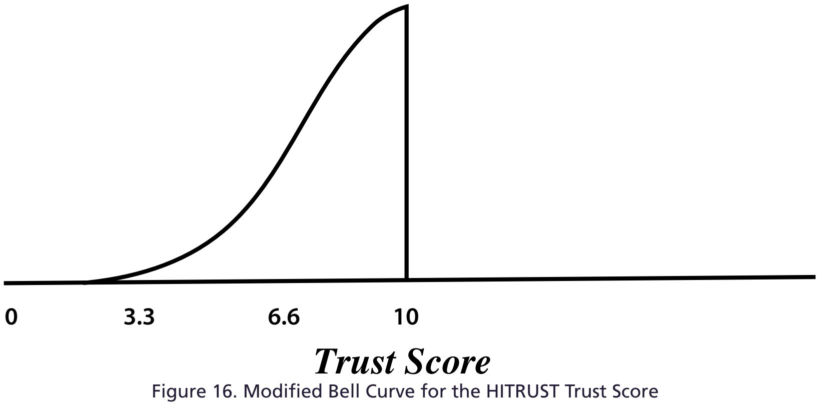


Figure 16. Modified Bell Curve for the HITRUST Trust Score

A third party's Trust Scores, *TS*, may be interpreted as shown in Table *6*.

Table 6. Interpreting a HITRUST Trust Score

HITRUST Trust Score	Interpretation
9 ≤ *TS* ≤ 10	Very Trustworthy
8 ≤ *TS* < 9	Trustworthy
7 ≤ *TS* < 8	Slightly (Un)Trustworthy
6 ≤ *TS* < 7	Untrustworthy
TS < 6	Very Untrustworthy

While HITRUST recommends organizations interpret these scores in the overall context of the relationship, the HITRUST Trust Score provides another useful data point in an organization's evaluation of the overall trustworthiness of a third party and additional confidence in the assurances it provides. And just knowing the organization will be presented this information with every assessment submitted after the HITRUST CSF Readiness Assessment could have the added benefit of encouraging third parties to be more 'circumspect' when conducting their self-assessments.

Summary

Once an appropriate assurance mechanism is selected during risk triage, the organization works with the third party to establish a timeline for compliance, assist and/or monitor the third party until the appropriate assurances are provided, and then reviews the assurances for accuracy and completeness.

One area in which the organization can assist the third party is to help ensure applicable organizational and system elements are included in the assessment. This includes specification of the physical and logical systems used by a third party that support the workflow(s) for the product(s) and/or service(s) being or to be provided the organization, as well as the logical interfaces to the systems included in the assessment scope. The HITRUST CSF control requirements included in the assessment will also be determined by relevant organizational, system (technical) and regulatory (compliance) risk factors applicable to the required scope.

At this point, all elements of the requisite assurance are addressed: the rigor of the control requirements to provide an acceptable level of due diligence and due care, the rigor of the control implementation to ensure an acceptable level of residual risk, and the rigor of the assessment to ensure an acceptable level of confidence in the assurances provided.

The TPRM Step 3 – Qualify process allows an organization to pass through multiple 'gates' by submitting successively rigorous assurances based on the completeness of the control requirements specified—whether it's conducted by a third party or an independent HITRUST CSF assessor, the rigor of the assessment and scoring approach, and the maturity of program implementation as reflected by the scores—until the required level of assurance is provided.

And to further increase the level of trust provided by a HITRUST CSF Readiness Assessment, HITRUST also incorporates a trust score to support third-party qualification by comparing the results of a HITRUST CSF Readiness Assessment with the results of any HITRUST CSF Validated Assessment(s) generated later in the process, which will provide another useful data point in an organization's evaluation of the overall trustworthiness of a third party.

Qualify Step 4 – Risk Mitigation

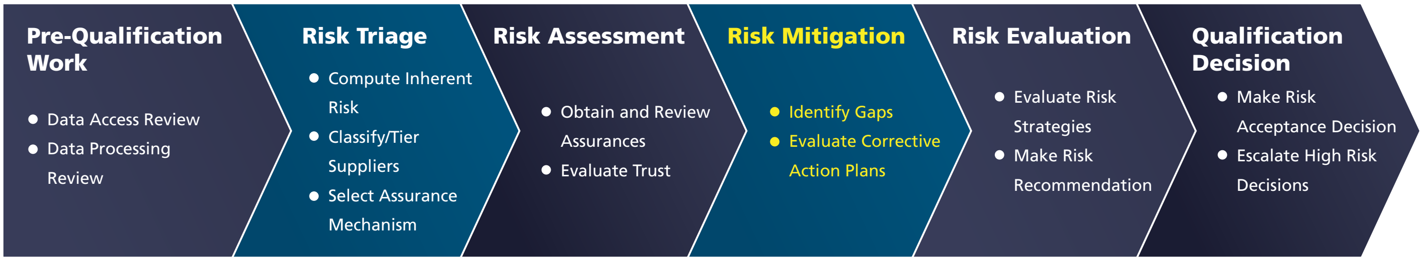

Pre-Qualification Work
● Data Access Review
● Data Processing Review
Risk Triage
● Compute Inherent Risk
● Classify/Tier Suppliers
● Select Assurance Mechanism
Risk Assessment
● Obtain and Review Assurances
● Evaluate Trust
Risk Mitigation
● Identify Gaps
● Evaluate Corrective Action Plans
Risk Evaluation
● Evaluate Risk Strategies
● Make Risk Recommendation
Qualification Decision
● Make Risk Acceptance Decision
● Escalate High Risk Decisions

Figure 17. Qualify Step 4 – Risk Mitigation

Although risk mitigation is technically a separate step in the qualification process, it should be initiated after the receipt of any assessment received by the organization from a third party as a matter of routine, whether as an interim step or the final. This is necessary as each assessment serves as a gate during which the organization evaluates—or reevaluates—the level of anticipated residual risk and determines if the third party may continue through the qualification process. This 'iterative' adjustment to the generic TPRM Step 3 – Qualify process model process shown above is reflected in Figure 18.

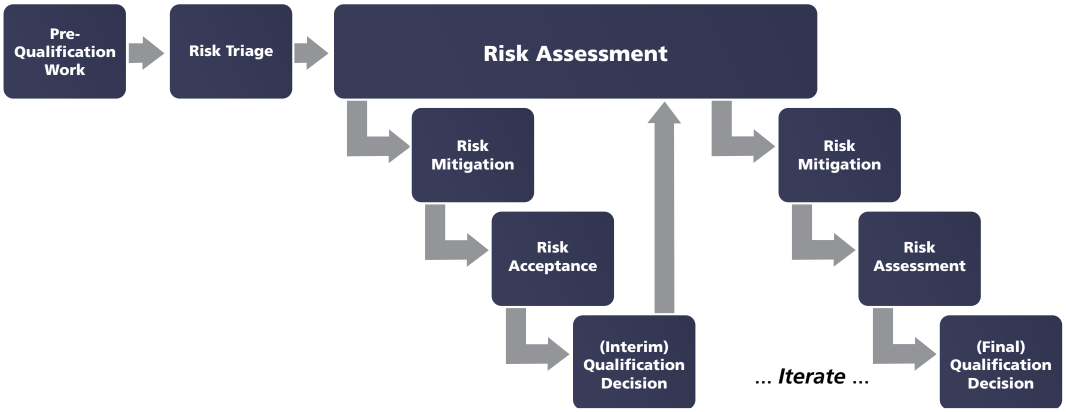


Figure 18. Iterative View of the TPRM Qualify Process

The last three steps of the qualification process may iterate as often as needed until the organization is confident the residual risk posed by the third party is acceptable or, alternatively, the residual risk is considered too great and the third party is disqualified.

Identifying Gaps and Corrective Actions

For each assessment submitted during the qualification process, the organization should compare the third party's current and target security profiles and identify any gaps that may need to be addressed prior to entering Qualify Step 5 – Risk Acceptance. The third party's target profile is obtained when its organizational elements and systems are scoped for the assessment and the HITRUST CSF controls are tailored to the scope based on its applicable risk factors. The third party's current profile is obtained once an assessment is completed and the results are delivered to the organization. Potential gaps are identified by comparing the two profiles.[66]

The HITRUST CSF Rapid and Readiness Assessment reports do not typically come with CAPs, so the organization will need to work with the third party to ensure the appropriate CAPs are developed and ensure the actions taken will adequately address the gaps. All HITRUST CSF Validated Assessment reports come with 'required' CAPs to address gaps that prevent it from meeting the minimum requirements for certification, and all Validated Assessment reports that meet the requirements for HITRUST CSF certification will come with 'required' CAPs for similar reasons; however, the third party must typically address those requirements before it can recertify.[67]

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

Although organizations and third parties typically have no problem with identifying the corrective actions needed to address specific gaps, some have difficulty rating the risks and subsequently prioritizing the work. To help with CAP prioritization, HITRUST provides non-contextual impact ratings for each CSF control, which allows the computation of relative risk for each deficiency identified in an assessment. The ratings are non-contextual in that they assume the probable impact should the control fail, assuming all other controls are in place. HITRUST also provides implementation dependencies amongst CSF controls based on priority codes for federal controls. The priority codes indicate relative order of priority (sequencing) for implementation, which helps provide a more structured, phased approach by ensuring controls upon which others depend are implemented first.[68]

For those control requirements a third party may not wish to implement but cannot accept the associated residual risk, HITRUST provides for the selection of compensating controls based on a standardized risk analysis, which is used to justify the exception for a specific organization or gain HITRUST approval for its broader application across the industry. HITRUST refers to compensating controls submitted to and approved by the HITRUST Alternate Controls Committee for general use by organizations seeking validation or certification against the CSF, as 'alternate controls.'[69]

Inputs, activities and outputs of the gap analysis and CAP development process are shown in Table *7*.

Table 7. Gap Analysis and CAP Development & Prioritization

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

Evaluating Corrective Action Plans

Once CAPs are received from the third party, the organization must review them and ensure the actions and the timeline for their implementation are acceptable. If not, the organization will need to work with the third party to determine if any outstanding issues with the plan(s) can be addressed before proceeding to the next step, Qualify Step 5 – Risk Acceptance.

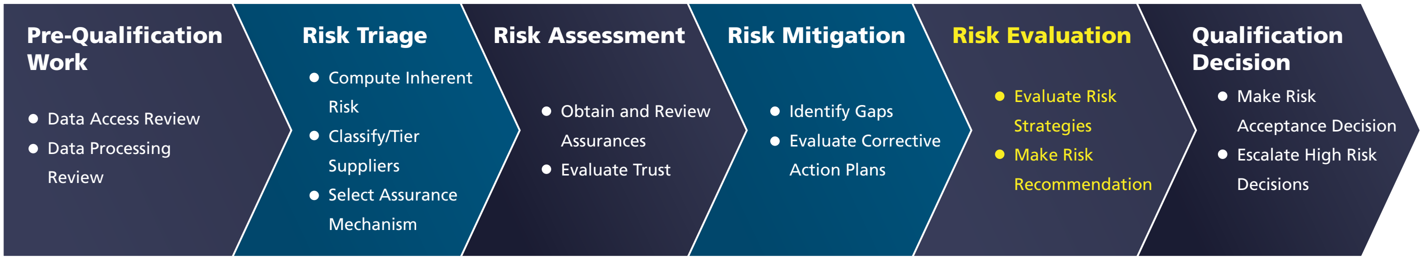
Summary

Although risk mitigation is technically a separate step in the qualification process, it should be initiated after the receipt of any assessment received by the organization from a third party as a matter of routine, whether as an interim step or the final. This is necessary as each assessment serves as a gate during which the organization evaluates—or reevaluates—the level of anticipated residual risk and determines if the third party may continue through the qualification process.

For each assessment submitted during the qualification process, the organization should compare the third party's current and target security profiles and identify any gaps that may need to be addressed prior to entering Qualify Step 5 – Risk Acceptance. The organization should consider assisting third parties with CAP development, especially when submitting HITRUST CSF Rapid and Readiness Assessments and must review all CAPs submitted with any assessment for effectiveness, completeness and timeliness.

HITRUST also provides additional guidance on CAP development, prioritization and the submission and approval of compensating controls as an alternative to existing HITRUST CSF control requirements.

Qualify Step 5 – Risk Evaluation



Pre-Qualification Work
- Data Access Review
- Data Processing Review

Risk Triage
- Compute Inherent Risk
- Classify/Tier Suppliers
- Select Assurance Mechanism

Risk Assessment
- Obtain and Review Assurances
- Evaluate Trust

Risk Mitigation
- Identify Gaps
- Evaluate Corrective Action Plans

Risk Evaluation
- Evaluate Risk Strategies
- Make Risk Recommendation

Qualification Decision
- Make Risk Acceptance Decision
- Escalate High Risk Decisions

Figure 19. Qualify Step 5 – Risk Evaluation

Once an assessment is complete, whether provided as interim assurance or as the third party's final submission, the organization must evaluate the remaining residual risk and prepare a recommendation to the individual or office authorized to accept risk on behalf of the organization.

Risk Strategies

Since the organization determines that the HITRUST CSF control requirements specified for the required scope will minimize the residual risk of entering a business relationship with a third party, any deviation from the full implementation of the requirements may potentially result in excessive residual risk. It is the attempt to minimize this excessive risk—preferably as close to zero as possible—that is the goal of all four of the preceding steps in the TPRM Step 3 – Qualify process.

The organization must therefore evaluate any unresolved gaps in mitigation of these controls by the third party, as well as any third party decisions to transfer, avoid or accept a particular risk.

Mitigation

The organization should review the status of the controls and identify any outstanding gaps to determine if the risk has been mitigated appropriately. For example, some gaps may present very small amounts of excessive residual risk. This may be due to an incomplete implementation due to architectural, technical, legal, or similar constraints. Or it may be due to the implementation of an alternative control that does not fully mitigate the type and amount of risk mitigated by the original CSF control (albeit some consider compensating or alternate controls to be a combination of risk avoidance and risk acceptance[70]).

Transference

The organization should review the policies for any risk the third party has insured and the agreements for any risk the third party has received indemnification.

Avoidance

The organization should review any policies, agreements or other authoritative documentation that prohibits the third party engaging in a particular activity and subsequently avoiding the associated inherent risk.

Acceptance

The organization should review all risk that was not fully mitigated, transferred or avoided and ensure the third party has appropriately and formally accepted the risk based on a valid risk analysis.

Risk Recommendation

Risk strategies must be carefully aligned with the organization's needs and the value of the proposed product or service priority. Furthermore, risk strategies must consider the impact that the risk could have on the organization to ensure that its trust in a third party is well-placed.

Risk Scoring[71]

HITRUST takes a quasi-quantitative approach to scoring risk based on the maturity of a control requirement's implementation and a non-contextual impact score.

Likelihood

As discussed previously, control implementation is evaluated against the HITRUST CSF control maturity model, which consists of five levels with a specific number of 'points' available for each level: Policy (25 points), Procedures (25 points), Implementation (25 points), Measured (15 points) and Managed (10 points).

Each of the five maturity levels are evaluated against five levels of compliance with specified requirements, as shown in Table *8*.

Table 8. HITRUST CSF Control Scoring Model

Score	Description
Non-Compliant (NC) 0%	Very few if any of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 0% (point estimate) or 0% to 12% (interval estimate).
Somewhat Compliant (SC) 25%	Some of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 25% (point estimate) or 13% to 37% (interval estimate).
Partially Compliant (PC) 50%	About half of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 50% (point estimate) or 38% to 62% (interval estimate).
Mostly Compliant (MC) 75%	Many but not all the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 75% (point estimate) or 63% to 87% (interval estimate).
Fully Compliant (FC) 100%	Most if not all the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 100% (point estimate) or 88% to 100% (interval estimate).

HITRUST considers a fully implemented control that is continuously monitored to be the most mature possible as it is less likely to fail and, should it fail, more likely to be remediated efficiently and effectively. Control maturity is therefore a valid estimator for the likelihood a risk will materialize when aggregated over a HITRUST CSF control specification, control objective, control category or other area of interest.

Impact

Impact of a control failure is generally unique to an organization as it is based on many factors such as the status of other controls in place and the criticality of the information affected by the failure, amongst others. However, HITRUST provides non-contextual Impact Codes, which help provide a starting point for organizations in evaluating the relative impact between and amongst the HITRUST CSF controls and their underlying requirements. The impact codes range from Very Low (1), Low (2), Moderate (3), High (4) and Very High (5) and may be converted to an impact estimate for the purposes of computing a risk estimate.

Risk

Risk can therefore be estimated using the HITRUST CSF control maturity scores and impact codes as

$$R = L * I = \left[\frac{(100 - MS)}{100}\right][(IR - 1) * 25]$$

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

These scores may be aggregated across HITRUST CSF controls, control objectives, and control categories; or topical/targeted groupings of control requirements (e.g., wireless networks and devices).

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

Table *9* provides the intervals for both models:

Table 9. Risk Scales

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

Risk grades may be computed from the academic risk scores by subtracting them from 100 and using a traditional academic grading scale: A (90-100), B (80-89), C (70-79), D (60-69) and F (0-59). The grades basically let management know how well they are managing residual risk due to "immature" controls in the environment. Full implementation of a control, i.e., full credit for the policy, procedures and implementation maturity levels, would generally provide an overall "C" for the organization, which would be considered average for the industry. Organizations receive higher grades (an "A" or "B") through continuous monitoring (measurement) and active management of control effectiveness.

Figure 20 below provides an example of an academic scorecard based on a comprehensive security assessment with scores aggregated across HITRUST CSF control objectives and control categories.

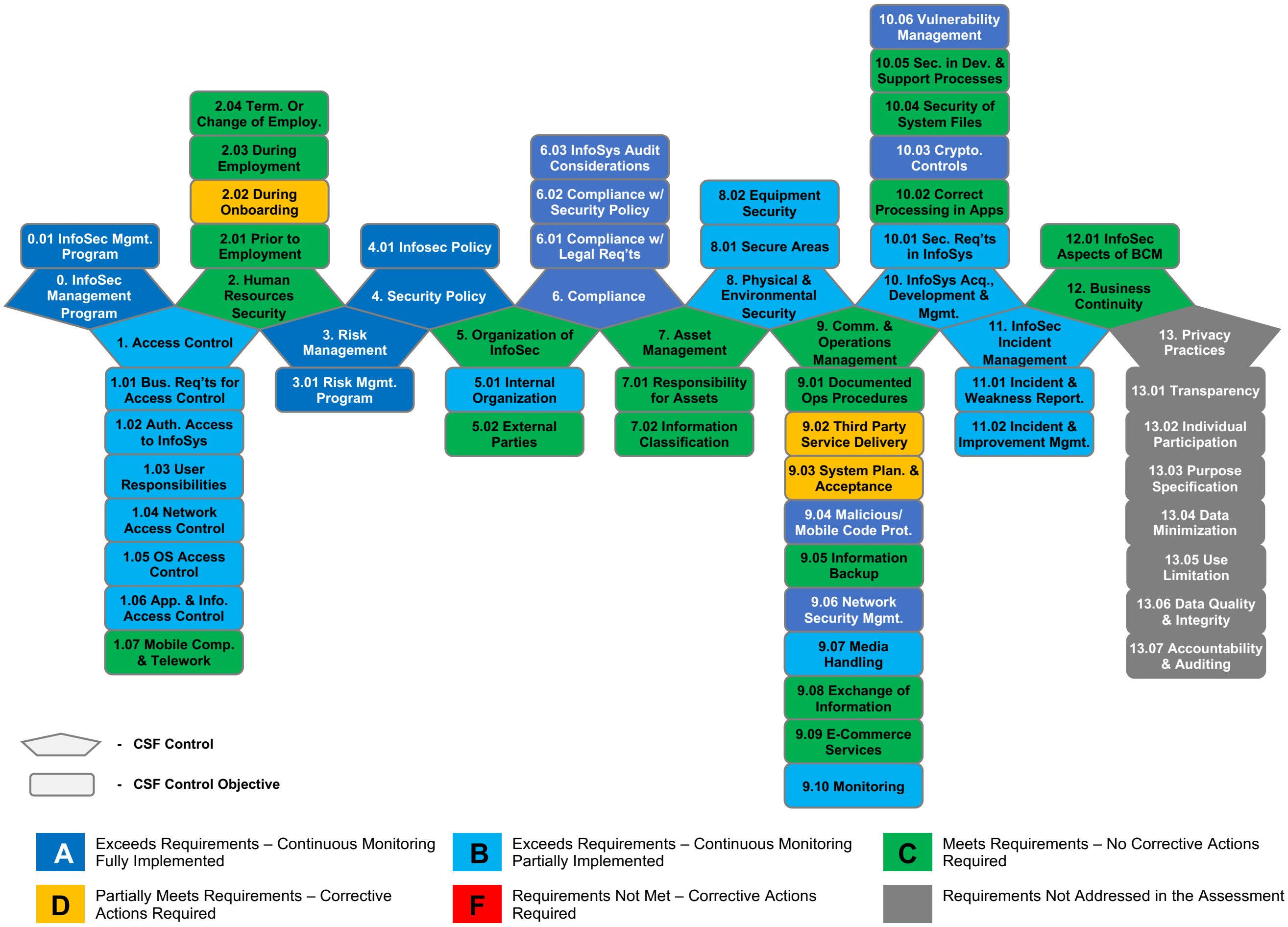

0.01 InfoSec Mgmt. Program
0. InfoSec Management Program
1. Access Control
1.01 Bus. Req'ts for Access Control
1.02 Auth. Access to InfoSys
1.03 User Responsibilities
1.04 Network Access Control
1.05 OS Access Control
1.06 App. & Info. Access Control
1.07 Mobile Comp. & Telework
2.04 Term. Or Change of Employ.
2.03 During Employment
2.02 During Onboarding
2.01 Prior to Employment
2. Human Resources Security
3. Risk Management
3.01 Risk Mgmt. Program
4.01 Infosec Policy
4. Security Policy
5. Organization of InfoSec
5.01 Internal Organization
5.02 External Parties
6.03 InfoSys Audit Considerations
6.02 Compliance w/ Security Policy
6.01 Compliance w/ Legal Req'ts
6. Compliance
7. Asset Management
7.01 Responsibility for Assets
7.02 Information Classification
8.02 Equipment Security
8.01 Secure Areas
8. Physical & Environmental Security
9. Comm. & Operations Management
9.01 Documented Ops Procedures
9.02 Third Party Service Delivery
9.03 System Plan. & Acceptance
9.04 Malicious/ Mobile Code Prot.
9.05 Information Backup
9.06 Network Security Mgmt.
9.07 Media Handling
9.08 Exchange of Information
9.09 E-Commerce Services
9.10 Monitoring
10.06 Vulnerability Management
10.05 Sec. in Dev. & Support Processes
10.04 Security of System Files
10.03 Crypto. Controls
10.02 Correct Processing in Apps
10.01 Sec. Req'ts in InfoSys
10. InfoSys Acq., Development & Mgmt.
11. InfoSec Incident Management
11.01 Incident & Weakness Report.
11.02 Incident & Improvement Mgmt.
12.01 InfoSec Aspects of BCM
12. Business Continuity
13. Privacy Practices
13.01 Transparency
13.02 Individual Participation
13.03 Purpose Specification
13.04 Data Minimization
13.05 Use Limitation
13.06 Data Quality & Integrity
13.07 Accountability & Auditing
- CSF Control
- CSF Control Objective
A Exceeds Requirements – Continuous Monitoring Fully Implemented
B Exceeds Requirements – Continuous Monitoring Partially Implemented
C Meets Requirements – No Corrective Actions Required
D Partially Meets Requirements – Corrective Actions Required
F Requirements Not Met – Corrective Actions Required
Requirements Not Addressed in the Assessment

Figure 20. Example Academic Risk Scorecard

Formal Recommendation

The organization's TPRM function would compile information from the report and generate any additional information, e.g., various risk scorecards to address specific areas of interest or concern, and include a recommendation for or against risk acceptance by the organization based on a comparative analysis of the assessment results with the required assurance level specified in Qualify Step 3 – Risk Triage.

Summary

After an assessment is received, the organization reviews the status of the controls implemented by the third party and reviews each aspect of its strategies for mitigating, transferring avoiding and accepting risk. It then prepares a risk recommendation report based on the resulting risk profile computed from the control maturity scores provided in the assessment and HITRUST's standard non-contextual impact codes.

Two models for expressing risk are available: a traditional, bell-curve shaped model, which is generally suitable for communicating risk to external stakeholders, and an academic, grade-based model that provides a more intuitive approach to interpreting risk, which is suitable for internal stakeholders. But regardless of the approach used to communicate risk, the risk recommendation should be based on a comparative analysis of the assessment results with the required assurance level.

Qualify Step 6 – Qualification Decision

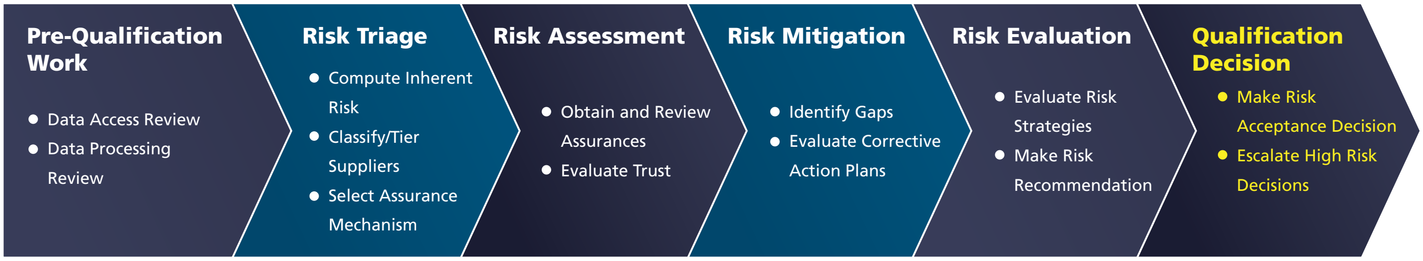


Figure 21. Qualify Step 6 – Qualification Decision

Once the risk recommendation is submitted, management will decide whether to accept the estimated residual risk of doing business with a third party on behalf of the organization based on its general risk appetite and specific risk tolerances. The decision maker may also decide to escalate the decision when the correct decision is not clear.

Risk Acceptance

The risk acceptance decision has two potential outcomes—accept the risk or not. But to make that decision, the organization needs to understand the residual risk a third party presents in relation to its capacity and general appetite for risk as well as risk tolerances and targets specific to the business relationship. In the context of this discussion:[72,73]

- *Risk capacity is the amount of risk an organization can actually bear,*
- *Risk appetite is the total exposed amount [of risk] that an organization wishes to undertake on the basis of risk-return trade-offs for one or more desired and expected outcomes,*
- *Risk tolerance is the amount of uncertainty an organization is prepared to accept in total or more narrowly within a certain business unit, a particular risk category or for a specific initiative,*
- *Risk target is a desired level of risk that an organization believes is optimal to meet its objectives, and*
- *Residual risk refers to [the amount] of risk remaining after security measures have been applied,*

The relationship between each of these risks is depicted in Figure 22.

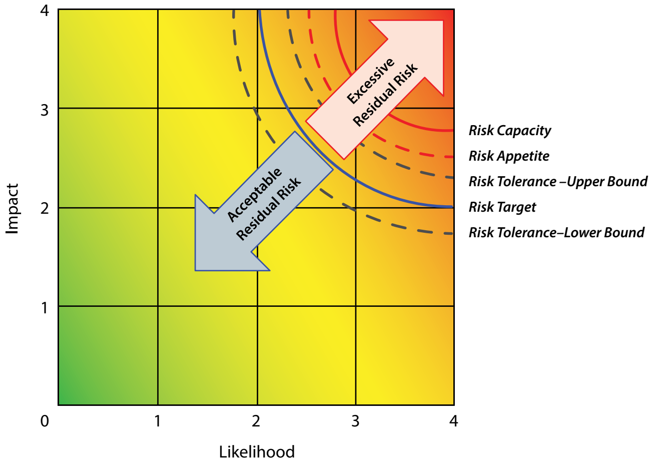


Figure 22. Relationship of Relevant Risk Types

The third party's target profile provides the risk target for the risk acceptance decision and should always be less than the total amount of risk the organization is willing to tolerate for the business relationship under consideration. Similarly, the maximum amount of risk tolerated should not exceed the organizations risk appetite, and at no time should the organization's risk appetite exceed its overall capacity to accept that risk.[74]

If the organization's current profile, as represented by the assessment results, completely addresses the organization's target profile, as represented by the HITRUST CSF control requirements tailored to the specified scope, then the amount of excessive residual risk is negligible. However, any gaps in implementation indicated by the HITRUST CSF control maturity scores represent a positive amount of excessive residual risk that should not exceed the organization's upper bound for risk tolerance.

Escalation

An organization's decision maker should be allowed to escalate the risk decision to executive management, enterprise risk management board, or even a board of directors under specific circumstances, e.g., when there is significant stakeholder interest or concerns about the proposed business relationship and the organization's level of risk tolerance is exceeded or close to being exceeded. HITRUST recommends organizations identify conditions for escalation in advance as part of their formal TPRM program.

Summary

To qualify a third party for a business relationship, the organization must understand the level of residual risk presented by the third party and ensure it does not exceed its ability to tolerate that risk. The HITRUST TPRM Qualification Methodology provides a robust method of establishing an appropriate risk target through the HITRUST CSF scoping and tailoring process and the resulting level of residual risk through the current profile established by a HITRUST CSF assessment. HITRUST also recommends organizations establish a formal escalation process with specific criteria for Qualify Step 6 – Qualification Decision to make decisions when organizational risk tolerances for the business relationship are exceeded or close to being exceeded.

Conclusion

The ‘heart’ of TPRM is the HITRUST TPRM Qualification Methodology, which provides organizations a comprehensive approach to defining inherent risk factors, triaging third parties based on inherent risk, working with third parties to obtain assurances, evaluating and reporting residual risk, and qualifying third parties for business by formally accepting the risk. And the ‘heart’ of the HITRUST TPRM Qualification Methodology is third-party triage based on inherent risk and the iterative assessment approach to obtaining necessary assurances.

By providing a common set of risk factors that are independent of the security and privacy controls that may or may not be implemented by a third party, an organization can readily ascertain the relative inherent risk between and amongst its vendors and determine a reasonable and appropriate mechanism to provide the assurances it needs at a reasonable cost. The approach also provides the flexibility organizations need in managing risk in terms of weighting some factors more heavily than others when computing likelihood and impact values or requiring more robust assurances, e.g., by mandating a HITRUST CSF Assessment against all the control requirements for which a vendor is responsible, as determined by its scoping and risk factors.

Qualification also supports multiple assessment types that may be used to obtain successively rigorous assurances based on the completeness of the control requirements specified —whether it’s conducted by a third party or an independent HITRUST CSF assessor, the rigor of the assessment and scoring approach, and the maturity of program implementation as reflected by the scores—until the required level of assurance is provided. HITRUST also incorporates a trust score to support third-party qualification by comparing the results of a HITRUST CSF Readiness Assessment with the results of any HITRUST CSF Validated Assessment(s) generated later in the process, providing yet another useful data point in the evaluation of a third party’s overall trustworthiness.

The HITRUST TPRM Qualification Methodology—based on one of the most comprehensive, prescriptive, yet tailorable control-based security and privacy risk and compliance risk management frameworks available—provides a common, standard approach for organizations in any industry, foreign and domestic, to manage their third-party risk consistently, efficiently, and effectively at a reasonable cost. Widespread adoption of the HITRUST TPRM Qualification Methodology will also provide similar benefits for third parties, who will be able to leverage their TPRM-based assessments for multiple organizations: a ‘win-win’ for organizations and third parties alike.

The Q4 2019 release of the HITRUST Assessment XChange™ (HAX) Manager platform now automates the vendor qualification process in the TPRM Methodology as well as the organization’s management of its vendors. The platform enables organizations to communicate to vendors, and vendors to communicate with customers, including the distribution of HITRUST Inherent Risk Questionnaires, Rapid Assessments, Validated Assessments and Trust Scores, managing requests between organizations, and tracking vendors who are already HITRUST CSF Certified. For more information on HAX, go to the HAX portal at https://hitrustax.com.

About HITRUST

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

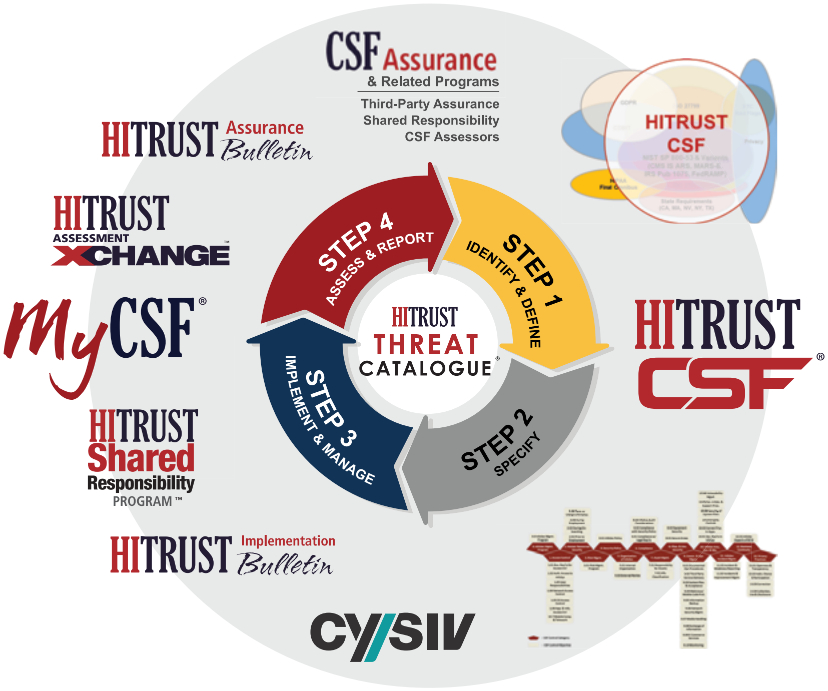


Figure 23. The HITRUST Approach

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

About the Author

Bryan Cline, Ph.D., Chief Research Officer

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 CSF Assurance Programs, for which he provides technical direction and oversight. He's 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.

Appendix A – Risk Triage Inherent Risk Factor Ratings

An explanation of the ratings used during the Risk Triage Process (Qualify Step 2 – Risk Triage) for each of the inherent risk factors are provided below:

- Risk Component – Impact
    - Organizational Risk Factor Type
        - IO1: Percentage of organizational data
            - ≤ 20%: The third party has access to 20% or less of the organization's sensitive information
            - 20 – 40%: The third party has access to over 20% but no more than 40% of the organization's sensitive information
            - 40 – 60%: The third party has access to over 40% but no more than 60% of the organization's sensitive information
            - 60 – 80%: The third party has access to over 60% but no more than 80% of the organization's sensitive information
            - > 80%: The third party has access to more than 80% of the organization's sensitive information
        - IO2: Total amount of organizational data
            - N/A: Not used
            - ≤1M Records: The third party has access to information on no more than 1M individuals
            - 1M – 10M Records: The third party has access to information on more than 1M individuals but no more than 10M
            - 10M – 60M Records: The third party has access to information on more than 10M individuals but no more than 60M
            - > 60M Records: The third party has access to information on more than 60M individuals
        - IO3: Criticality of the Relationship
            - Minimal: Little to no impact to business operations due to a loss of the service(s) or data; no need for workarounds; minimal to no impact on costs and/or revenue
            - Low: Operations can continue with some impact to the business due to a loss of the service(s) or data; little or no need for workarounds; small increase in costs and/or loss of revenue
            - Moderate: Business operations are somewhat limited due to a loss of the service(s) or data; reasonable workarounds exist; noticeable increase in costs and/or loss of revenue
            - High: Business operations are severely limited due to a loss of the service(s) or data; workarounds are inconvenient or do not exist; significant increase in costs or loss of revenue
            - Critical: The business is unable to reasonably continue operations due to a loss of the service(s) or data; workarounds do not exist; catastrophic increase in costs and/or loss of revenue

- Compliance Risk Factor Type
    - IC1: Comprehensiveness and specificity of requirements
        - None: There are no relevant laws, regulations, and/or mandatory standards that address security requirements for the type of information shared with the third party
        - General, Non-specific: Relevant laws, regulations, and/or mandatory standards specify a risk-based approach to protection but do not provide specific security practices or the practices that are prescribed do not provide a comprehensive control specification
        - General Framework-based Requirements: Relevant laws, regulations, and/or mandatory standards prescribe a comprehensive but general or objective-level framework such as the NIST Cybersecurity Framework or ISO 27001
        - Prescriptive Framework-based Requirements: Relevant laws, regulations, and/or mandatory standards prescribe a comprehensive and prescriptive framework such as the NIST SP 800-53 or the HITRUST CSF
        - N/A: Not used
    - IC2: Level of assurance required
        - None: Relevant laws, regulations, and/or mandatory standards do not specify an assurance requirement for organizational compliance
        - Self-Assessment / Attestation: Relevant laws, regulations, and/or mandatory standards allow for self-assessment or attestation of organizational compliance
        - Risk-based (Determined by the Org.): Relevant laws, regulations, and/or mandatory standards allow the organization to determine the level (rigor and kind) of assurance needed to demonstrate compliance
        - Specific Reporting Format: Similar to risk-based but prescribes a specific reporting format, such as an AICPA SOC 2 or IASE 3402
        - Specific Ctrl Requirement Framework: Relevant laws, regulations, and/or mandatory standards that prescribe an assessment and reporting methodology, such as NIST SP 800-18 or HITRUST CSF Assurance
    - IC3: Specified or observed fines and penalties
        - Insignificant: Little to no budgetary impact to the organization
        - Minor: Costs can be readily absorbed by the organization, such as by tapping into a contingency fund or reallocating funding across the budget
        - Moderate: Relies on cyber insurance to address potential impact to the organizational budget; would have a noticeable budgetary impact without cyber insurance
        - Significant: Has a noticeable budgetary impact to the organization, even if cyber insurance is used
        - Catastrophic: Potentially business ending event due to an inability to cover fines and other penalties and still maintain fiscal solvency
    - IC4: Level of enforcement

        - None: Relevant laws, regulations, and/or mandatory standards do not provide a compliance enforcement mechanism or there has been no enforcement to date and no indication of future enforcement
        - Inconsistent or Ad Hoc: Enforcement by the courts, regulators, and/or standards bodies have been haphazard at best
        - Reactive: Enforcement by the courts, regulators, and/or standards bodies have only been the result of complaints and/or publicly known incidents
        - Proactive: Enforcement by courts, regulators, and/or standards bodies have been the result of inspections and/or audits as well as a response to complaints and/or publicly known incidents
        - Aggressive: Similar to proactive but enforcement is performed aggressively, e.g., by applying significant budget and resources to enforcement activity and/or generally seeking maximum fines and/or other penalties
- Risk Component - Likelihood
    - Technical Risk Factor Type
        - LT1: Data processing environment
            - N/A: Not used
            - On-premise: Third-party processing is performed with the organization’s data processing facilities and resources
            - Hosted (IaaS): Third-party processing leverages an Infrastructure as a Service (IaaS) environment or similar hosted data processing environment
            - Cloud (PaaS): Third-party processing leverages a Platform as a Service (PaaS) or similar environment
            - Cloud (SaaS): Third-party processing leverages a Software as a Service (SaaS) or similar environment
        - LT2: Type of cloud environment
            - N/A: Not used
            - Private: Third-party processing only leverages private cloud services (with respect to the third party)
            - Hybrid: Third-party processing leverages a hybrid of public and private cloud services
            - Public: Third-party processing only leverages public cloud services
        - LT3: Data access approach
            - Onsite (Supervised): The third party can only access sensitive information from within the organization’s facilities and such access is supervised by the organization
            - Onsite (Unsupervised): The third party can only access sensitive information from within the organization’s facilities, but such access is unsupervised
            - Offsite (No Remote Access): The third party cannot access the organization’s sensitive information remotely but is provided the information for use outside of the organization’s facilities (e.g., on a disk, one-time FTP)

    - Remote Access (Individual): The organization provides the third party remote access to sensitive information but only through individual user accounts
    - Remote Access (Group): The organization provides the third party remote access to sensitive information through group or shared user accounts
- LT4: Data storage location
    - None: The third party does not store data
    - Onsite (Controlled): The third party can only store sensitive information onsite and such storage is controlled and supervised by the organization
    - Onsite (Uncontrolled): The third party can store sensitive information onsite and such storage is neither controlled nor supervised by the organization
    - Off Site (Single Location): The third party can store sensitive information offsite but may only do so at a single location (e.g., a data center)
    - Offsite (Multiple Locations): The third party can store sensitive information offsite in multiple locations (e.g., via cloud-based data storage)
- LT5: Use of subcontractors, if any
    - None: The third party does not intend to use subcontractors to process the organization’s sensitive information
    - One-level Subcontractor: The third party intends to use one or more subcontractors to process the organization’s sensitive information but does not allow its subcontractors to also subcontract such services
    - Multiple Levels or Not Specified: The third party intends to use one or more subcontractors to process the organization’s sensitive information and either allows its subcontractors to also subcontract such services or does not explicitly prohibit such activity

Appendix B – HITRUST CSF Rapid Assessment

The HITRUST Rapid Assessment was designed to support a quick evaluation of an organization's security posture by selecting specific 'good security hygiene' practices from the HITRUST CSF that are suitable for any organization regardless of size or industry. The requirements are based on HITRUST's prior work on small business security and privacy programs and assessment along with recommended security practices from NIST and the U.S. Small Business Administration. In addition to supporting the third-party qualification process for all sizes and types of organizations, the HITRUST Rapid Assessment requirements may also be used to support HITRUST verification of small, low risk businesses meeting SBA size criteria after the HITRUST CSF v10 release expected in Q4 2020. The Rapid Assessment's 78 requirements, current as of the date of publication, are provided in Table *10*.

Table 10. HITRUST CSF Rapid Assessment Requirements

Topical Area	Req. #	Plain Language Requirement
Information Protection Program	IP1	**SOMEONE WITH AUTHORITY IS RESPONSIBLE FOR INFORMATION SECURITY.** The business owner or executive management (e.g., a CEO, president or partner) formally assigns a senior or management-level individual the responsibility and the authority necessary to protect its information and manage related risk from its use.
	IP2	**INFORMATION SECURITY POLICIES AND SUPPORTING PROCEDURES ARE IN PLACE, REVIEWED REGULARLY, AND UPDATED AS NEEDED.** The organization formally documents, reviews and periodically updates its information security policy and makes these documents readily available to the workforce.
	IP3	**USERS KNOW ABOUT THE INFORMATION SECURITY PROGRAM.** The information security program is communicated to and understood by the workforce.
	IP4	**PERIODIC SECURITY PROGRAM REVIEWS ARE CONDUCTED BY QUALIFIED PROFESSIONALS.** The organization's information security program is reviewed regularly by qualified individuals (e.g., experienced professionals with information security and privacy expertise) who are independent of the area under review (e.g., third-party consultants or internal audit).
Endpoint Protection	EP1	**ANTI-VIRUS AND ANTI-SPYWARE SOFTWARE IS USED TO SCAN EVERYTHING FOR MALWARE.** Anti-virus and anti-spyware software are installed and operating on all desktops and laptops, and the software is updated whenever updates are available.
	EP2	**USERS CAN'T INSTALL SOFTWARE.** The organization does not allow users to install unauthorized software, including data and software from an external network. When discovered, such unauthorized software is removed.
Portable Media Security	PM1	**THE ORGANIZATION INVENTORIES ITS PORTABLE MEDIA BEFORE USE, AND SUCH USE IS LIMITED.** All portable media such as USB drives are included in the organization's equipment inventory (registered) before being issued for use. The type of portable (removable) media workforce members can use, e.g., USB drives, is limited to that which (1) can be safeguarded (e.g., encrypted) and (2) is necessary for valid business purposes.
	PM2	**MEDIA WITH SENSITIVE INFORMATION IS PROTECTED UNTIL DESTROYED.** Until destroyed or sanitized, media with sensitive data (e.g., hard drives, USB drives, CD-ROMs) is encrypted and physically protected until it is destroyed or sanitized using an approved method, e.g., pulping, shredding or burning, appropriate to the media type. Any media with sensitive information not encrypted is identified and the organization has a valid, documented rationale for not doing so.
Mobile Device Security	MD1	**PORTABLE COMPUTERS AND HANDHELDS ARE PROTECTED UNTIL SECURELY DISPOSED.** Mobile computing devices (e.g. laptops, tablets) must be (1) protected physically (e.g., locking cables, locked storage) and logically, including access controls (e.g., user ID and password), cryptography (e.g., encryption) and virus protection (e.g., anti-virus software); and (2) the data is backed up (e.g., onto DVD-ROM, USB drives, or central network storage).
	MD2	**COMPUTERS THAT CAN CONNECT DIRECTLY TO THE INTERNET HAVE THEIR OWN FIREWALL PROTECTION.** Personal firewall software is required on all computing devices (most often mobile devices like laptops) that connect to the organization's network or systems, but which can also be connected to the Internet (e.g., from home or a commercial hotspot like a coffee shop or hotel).
	MD3	**COMPUTERS AND OTHER DEVICES WITH SENSITIVE INFORMATION ARE LOCKED UP WHEN NO ONE IS AROUND.** Equipment with sensitive information is physically protected when left unattended, e.g., in a locked container or behind a locked door.
	MD4	**ONLY TRUSTED MOBILE DEVICES ARE USED TO ACCESS THE OFFICE NETWORK AND COMPUTERS.** Users are only allowed to connect equipment that meets organizational requirements for configuration (e.g., specific hardware and software specifications and settings) and usage (e.g., ability to process PII) to the organization's networks, systems and other information resources.
	MD5	**SOFTWARE CANNOT RUN WITHOUT THE USER ALLOWING IT.** Mobile devices cannot run software code (e.g., installation of software or modification of software settings) unless specifically allowed by the user at that time (e.g., by notifying the user and requesting whether or not to allow the program to run.)
	MD6	**USERS ROUTINELY WORKING AWAY FROM THE OFFICE USE THE SAME SECURITY SAFEGUARDS AS THE OFFICE.** The organization formally manages teleworking to ensure the same protections afforded to sensitive information as those provided for office workers. This includes the use of individual rather than shared or group accounts, securely configured organization-owned computers and devices (e.g., with firewalls and antivirus software, routinely patched applications), securely configured home networks (e.g., WPA or stronger encryption), secure remote connections (e.g., SSL/TLS), and other safeguards.
	MD7	**USERS GIVE BACK THEIR EQUIPMENT WHEN NO LONGER ALLOWED TO WORK AWAY FROM THE OFFICE.** Teleworkers return equipment and their access is revoked when teleworking is no longer authorized.

Topical Area	Req. #	Plain Language Requirement
Wireless Security	WS1	**WIRELESS DEFAULT SETTINGS ARE CHANGED.** The “out of the box” default configuration settings of wireless access points are changed before they are installed.
	WS2	**WPA OR STRONGER WIRELESS ENCRYPTION IS USED.** Wireless access points use Wireless Access Protection (WPA) or stronger encryption.
Configuration Management	CM1	**SYSTEM SECURITY SETTINGS ARE CHECKED REGULARLY.** Technical checks of a system’s security configuration (e.g., disallowed ports or services, allowed functionality) are performed at least annually by someone knowledgeable of the system and/or with an automated tool designed to inspect and report on the system’s configuration.
	CM2	**TECHNICAL SECURITY PROBLEMS ARE FIXED.** If any problems are discovered with a system’s security configuration (e.g., an unauthorized service is available in the system), the cause of the problem is identified, investigated and corrected.
	CM3	**SOFTWARE AND HARDWARE THE VENDOR NO LONGER SUPPORTS IS REPLACED.** Obsolete systems or system components that cannot be updated or patched are identified and plans are in place to replace them.
Vulnerability Management	VM1	**A COMPLETE INFORMATION ASSET INVENTORY IS DOCUMENTED AND UPDATED WHEN CHANGES OCCUR.** A complete inventory of the organization’s information assets (e.g., hardware, software) is current (typically conducted or reviewed annually) and includes the relative importance of the asset (e.g., low, medium, high), type or classification of the asset (e.g., PCI, PII, sensitive), format (e.g., paper, SAN, CD-ROM), location (e.g., room, building), backup information (e.g., backup medium, format and location), licensing information (including vendor, version number, current state of deployment), the individual in the organization responsible for the asset (e.g., the system or application owner), and its business value (e.g., low, medium, high or estimated dollar value).
	VM2	**EQUIPMENT AND APPLICATIONS ARE CONFIGURED SECURELY.** Systems are configured securely, e.g., with only necessary, secure services, ports and protocols enabled for use. The use of any non-secure services, ports and protocols or any non-secure configuration settings should be documented, and their use approved by management. Additional security functionality unique to the application should also be enabled, e.g., configure email systems to tag email received from outside the organization as ‘EXTERNAL’ and configure Web browsers to blacklist prohibited Websites.
	VM3	**VULNERABILITIES ARE FIXED.** The organization actively looks for technical vulnerabilities (e.g., vulnerable system configurations or software defects) and corrects them based on the risks posed to the organization.
Network Protection	NP1	**THE OFFICE NETWORK IS PROTECTED.** Firewalls are used to separate and control traffic between the organization’s network and other networks, such as the Internet as well as between wireless networks and any other network, including the organization’s “wired” network and any publicly accessible systems. Implement an intrusion prevention system and configure (IPS) and configure the system to update automatically.
	NP2	**ONLY APPROVED DEVICES ARE ALLOWED TO CONNECT TO THE NETWORK.** The organization identifies and authenticates equipment and devices that connect to the network before allowing the connection to ensure that unauthorized devices can be identified and not allowed to connect to the network. Disable network ports that are not in use.
	NP3	**ESTABLISH AND ENFORCE NETWORK TRAFFIC RESTRICTIONS:** Segment the organization’s network and establish/enforce network traffic restrictions. All outgoing network traffic to the Internet must pass through at least one (1) application layer filtering proxy server or Web filter. Do not allow inbound Internet access into your organization’s network, protect public-facing Web-applications with application-level firewalls and non-Web-based applications with a network-based firewall specific to the application type, or consider using a secure third-party vendor as host. Remote user access is also restricted to a managed access control point.
Transmission Protection	TP1	**SECURITY IS ADDRESSED BEFORE ALLOWING THE ELECTRONIC EXCHANGE OF SENSITIVE INFORMATION.** The organization ensures information systems can exchange information securely before allowing its use for that purpose.
	TP2	**SENSITIVE INFORMATION IS ALWAYS ENCRYPTED DURING TRANSMISSION.** Sensitive information transmitted using end-user messaging technologies (e.g., email, chat) is always encrypted from “end-to-end” (essentially from one user’s device to another) unless the complete transmission path is protected (e.g., by a physically protected distribution system, or PDS).
	TP3	**ADDITIONAL SAFEGUARDS ARE PROVIDED FOR VERY SENSITIVE MESSAGES.** Stronger safeguards (e.g., read receipts, electronic aka digital signatures, avoiding the use of ‘free’ or ‘consumer’ email systems that are inherently nonsecure) are used to protect certain electronic messages (e.g., emails containing PII).
Password Management	PW1	**PASSWORDS SHOULD NOT BE EASILY GUESSABLE.** Passwords not easily guessable, commonly used or expected (e.g., uses words, telephone numbers, and/or anniversary or birth dates), and should not be one that is known to have been compromised. The organization should allow user-selection of long passwords and passphrases, including spaces and all printable characters. Group, shared or generic passwords are not used.
	PW2	**PASSWORDS ARE CHANGED PERIODICALLY AND AS NEEDED TO ENSURE GOOD SECURITY.** User passwords shall be changed whenever there is any indication of possible system or password compromise. Default passwords should be changed immediately and temporary passwords (e.g., for new users or password resets) should be changed immediately upon first use.
	PW3	**PASSWORDS SHOULD NOT BE REUSED.** Users should not reuse any of their recent six passwords.
Access Control	AC1	**SECURITY REQUIREMENTS ARE DEFINED FOR EACH INDIVIDUAL APPLICATION OR INFORMATION SYSTEM.** To determine users’ access to information and associated privileges, the security requirements for the applications or information systems that contain that information must also be determined.
	AC2	**ACCESS TO INFORMATION IS BASED ON ITS SENSITIVITY AND BUSINESS REQUIREMENTS FOR ITS USE.** The organization should determine who will need access to information and how they will be provided access. Access, whether on paper or electronically, is based on its sensitivity/classification and limited to documented business requirements for its use. For example, consider restricting access to information assets (such as IoT) with potentially high impact in the event of a compromise to only those individuals that work with the assets and confining third-parties to separate network(s) or allowing them to only connect to the primary network through tightly controlled interfaces.
	AC3	**ACCESS IS STANDARDIZED.** The organization specifies the same type of access for individuals with common job roles. Access should be different for these types of individuals only if they perform some duties that are different.

Topical Area	Req. #	Plain Language Requirement
Access Control	AC4	**USER ACCOUNTS ARE FORMALLY MANAGED.** User accounts are managed and monitored by the organization from the time the account is requested and created to the time the account is disabled and/or removed, including any modifications required due to changes in the user's business responsibilities.
	AC5	**EVERY USER HAS THEIR OWN INDIVIDUAL ACCOUNT.** User (account) IDs must be unique to a specific individual and are never reissued to another user (e.g., when John Doe leaves the organization, his user ID, j.doe, is not subsequently issued to a new employee, Jane Doe).
	AC6	**USER PRIVILEGES ARE MANAGED AND DOCUMENTED.** User access to specific types of information is formally authorized by management and reviewed and updated as needed to ensure the minimum necessary access required for job performance.
	AC7	**USERS ARE ONLY GIVEN ACCESS TO INFORMATION WHEN NEEDED.** User privileges are only provided when and as necessary for business purposes consistent with their job role.
	AC8	**USERS ADHERE TO A CLEAR DESK, CLEAR SCREEN POLICY.** Paper and other physical media with sensitive information is placed behind "lock and key" and not left out in the open when not being used. Sensitive documents are removed from printers, copiers and fax machines immediately after they are produced. Computers and mobile devices have password-protected screensavers and requires the user to reestablish access using appropriate identification and authentication procedures.
	AC9	**REMOTE ACCESS IS PROVIDED SECURELY.** At least two of three factors (something you know, e.g., a password; something you have, e.g., an RSA token; and something you are, e.g., a fingerprint) is used to authenticate users connecting to office resources from a remote location (e.g., their home or while on travel).
	AC10	**USERS ACCEPT TERMS AND CONDITIONS WHEN ACCESSING SYSTEMS.** Users are presented with a suitable warning notice during a secure log-on process when accessing the organization's network or a network resource (e.g., a computer or application), and the network.
	AC11	**SUPER USER ACCOUNTS ARE NOT USED FOR NORMAL EVERYDAY BUSINESS.** "Super users" (e.g., system administrators or anyone that has "elevated" privileges compared to a typical user) must have a separate, standard or "normal" user account in which to perform ALL their regular everyday business.
	AC12	**USERS READ AND SIGN ACCEPTABLE USE AGREEMENTS BEFORE BEING ALLOWED ACCESS TO SENSITIVE INFORMATION.** Agreements for the acceptable use of the organization's information resources (e.g., networks, systems, computers) are read and signed by all workforce members before being allowed access to resources, annually thereafter, and whenever the rules are changed.
	AC13	**MORE THAN ONE PERSON IS REQUIRED TO COMPLETE RISKY TASKS.** More than one person is required to complete a task that could result in the risk of unauthorized or unintentional modification of information (e.g., to prevent fraudulent financial transactions).
Audit Logging and Monitoring	LM1	**AUDIT RECORDS INCLUDE WHO DID WHAT AND WHEN.** Audit records include the unique user ID, unique data subject ID, function performed, and date/time an event occurred (e.g., login, read or write was performed). Audit records for privileged users (e.g., administrators or other users with elevated privileges compared to a typical user) include the success/failure of events, time the event occurred, the account involved, the processes involved, and additional information about the event.
	LM2	**AUTOMATED DETECTION AND ALERTING TOOLS ARE USED.** Information systems containing sensitive information are provided with automated tools for monitoring system events, detecting attacks and analyzing logs and audit trails. Monitoring is conducted at strategic and ad hoc locations to track specific transactions and the impact of security changes to information systems to allow the identification of all access or modification of any given record by any given system user over a given period.
	LM3	**PHYSICAL ACCESS LOGS ARE REVIEWED.** The organization reviews physical access logs weekly and upon occurrence of security incidents involving physical security.
Personnel Security	PS1	**EMPLOYEES RECEIVE SECURITY AND PRIVACY TRAINING.** Security training is provided to employees as part of their "onboarding" process within 60 days of hire and as part of an ongoing awareness program specific to their roles, which includes why it's important, what it covers, and what they must do (e.g., logon procedures), what they can and cannot do (e.g., use of software, installation of unauthorized software) with the organization's information resources (e.g., networks, systems, and facilities), and what will happen if they do something wrong (e.g., information on the disciplinary process). Training programs should also focus on current threats to organizational information and how best to deal with these threats, including but not limited to such good security hygiene practices such as not giving out personal or business information; not responding to 'pop-ups' or email attachments and Weblinks from unverified sources (e.g., phishing); not using personal computers, mobile devices, and accounts for business purposes (and vice versa); and simply being aware of the people you work with and around to help spot unusual activity.
	PS2	**THE OFFICE DOCUMENTS WHAT IS ACCEPTABLE AND UNACCEPTABLE USE OF ITS INFORMATION ASSETS.** Documented rules of behavior describe users' responsibilities and acceptable use of information resources (e.g., networks, computers, systems, and information). Acceptable use agreements address, at a minimum, rules of behavior for email, Internet, mobile devices, social media, and facilities/grounds.
	PS3	**USERS UNDERSTAND THEY MAY BE DISCIPLINED IF THEY VIOLATE THE ACCEPTABLE USE AGREEMENT.** Workforce members receive written notification (e.g., when they sign an acceptable use agreement) that violations of information protection policy will result in specific disciplinary action (e.g., verbal or written warnings, termination).
	PS4	**CONDUCT BACKGROUND CHECKS.** The organization establishes screening requirements for all employees, contractors and third-party users based on the risk associated with their job positions and conducts background checks accordingly.
Third-Party Assurance	TA1	**SECURITY AND PRIVACY REQUIREMENTS FOR THIRD PARTY ACCESS TO SENSITIVE INFORMATION ARE IMPLEMENTED BEFORE ANY AGREEMENTS ARE SIGNED AND ACCESS IS GRANTED.** Security requirements for third-party access (e.g., consultants, vendors) to the organization's information resources (e.g., networks, systems, and computers) are identified and implemented before a contractual relationship with the third party is established AND before access to sensitive information is granted. All security requirements related to the organization's work with an external party are identified in the contractual agreement with the external party.
	TA2	**THIRD PARTIES UNDERSTAND THEIR OBLIGATIONS AND AGREE TO PROTECT SENSITIVE INFORMATION.** External parties (e.g., customers, clients, business partners) acknowledge and accept their information protection roles and responsibilities and any liabilities they incur when accessing, processing, communicating, or managing the organization's information and information assets. This is typically done by ensuring all third-party obligations to protect the organization's sensitive information are documented in a third-party agreement, and all third parties sign the agreement acknowledging their obligations.

Topical Area	Req. #	Plain Language Requirement
Third-Party Assurance	TA3	**SATISFACTORY ASSURANCES ARE OBTAINED BEFORE DISCLOSING SENSITIVE INFORMATION TO A THIRD PARTY.** An organization may disclose sensitive information (e.g., PII, PCI) to a business partner or other third party and may allow the creation, receipt, maintenance or transmittal of sensitive information on its behalf, if the organization obtains satisfactory, written assurances. It should also ensure a valid agreement is in place that addresses the proper management/oversight of the business partner or other third party and specifies applicable requirements (e.g., around use, further disclosure, and the implementation of reasonable and appropriate safeguards).
	TA4	**SERVICE ARRANGEMENTS ARE SUPPORTED BY A FORMAL AGREEMENT.** Service Level Agreements (SLAs) or contracts with an agreed service arrangement address liability, service definitions, security controls, and other aspects of services management. An SLA may supplement a standard third-party agreement (contract) or replace such an agreement if all third-party assurance requirements are adequately addressed.
Incident Management	IM1	**EVERYONE KNOWS TO WHOM THEY SHOULD REPORT SECURITY ISSUES.** Everyone knows to whom they should report possible information security issues, and that individual provides a meaningful response in a reasonable timeframe. There are no negative consequences to anyone for reporting a possible security issue.
	IM2	**THE ORGANIZATION KNOWS HOW TO RESPOND TO A POTENTIAL BREACH.** A formal process exists for responding to reports of possible information security issues, including how soon the organization should respond, how issues should be escalated to management when needed, how to determine if a breach has occurred and the date/time the breach can be considered "discovered."
	IM3	**BREACHES ARE REPORTED AS REQUIRED BY RELEVANT LAW OR REGULATION.** Legal and regulatory requirements for responding to and reporting a breach of sensitive information (e.g., personal data or personally identifiable information, PII) are met.
Business Continuity and Disaster Recovery	BC1	**INFORMATION AND SOFTWARE IS BACKED-UP.** The organization makes backup copies of information and software and these backups are tested regularly along with system restoration procedures. The level of backups for each system is formally specified and documented including the specific data that will be backed up, how often, and how long the backups will be kept in accordance with relevant contractual, legal, regulatory and business requirements.
	BC2	**BACKUPS ARE ENCRYPTED AND KEPT SAFE FROM THEFT OR PHYSICAL DAMAGE IN A SAFE LOCATION.** Backups of sensitive information (e.g., PII, PCI) are encrypted, kept in a safe, secure location sufficiently separate from where the data is used and protected from physical and environmental hazards.
	BC3	**CONTINUITY PLANNING ADDRESSES SPECIFIC INFORMATION SECURITY AND OTHER RELATED REQUIREMENTS.** To continue business operations in the event of an emergency or system outage, it's important to understand what information, systems and processes are critical and ensure that staff, clients and visitors remain safe and that information, equipment and facilities are protected. Part of this protection strategy includes the consideration and possible purchase of cyber insurance.
	BC4	**CONTINUITY PLANNING INCLUDES RECOVERY AND RESTORATION REQUIREMENTS.** To continue business operations in the event of an emergency or system outage, organizations should formally document their continuity plans and procedures for continuity, periodically test at least a portion of the plans and procedures, and update them as needed (e.g., when systems and workflows change, personnel are replaced, and problems with the plans/procedures are discovered).
	BC5	**SENSITIVE INFORMATION CAN BE OBTAINED DURING AN EMERGENCY OR SYSTEM OUTAGE.** It's important for organizations to have access to critical information when business operations continue during an emergency or system outage. This includes staff access as well as access by third parties based on collaborative or reciprocal agreements.
	BC6	**SYSTEMS CAN BE RESTORED WITHOUT COMPROMISING INFORMATION SECURITY.** It's important to maintain the security and privacy of sensitive information during reduced operations as well as during the process of recovering systems and restoring normal operations.
Risk Management	RM1	**RISK ASSESSMENTS ARE PERFORMED.** The organization conducts comprehensive risk assessments that cover the entirety of the HITRUST CSF controls specified by their organizational, system and regulatory risk factors to identify their security risks from all reasonably anticipated threats. Risk assessments are performed regularly, when something significant in their environment changes (e.g., new systems, mergers & acquisitions), and management reviews the results of these assessments at least once every year.
	RM2	**POTENTIAL IMPACTS FROM AN UNAUTHORIZED USE OR DISCLOSURE OF SENSITIVE INFORMATION ARE ADDRESSED.** All sensitive information is classified appropriately, which provides for specific limitations on its disclosure internal and external to the organization. Actions are taken to reduce the impact of an unauthorized use or disclosure of sensitive information to the office, its business partners, and the individuals affected (e.g., through the purchase of cyber insurance, indemnification in contracts, and other impact reducing controls such as incident response).
Physical and Environmental Security	PE1	**ACCESS TO SENSITIVE AREAS IS FORMALLY MANAGED.** Areas where sensitive information (e.g., PII or Payment Card Information, PCI) is stored or processed is restricted to individuals specifically authorized by the organization. The organization maintains a list of individuals authorized to access restricted areas (where sensitive information is stored or processed), issues credentials for access (e.g., access codes or badges), updates the credentials and access list no less than quarterly, and removes individuals from the access list when access is no longer required. Access to these areas by third party support personnel is authorized only when needed for as long as needed and monitored for as long as the third party has access.
	PE2	**VISITOR ACCESS TO SENSITIVE AREAS IS RECORDED AND SUPERVISED.** Visitor access to sensitive areas (e.g., where sensitive information is stored or processed) is recorded with enough information to identity the visitor and the purpose and duration of the visit. All visitors are supervised by someone with authorized access to the area visited unless the visitor's access was approved by the facility's operational manager (e.g., the data center manager, business unit manager) before the date and time of the visit.
	PE3	**ACCESS TO SENSITIVE EQUIPMENT IS RESTRICTED.** Sensitive equipment (e.g., wireless access points, handheld devices, and networking/communications hardware) is protected from unauthorized physical access (e.g., by locked equipment closets, rooms, and alarmed facilities).
	PE4	**MAINTENANCE IS PERFORMED ACCORDING TO MANUFACTURER RECOMMENDATIONS.** System maintenance is performed as required by the manufacturer, e.g., in a recommended service schedule, or applicable insurance policies (e.g., cyber insurance).

Topical Area	Req. #	Plain Language Requirement
Physical and Environmental Security	PE5	**ACCESS BY MAINTENANCE PERSONNEL IS FORMALLY MANAGED.** Only authorized personnel are allowed un-escorted access to equipment to perform maintenance activities, and escorts assigned to monitor non-authorized maintenance personnel must be authorized access and technically competent to ensure only required maintenance is performed and the equipment remains in a secure state. Information resources are protected based on whether maintenance is performed locally (onsite) or remotely through a secure connection. Remote maintenance is only performed when authorized in writing, and such remote maintenance is monitored and controlled. Ensure equipment removed for off-site maintenance is sanitized.
	PE6	**MAINTENANCE CAUSES MINIMAL DISRUPTION TO BUSINESS PROCESSES.** Maintenance downtime is less than the amount of time allowed by the organization—typically defined in a security, contingency or business continuity plan as the Recovery Time Objective, or RTO—to ensure minimal disruption to business processes.
	PE7	**APPROVED METHODS ARE USED WHEN EQUIPMENT OR MEDIA WITH SENSITIVE INFORMATION IS SANITIZED OR DESTROYED.** Sensitive information is sanitized, i.e., unrecoverable using standard laboratory methods, or destroyed, i.e., unrecoverable and the media unusable, when no longer needed for business, legal or regulatory purposes using generally accepted 'best practices.'
	PE8	**EQUIPMENT IS PROTECTED FROM PHYSICAL AND ENVIRONMENTAL HAZARDS.** Policies and procedures are in place to address physical and environmental hazards (e.g., through policy, standards, guidelines, and procedures) and address specific protections for electrical (e.g., surge protectors, uninterruptible power supplies, backup generators), fire (e.g., fire alarms, fire extinguishers), and water hazards (e.g., location of IT facilities, routing of water pipes).
Data Protection and Privacy	DP1	**INFORMATION IS FORMALLY MANAGED.** Guidelines are issued by the organization on the ownership, classification, retention, storage, handling and disposal of ALL records and information.
	DP2	**SENSITIVE RECORDS ARE RETAINED AND PROTECTED AS REQUIRED BY APPLICABLE LAW AND COMPANY POLICY.** The organization produces and maintains a retention schedule for sensitive information/ records and retains the information/records as required.
	DP3	**THE SECURITY AND PRIVACY OF SENSITIVE INFORMATION IS PROTECTED.** The confidentiality and integrity of sensitive information processed/retained by the office is protected using an appropriate encryption method wherever it is stored. If not encrypted, the organization has a documented, approved rationale for not doing so.

Appendix C – Impact and Priority Codes

HITRUST's Rapid Assessment requirements, current as of the date of publication, are provided in Table *10*.

Impact Codes

Impact is described using five rating levels or codes: Very Low (1), Low (2), Moderate (3), High (4) and Very High (5). Since HITRUST CSF control maturity scores are provided on a 100-point scale, we similarly compute impact (I) as a function of the impact code (IC) as follows:

$$Impact=I=(IC-1)\ \ (25)$$

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

Table *11* provides the HITRUST impact codes for all 135 CSF security controls:[76]

Table 11. HITRUST CSF Control Impact Codes

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

The numbers are intended to provide a starting point for assignment of relative risk for risk reporting and corrective action planning based on relative maturity of the controls as determined by a HITRUST CSF Assessment. Organizations may adjust the impact ratings/ codes for internal purposes based on the status of other controls in the environment or the sensitivity and/or criticality of the information assets in scope.

Priority Codes

Priority codes indicate a relative order of priority (sequencing) for control implementation or remediation by identifying controls upon which other controls depend:

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

Table *12* provides the HITRUST priority codes for all 135 CSF security controls:[77]

Table 12. HITRUST CSF Priority Codes

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

Whether these priority codes will be useful to an organization will depend on the specific deficiencies requiring CAPs, and organizations must fully understand the requirements to understand their dependencies.

CAP prioritization will also depend on other factors unique to the organization, which cannot be addressed by a risk management framework (RMF) like the HITRUST Approach or NIST RMF. Examples include available operational and capital budget, budget planning processes, architecture and infrastructure constraints, and even organizational culture and politics.

Endnotes

[1] When referring to 'risk' or 'inherent risk' throughout the rest of the document, we mean risk specific to information security, privacy, and compliance.

[2] Due diligence is defined here as "a reasonable person under the same circumstances would use; use of reasonable but not necessarily exhaustive efforts" (https://dictionary.findlaw.com/definition/due-diligence.html); also called reasonable diligence. Diligence may be defined as "earnest and persistent application of effort esp. as required by law." See https://dictionary.findlaw.com/legal-terms/d.html.

[3] Due care is defined here as "the care that an ordinarily reasonable and prudent person would use under the same or similar circumstances" (https://dictionary.findlaw.com/definition/due-care.html); also called ordinary care or reasonable care.

[4] Information is defined here as "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." See https://csrc.nist.gov/glossary/term/information. Not to be confused with the term 'data,' which we define here as "information in a specific representation, usually as a sequence of symbols that have meaning" or "pieces of information from which 'understandable information' is derived." See https://csrc.nist.gov/glossary/term/data.

[5] Sensitive information is defined here as "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]." Adapted from https://csrc.nist.gov/glossary/term/sensitive-information.

[6] Personal data is defined here to mean "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." A natural person may be defined as "a human being as distinguished from a person (as a corporation) created by operation of law." See https://gdpr-info.eu/art-4-gdpr/.

[7] Assurance is defined here as "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." See https://csrc.nist.gov/glossary/term/assurance.

[8] Risk is defined here as "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. [Information-related] … risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, [and] other organizations…." Adapted from https://csrc.nist.gov/glossary/term/risk.

[9] Risk management is defined here as "the program and supporting processes to manage information security risk … and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time." Adapted from https://csrc.nist.gov/glossary/term/risk-management.

[10] Compliance is defined here as "an adherence to the laws, regulations, standards, guidelines and other specifications [such as contractual obligations] relevant to an organization's business." For more information on compliance and compliance-related risk, see https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf, p. 3.

[11] A third party may be defined as "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." See https://hitrustalliance.net/content/uploads/HITRUST_Glossary_of_Terms_and_Acronyms.pdf.

[12] Defined here as the "operation or set of operations performed on [information] that can include, but is not limited to, the collection, retention [storage], logging, generation, transformation, use, disclosure, transfer and disposal of [information]." See https://csrc.nist.gov/glossary/term/Processing.

[13] For example, see https://www.cyber.nj.gov/threat-analysis/supply-chain-compromise-of-third-parties-poses-increasing-risk or https://www.sdcexec.com/risk-compliance/blog/20995547/data-security-best-practices-for-mitigating-supply-chain-risk.

[14] For example, see https://www.reedsmith.com/en/perspectives/2017/09/mitigating-third-party-data-breach-risks for a discussion around information-related risk in the supply chain or https://www.scmr.com/article/five_techniques_to_manage_supply_chain_risk for a broader discussion around managing supply chain risk.

[15] For example, see https://digitalguardian.com/blog/what-nydfs-cybersecurity-regulation-new-cybersecurity-compliance-requirement-financial for a discussion of third-party assessment requirements in NYDFS Cybersecurity Regulation (23 NYCRR 500).

[16] See https://www.researchgate.net/publication/281121552_Mitigating_Reputational_Risks_in_Supply_Chains.

[17] For example, see https://smallbiztrends.com/2019/07/supply-chain-cybersecurity.html or https://www.mckinsey.com/business-functions/risk/our-insights/managing-when-vendor-and-supplier-risk-becomes-your-own.

[18] Defined here as the "total amount and type of risk an organization is willing to pursue or retain." See https://www.iso.org/standard/44651.html.

[19] Defined here as the amount and type of risk "an organization is prepared to accept in total or more narrowly within a certain business unit, a particular risk category, or for a specific initiative." See https://ermgovernance.com/Resources/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf.

[20] Definitions of a dataset (or data set) are many and varied and often depend on the context. For example, see http://www.meloda.org/data-set-definition/, https://www.techopedia.com/definition/3348/data-set-ibm-mainframe, and https://stats.oecd.org/glossary/detail.asp?ID=542. We define dataset as a collection of data intended for one or more purposes.

[21] Metadata may be defined as "information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels)." See https://csrc.nist.gov/glossary/term/metadata.

[22] See https://www.researchgate.net/publication/327631764_How_to_create_a_data_inventory, p. 3.

[23] The metadata described in the definition for a data inventory is very similar to the type of data associated with 'data provenance.' "Data provenance documents the inputs, entities, systems, and processes that influence data of interest, in effect providing a historical record of the data and its origins." See http://siis.cse.psu.edu/provenance.html. Closely related to, if not synonymous with, 'data lineage.'

[24] See https://dictionary.cambridge.org/us/dictionary/english/data-flow-diagram.

[25] See https://ratandon.mysite.syr.edu/cis453/notes/DFD_over_Flowcharts.pdf, p. 1.

[26] Diagram adapted from https://security.ufl.edu/it-workers/risk-assessment/creating-an-information-systemdata-flow-diagram/.

[27] Defined here as a "progression of steps (tasks, events, interactions) that comprise a work process, involve two or more persons, and create or add value to the organization's activities." See http://www.businessdictionary.com/definition/workflow.html.

[28] Diagram made available from https://www.edrawsoft.com/template-logistic-management-workflow.php.

[29] See https://www.merriam-webster.com/dictionary/triage.

[30] Inherent risk is typically defined as the amount of risk that exists in the absence of controls; however, this definition is somewhat problematic as there will most likely be some level of protection applied to information in an organization. We subsequently concur with the FAIR Institute's view of inherent risk in which the prior definition is modified to reflect this notion and provide the following definition for our purposes: inherent risk is the risk that exists when the status of key controls is not taken into consideration or is otherwise unknown. For more information, see https://www.fairinstitute.org/blog/using-the-fair-model-to-measure-inherent-risk.

[31] See https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, p. 8.

[32] See https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, p. 10.

[33] Risk appetite and risk tolerance are addressed in more detail in the discussion of Qualify Step 6 – Qualification Decision.

[34] For a well-written discussion of what is and is not (e)PHI, see https://cphs.berkeley.edu/hipaa/hipaa18.html.

[35] See https://www.pcisecuritystandards.org/pci_security/glossary#C.

[36] See https://doi.org/10.6028/NIST.IR.7298r2, p. 141.

[37] See https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.

[38] For example, see https://www.ponemon.org/news-2/23.

[39] See https://www.hipaajournal.com/gao-report-hhs-improve-hipaa-oversight-ephi-security-guidance-3608/.

[40] Organizations should consider all their regulatory and other compliance obligations and not just those that are integrated as authoritative sources in the HITRUST CSF.

[41] Typically refers to compliance with relevant laws, regulations, and/or standards but could include significant private contracts obligating the organization to specific protection requirements.

[42] Requirements

[43] For example, ISO/IEC 27001, NIST Cybersecurity Framework, AICPA Trust Services Criteria.

[44] For example, HITRUST CSF, FISMA (NIST SP 800-53).

[45] For example, AICPA SOC 2.

[46] For example, NIST SP 800-18 or HITRUST CSF Assurance.

[47] Additional information on the HITRUST CSF and CSF Assurance Program is available from the HITRUST Website at https://hitrustalliance.net/downloads/.

[48] A HITRUST CSF Readiness Assessment is a HITRUST CSF Self-Assessment that is generally facilitated by a HITRUST CSF Assessor. Note: After the release of HITRUST CSF v10 planned in late 2020, small businesses that present very low inherent risk may qualify for certification based on the controls addressed in a HITRUST CSF Rapid Assessment.

[49] With

[50] Corrective Action Plan

[51] More information on the HITRUST CSF control maturity and scoring model is available from https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf.

[52] For more information on the structure of the HITRUST CSF security and privacy control framework, see https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf, pp. 8-9.

[53] The following discussion of the Scope Overview and Scope Description was derived from https://hitrustalliance.net/content/uploads/Scope-Definition-Guidance-1.pdf.

[54] For example, see https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf, pp. 9-13.

[55] For more information, see https://hitrustalliance.net/content/uploads/2016/01/Leveraging-a-Control-Based-Framework-to-Simplify-the-Risk-Analysis-Process.pdf.

[56] Tailoring is 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. See https://csrc.nist.gov/glossary/term/tailoring.

[57] 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. See https://csrc.nist.gov/glossary/term/overlay.

[58] For more information on tailoring and overlays, see https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, Ch. 3.

[59] For more information on the HITRUST assessment process, see https://hitrustalliance.net/content/uploads/2014/09/HITRUSTCSFAssessmentMethodology_2014.pdf.

[60] For more information, see https://cmmiinstitute.com/.

[61] For more information, see https://csrc.nist.gov/publications/detail/nistir/7358/final.

[62] For more information, see https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf, p. 9.

[63] A model in which the control requirements are assessed against policy, procedures, and implementation for compliance, partial compliance, or non-compliance.

[64] Small businesses, as defined by the U.S. Small Business Administration, that present very low risk may use the simplified version of the HITRUST CSF control maturity model.

[65] Requirements for participation in a formal information security continuous monitoring based, ongoing HITRUST CSF Certification program is currently under development with general availability expected in mid- to late 2020.

[66] For more information on how target and current profiles are created using the HITRUST Approach, see https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf, pp. 15-28.

[67] For more information on the requirements for CSF Certification, see https://hitrustalliance.net/documents/assurance/csf/CSFAssuranceProgramRequirements.pdf.

[68] For more information on impact and priority codes, see Appendix C.

[69] For more information on alternate controls, see https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf, pp. 34-40.

[70] For example, see https://ittoolkit.com/articles/control-project-risk.

[71] For a complete discussion of the HITRUST CSF control maturity, see https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf, pp. 15-25.

[72] Definitions for risk capacity, appetite, tolerance, and target are quoted directly from https://ermgovernance.com/Resources/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf.

[73] Definition for residual risk is quoted from https://csrc.nist.gov/glossary/term/residual-risk.

[74] For more information, see https://www.pmi.org/learning/library/understanding-risk-appetite-6296.

[75] For more information, see https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[76] Impact codes have not been developed for controls in HITRUST CSF Control Category 13 – Privacy Practices.

[77] Priority codes have not been developed for controls in HITRUST CSF Control Category 13 – Privacy Practices.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net