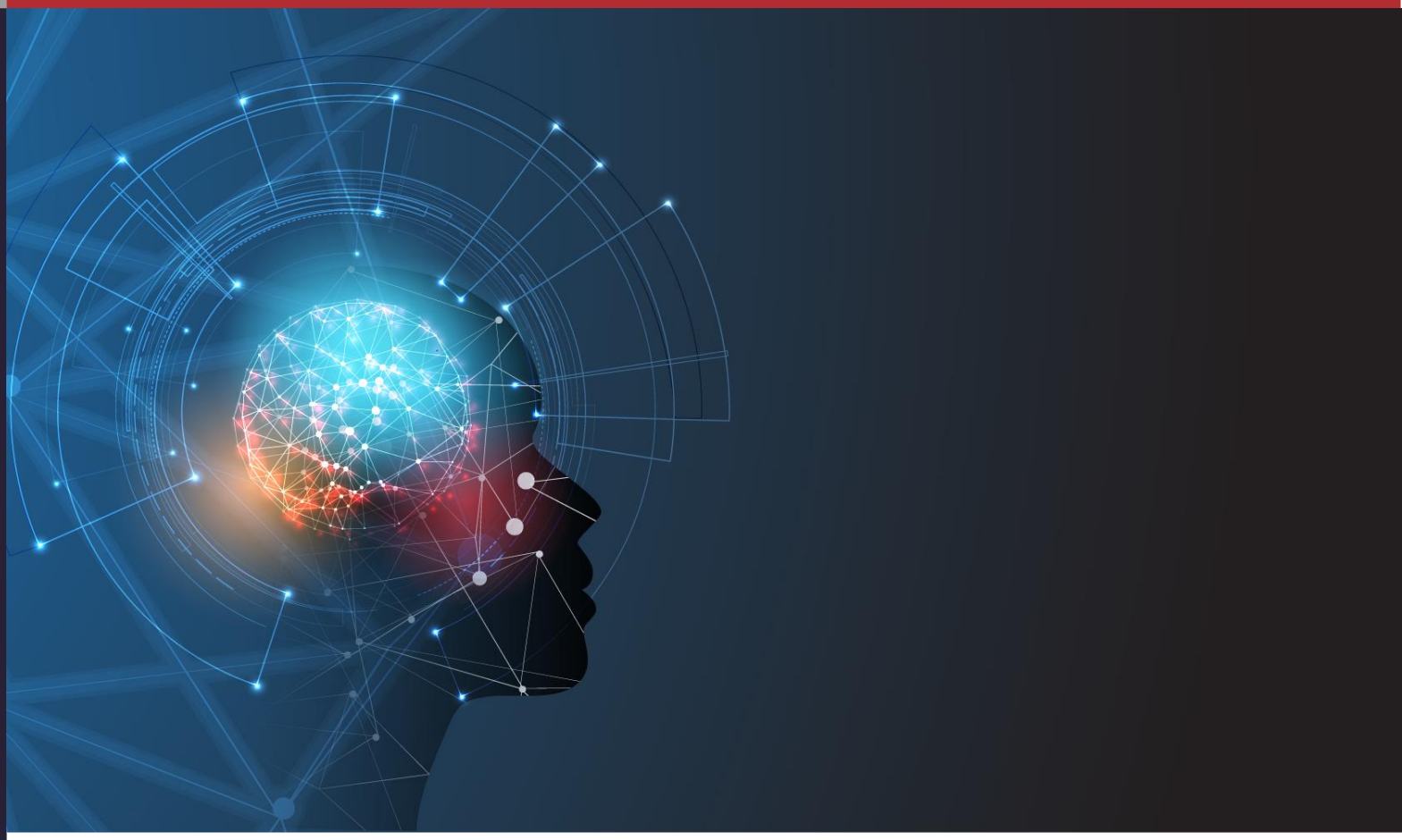
HITRUST



HITRUST Third Party Assurance (TPA) Risk Triage Methodology

A streamlined approach to assessing the inherent risk posed by a third party and selecting an appropriate assurance mechanism leveraging the HITRUST CSF and CSF Assurance Program

February 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—as organizations are seeking greater assurances from their third parties than is warranted based on risk or regulatory compliance requirements—or they are not seeking enough assurance—and organizations expose themselves to more risk than intended.

As shown in Table 1 on the following page, the HITRUST Third Party Assurance (TPA) Risk Triage Methodology provides

(1) Specific organizational, compliance and technical factors that help identify the type and amount of inherent risk
(1) 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.

The methodology can be used as the first step in an organization's third-party risk management process to quickly assess the risks inherent in the sharing of information with a particular third party and determine an appropriate assurance mechanism, thereby increasing efficiency and effectiveness of the process. Broad adoption will also significantly reduce costs for the organization as well as any third party that needs to provide assurances to multiple customers or business partners.

Table 1. Consolidated View of the HITRUST TPA Risk Triage Methodology

<table>
<tr><th>Risk Component</th><th>Risk Factor Type</th><th>Risk Factor</th><th>Risk Factor Rating</th><th>Risk Factor Type Score</th><th>Risk Comp. Score</th><th>Risk Score</th><th>Assessment Type (Based on Risk Score)</th></tr>
<tr><td rowspan="9">Impact (I)</td><td rowspan="3">Organizational (O)</td><td>IO1: Percentage of organizational data</td><td>0 – 4</td><td rowspan="3">Simple Average 0 – 4</td><td rowspan="9">High Watermark 0 – 4</td><td rowspan="10">Simple Average (Rounded UP to the Next Highest Integer) 0 - 4</td><td rowspan="10">0 – Facilitated or Remote Self-Assessment

1 – Validated Assessment w/[1] CAPs;[2] No Minimum Score

2 – Validated or Certified Assessment; Consolidated Score > 62 w/ CAPs

3 – Validated or Certified Assessment; Consolidated Score > 71 w/o[3] CAPs

4 – Validated or Certified Assessment; Consolidated Score > 87 w/ or w/o CAPs</td></tr>
<tr><td>IO2: Total amount of organizational data</td><td>0 – 4</td></tr>
<tr><td>IO3: Criticality of the business relationship</td><td>0 – 4</td></tr>
<tr><td rowspan="6">Compliance (C)</td><td>IC1: Comprehensiveness and specificity of requirements</td><td>0 – 4</td><td rowspan="4">Simple Average 0 – 4</td></tr>
<tr><td>IC2: Level of assurance required</td><td>0 – 4</td></tr>
<tr><td>IC3: Specified or observed fines and penalties</td><td>0 – 4</td></tr>
<tr><td>IC4: Level of enforcement</td><td>0 – 4</td></tr>
<tr><td rowspan="5">Likelihood (L)</td><td rowspan="5">Technical (T)</td><td>LT1: Data processing environment</td><td>0 – 4</td><td colspan="2" rowspan="5">Simple Average 0 – 4</td></tr>
<tr><td>LT2: Type of cloud environment, if used</td><td>0 – 4</td></tr>
<tr><td>LT3: Data access approach</td><td>0 – 4</td></tr>
<tr><td>LT4: Data storage location</td><td>0 – 4</td></tr>
<tr><td>LT5: Use of subcontractors</td><td>0 – 4</td></tr>
</table>

[1] With
[2] Corrective Action Plan
[3] Without

Contents

Introduction

HITRUST has been championing and delivering solutions to address the lack of a common understanding around the security and privacy controls needed to demonstrate an appropriate level of due diligence and due care for the protection of sensitive information, such as electronic Protected Health Information (ePHI) or Personally identifiable information (PII), as well as a common mechanism for providing assurances for both internal and external stakeholders around the state of an organization's information risk management and compliance program.

While HITRUST offers multiple means of providing industry various levels of assurance—such as with a self-assessment or a 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 Third Party Risk Triage Methodology, which provides a common approach that can be used across industries for efficient and effective third-party risk management. By providing a common set of risk factors that are independent of the security and privacy controls that may or may not implemented by a vendor, 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.

Figure 1. Generic Third-Party Risk Management Process Model

Third Party Risk Management (TPRM)

Third parties,[4] 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 with these third parties and how they process and potentially share this information themselves. Many organizations subsequently go to great lengths to manage their third-party risk, often through a formal management process such as the one shown in Figure 1 on the previous page.

While the actual implementation of TPRM varies from one organization to another, they will typically address each step in the generic process model 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 will provide, including documentation received from the third party (e.g., a short questionnaire about their business practices); and 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 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 into 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 current contract if a 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 assess the third party for changes in potential business risk, including information security, privacy and compliance risk.

The organization should re-enter the Initiate step 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).

[4] 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:
https://hitrustalliance.net/content/uploads/HITRUST_Glossary_of_Terms_and_Acronyms.pdf

Third Party Assurance

Third party assurance is essentially a measure of confidence that a third party will provide an appropriate level of due diligence and due care for the protection of information and individual privacy. Such assurances can take many forms, such as attestation of conformity, or some type of conformity assessment, such as a controls gap assessment against a security standard. This type of assurance is provided in step 3 of the TPRM process model when the third party is qualified to do business with the organization. A generic qualification process is depicted in Figure 2.

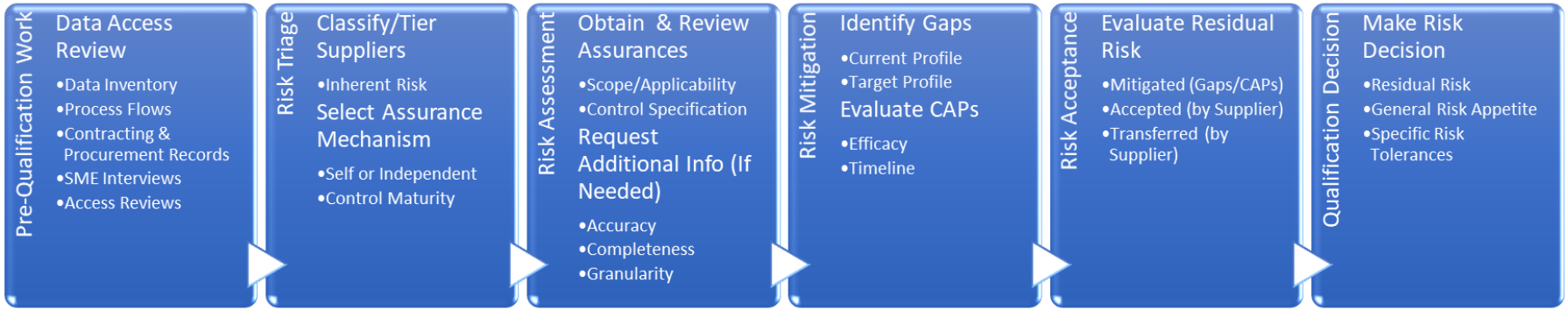


Figure 2. Generic Third-Party Qualification Process (TPRM Process Step 3 – Qualify)

The qualification process consists of six basic steps:

1. Data access is reviewed based on the information gathered in the prior step in the TPRM process model;
2. The third party is classified or tiered according to the level of inherent risk it presents based on risk factors specified by the organization;
3. 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. Any gaps in conformity are evaluated along with the third-party's corrective action plans (CAPs) to address those gaps, if any;
5. The remaining or residual risk is evaluated; and
6. Management determines if the organization is willing to accept that risk based on its general risk appetite[5] and specific risk tolerances."[6]

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

[6] Define 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: https://www.rims.org/resources/ERM/Documents/RIMS_Exploring_Risk_Appetite_Risk_Tolerance_0412.pdf

Scope

This paper addresses the first issue organizations must address in obtaining assurance, which is an inherent risk analysis methodology that may be used for initial 'triage" of third parties with respect to the risk they potentially represent to an organization, 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

The National Institute of Standards and Technology (NIST) defines risk as

> *"the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring"*[7]

and is generally computed as a function of (1) the likelihood an event will occur and (2) the probable impact should the event occur.

Inherent Risk

Inherent risk is typically defined as "the amount of risk that exists in the absence of controls," [8] however, this definition is somewhat problematic as there will most likely be some level of protection applied to information in an organization. We concur with the FAIR Institute's view of inherent risk in which the 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*.

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."[9] 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 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 with them, 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

[7] https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
[8] https://www.fairinstitute.org/blog/using-the-fair-model-to-measure-inherent-risk
[9] https://www.merriam-webster.com/dictionary/triage

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 as previously shown in *Figure 2*.

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 [emphasis added].*[10]

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."[11] We interpret this to mean that a pre-disposing 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, data hosted in certain public Cloud environments may be more likely to be compromised than data hosted by the organization on 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.

Risk Triage Approach

We define three types of factors for third party risk triage: organizational, compliance and technical.

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[12] or cardholder data[13] in particular and PII[14] or personal data[15] 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.[16]

---

[10] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, p. 8
[11] *Ibid*, p. 10

[12] For a well-written discussion of what is and is not (e)PHI, see https://cphs.berkeley.edu/hipaa/hipaa18.html
[13] https://www.pcisecuritystandards.org/pci_security/glossary#C
[14] https://doi.org/10.6028/NIST.IR.7298r2, p. 141
[15] See https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en.
[16] For example, see https://www.ponemon.org/news-2/23

Specific organizational factors addressed by the HITRUST Risk Triage 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 data expressed as the number of individual records; and
(iii) The criticality of the business relationship to the organization.

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 and subsequently influence 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,[17] and impact is subsequently not considered in the HITRUST model for these factors.

Specific compliance[18] 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 mandatory standard's protection requirements;
(ii) The specific assurance requirements of applicable regulations and mandatory standards;
(iii) The penalties specified in the regulations or mandatory standards or otherwise seen in practice; and
(iv) The level of enforcement provided by the regulatory or standards bodies.

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.

An explanation of the Factor Ratings for each Risk Factor is provided in the Addendum.

[17] https://www.hipaajournal.com/gao-report-hhs-improve-hipaa-oversight-ephi-security-guidance-3608/
[18] Organizations should consider all its regulatory and other compliance obligations and not just those that are integrated as authoritative sources in the HITRUST CSF

Table 2 on the next page 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.

An explanation of the Factor Ratings for each Risk Factor is provided in the Addendum.

Table 2. 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[19]	IC1: Comprehensiveness and specificity of requirements	None	General, Non-specific	General Framework-based Req'ts[20,21]	Prescriptive Framework-based Req'ts[22]	N/A	Simple Average	
		IC2: Level of assurance required	None	Self-Assessment / Attestation	Risk-based (Determined by the Org.)	Specific Reporting Format[23]	Specific Ctrl Requirement Framework[24]		
		IC3: Specified or observed fines 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		

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

[20] Requirements

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

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

[23] For example, AICPA SOC 2

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

Computing Inherent Risk

As shown in An explanation of the Factor Ratings for each Risk Factor is provided in the Addendum.

Table 2 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 3.

Table 3. 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 3.

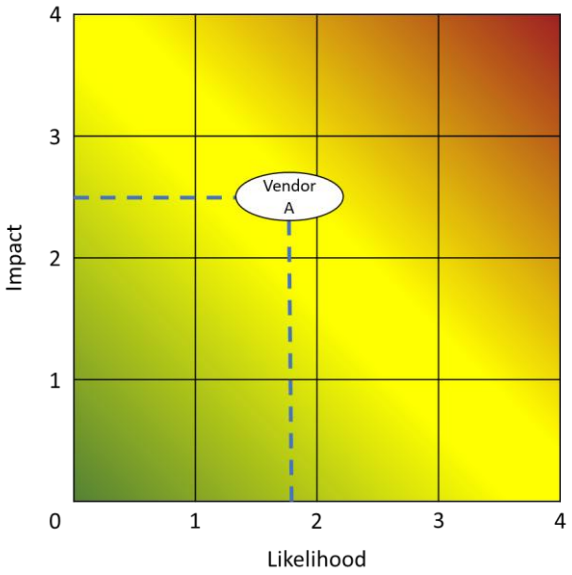


Figure 3. Example Heatmap (Vendor A)

The inherent risk posed by a particular 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 4.

Table 4. HITRUST-recommended Assurance Approaches[25]

Inherent Risk	Assurance Approach
0 – Very Low	Facilitated/Remote Self-assessment[26]
1 – Low	Validated with CAPS, no minimum score
2 – Moderate	Validated or Certified ≥ 62[27] with CAPs
3 – High	Certified ≥ 71 with no CAPs
4 – Very High	Certified ≥ 87 with or without CAPs

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

[26] Small businesses may opt for CSFBASICs certification if they present very low risk to the organization

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

EXAMPLE: Vendor A

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

$$= ROUND(UP)\left[\frac{1.8\ x\ 2.5}{4}\right]$$

$$= ROUND(UP)\,[1.125]$$

$$= 2$$

In this example, Vendor A would be asked to obtain a HITRUST CSF validated assessment and obtain a minimum score of 3- with corrective action plans (CAPs). With a limited number of CAPs, the organization could become HITRUST CSF certified as well.

Conclusion

Based on the HITRUST CSF and CSF Assurance Program, the HITRUST TPA Risk Triage Methodology provides a common approach that can be used across industries for efficient and effective third party risk management. By providing a common set of risk factors that are independent of the security and privacy controls that may or may not implemented by a vendor, 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 is intended to provide a minimally acceptable level of assurance; however, organizations have flexibility 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.

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.

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

Addendum

Explanation of Risk Factor Ratings from An explanation of the Factor Ratings for each Risk Factor is provided in the Addendum.

Table 2

- 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 nor 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 Req'ts: 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 Req'ts: Relevant laws, regulations and/or mandatory standards prescribe a comprehensive and prescriptive framework such as the CMS IS ARS, MARS-E or 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
      - On-premise: Third party processing is performed with the organization's data processing facilities and resources
      - N/A: Not used
      - 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
      - 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 access 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 organization remote access to sensitive information but only through individual user accounts
      - Remote Access (Group): The organization provides the organization 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
    - N/A: Not used
    - 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
    - N/A: Not used
    - 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