HITRUST®

Solving the Third-Party Risk Management Problem

Given evolving cyber threats; expanding international, federal, and state privacy and security compliance requirements; growing risks associated with data management; new business models that require access to more data by more parties; and the increasing, devastating impacts from data breaches, there is broad recognition that information risk and compliance management programs are crucial in today's business environment and that appropriate assurances about these programs must be demonstrated.

The HITRUST Approach

While breaches related to third parties continue to increase, the state of third-party risk management has remained relatively stagnant. To address the need for a comprehensive and practical approach to third-party risk management, HITRUST created and integrated a unique combination of methodologies, technologies, and services that can be leveraged incrementally, allowing organizations to only implement what they need when they need it.

Organizations must not only provide assurances to internal stakeholders such as internal audit, executive management, and corporate boards aboutthe state of their information risk and compliance programs, but also to external stakeholders such as regulators, business partners, customers, and other third parties.

A strong information risk and compliance program can also be an important market differentiator, as it is a key deciding factor when evaluating third-party relationships, equity investments, and strategic partnerships.

The Need for Third-Party Risk Management

To remain competitive, an organization must actively manage its supply chain, including the exchange of information that allows entities to coordinate and control the flow of materials, goods, and services up and down the supply chain. The quality of this information—or the lack thereof—can impact virtually every aspect of one's ability to coordinate one's supply chain activities. Subsequently, third parties must ensure relevant information is correct, available, and—for sensitive business information and personal data—confidential. And organizations receiving information must ensure that third parties in their own supply chains are engaging a formal third-party risk management (TPRM) program.

This is because third parties can introduce significant business risk to an organization simply due to the type and amount of information shared by an organization and how they process and potentially share this information amongst themselves.

Risk management within supply chains is one of the most significant challenges facing every organization by virtue of the fact that all organizations are a member of at least one and more probably, multiple supply chains[1].

Incidents of third-party breaches impacting organizations are numerous. Examples range from the well-publicized 2013 hacking of Target's corporate network through a heating, ventilation, and air conditioning (HVAC) vendor, which resulted in an $18.5M multi-state settlement and at least $202M spent on legal fees and other breach-related costs, to the more recent 2017 breach of Sabre Hospitality Solutions' SynXis Central Reservations system, impacting numerous downstream customers such as Google, Hard Rock Hotels and Casinos, Loews Hotels, the Four Seasons, and Trump Hotels.[2]

The typical 'flow down' of contractual requirements to downstream organizations in the supply chain is a necessary but insufficient part of third-party risk management.[3] Simply assuming third parties like vendors are protecting one's information assets can be disastrous. Organizations should perform an appropriate level of due diligence before sharing information with third parties consistent with the risk they present based on the sensitivity and amount of information being shared as well as the purpose for which the information is shared.

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, such as a need to comply with the Health Insurance Portability and Accountability Act (HIPAA) or the New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500).

Organizations may still be held financially accountable by customers and upstream partners for the failure of downstream third parties to protect the data they receive. For example, financial services regulators are increasingly holding institutions accountable for 'misdeeds' that occur in their supply chain, including third parties that process customer financial information (such as payment card data) which subsequently pose numerous security- and privacy-related risks.

And, while not as well understood as other supply chain risks, an organization's brand and reputation may also be affected by negative events in its supply chain. This is because the third party that is the source of the breach may not have as much brand recognition or the same financial wherewithal as the organization that receives its products or services, which makes it a bigger 'target' for journalists, regulators, and other interested stakeholders. In the end, the owner of the information also owns the risk.

The State of Third-Party Risk Management

While cyber-related incidents continue to increase, the state of third-party risk management has remained relatively stagnant. Organizations struggle to keep pace despite about 41% of respondents in a recent survey stating they have "mature practices with regard to assessing and managing critical third parties."[4] And that doesn't even address the management of moderate- to high-risk third parties.

The TPRM market is also replete with traditional TPRM solutions, the underlying methodologies for which are rudimentary and address basic TPRM functionality such as managing third-party contact and contract information and collecting and presenting third-party risk information. This may include assessment of risk based on proprietary questionnaires or, more recently, the use of publicly accessible information.

While the limitations of standardized questionnaires are well understood, the use of 'cybersecurity risk scorecards' or reputational assessment services is relatively new and not as well known. Based on publicly accessible information rather than an in-depth review of internal controls, the usefulness of the approach is limited and arguably unique for each organization's environment.

Security professionals have some concerns, however, about whether a single score can capture all the nuances of a security program, whether score issuers are comparing the same security metrics to produce a score, and if companies can even be compared to one another given that no two networks are the same.[5]

It is further recognized that each scorecard vendor uses a proprietary and often 'secret' approach to collecting data as well as proprietary analytics when computing the scores or ratings. In addition, any changes to these proprietary approaches can impact an organization's score, sometimes dramatically, when there has been no discernible change in their actual security posture.[6]

This general lack of a common, consistent approach to determining what information risk assurances should be provided and maintained when an organization shares sensitive information with a third party has subsequently created significant inefficiencies in the marketplace when organizations seek greater assurances from their third parties than is warranted (based on risk or regulatory compliance requirements) or when organizations do not seek enough assurance and expose themselves to more risk than intended (based on their tolerance or capacity to accept risk).

The HITRUST Approach to TPRM

Leveraging our extensive experience and knowledge of information risk management and assurance, the HITRUST Third-Party Risk Management Methodology[7] provides organizations a transparent, standardized approach to TPRM that specifies a level of assurance appropriate to the information security, privacy, and compliance risk a third party inherently poses to an organization.

The HITRUST Methodology provides organizations:

- An Inherent Risk Questionnaire (IRQ) that allows organizations to determine or 'triage' the inherent risk a third party poses and select a target assessment that provides a level of assurance appropriate to the risk;
- An iterative series of HITRUST CSF Assessments designed to support progressively increasing assurance until the requisite level can be achieved by the third party, including a Rapid Assessment that can quickly gauge a third party's basic security posture;
- A HITRUST CSF Trust Score that helps improve the reliability of self-attested assessments and supports an organization's evaluation of the overall trustworthiness of a third party.

In addition to being fully supported by the HITRUST CSF and CSF Assurance Program, which provides the best in class framework-based risk analysis, tailorable control specification, maturity-based control assessment, and multi-stakeholder reporting, the HITRUST TPRM Methodology is also supported and fully operationalized by the HITRUST Assessment XChange™ ("the XChange").[8]

The XChange is specifically designed to be an extension of an organization's TPRM program by facilitating the onboarding of organizations and third parties, automating third-party risk triage and assessment management, and providing key support services such as outreach and engagement with third parties and monthly status reporting.

Risk Triage and the Inherent Risk Questionnaire

While other TPRM approaches tend to tier third parties based on limited or even tangential information related to information risk, e.g., amount of annual spend for the third party's goods or services, HITRUST provides a more relevant and comprehensive approach by triaging third parties based on multiple factors that estimate the inherent risk posed simply by sharing information for processing. Examples of these factors include the percentage and total amount of organizational data shared, criticality of the business relationship to the organization, various aspects of related compliance obligations such as the level of assurance required and potential fines and penalties, and the type of data processing and storage employed.

The HITRUST Assessment XChange automates the collection of this information by and for Participating Organizations (POs) through the Inherent Risk Questionnaire. The XChange allows questions to be parsed and distributed to the appropriate data owner, whether internal to the PO or external with the third party. Once the information is collected, the XChange will automatically compute the third party's inherent risk score, determine if additional assurances are required, and recommend an appropriate HITRUST assessment if one is needed. POs also have the option to adjust these recommendations within the XChange based on their overall risk appetite or specific risk tolerances.

The result is a simple, but rigorous approach that is also more efficient and effective than others in the marketplace, and the types of assessments it specifies are generally more appropriate for the level of risk each third party represents.

HITRUST CSF Assessments and Iterative Assurance

The next stage in the iterative assurance process is generally a HITRUST CSF Readiness Assessment. Although self-attested, this assessment is based on a full specification of security and privacy controls appropriate to the third party's risk factors and employs the full HITRUST CSF control maturity model to provide a higher level of 'rely-ability.' Subsequent assessments in the iterative process are HITRUST CSF Validated Assessments, which continue to raise the scoring requirements until the target level of assurance is obtained.

And to help ensure the HITRUST CSF Readiness Assessment provides the best level of assurance possible for a self-attested assessment, the HITRUST Assessment XChange will compute a HITRUST Trust Score[9] based on a comparison with the first HITRUST CSF Validated Assessment performed. Intended to help POs evaluate a third party's overall trustworthiness, the Trust Score also encourages third parties to be more accurate and truthful when conducting the HITRUST CSF Readiness Assessment.

The HITRUST Assessment XChange also uses each of these 'interim' assessments as a 'qualifying gate' for the PO's TPRM process. Until the target assessment recommended in risk triage is completed, the XChange requires the PO to evaluate the third party's security posture based on each interim assessment and—based on the amount of residual risk presented—recommend whether to continue the iterative assurance process or discontinue the business relationship.

One of the many advantages of the HITRUST CSF Assurance-based approach is the ability to leverage existing assessments to satisfy requests from multiple customers, reducing the redundancy or allowing existing assessments to be converted to a higher assurance level without duplicating entry. By leveraging the XChange, POs can gain insight into the existence and scope of assessments already performed by their third parties which they may not have otherwise known existed, subsequently allowing them to reallocate their already limited time and resources to those third parties that pose higher risk to the organization.

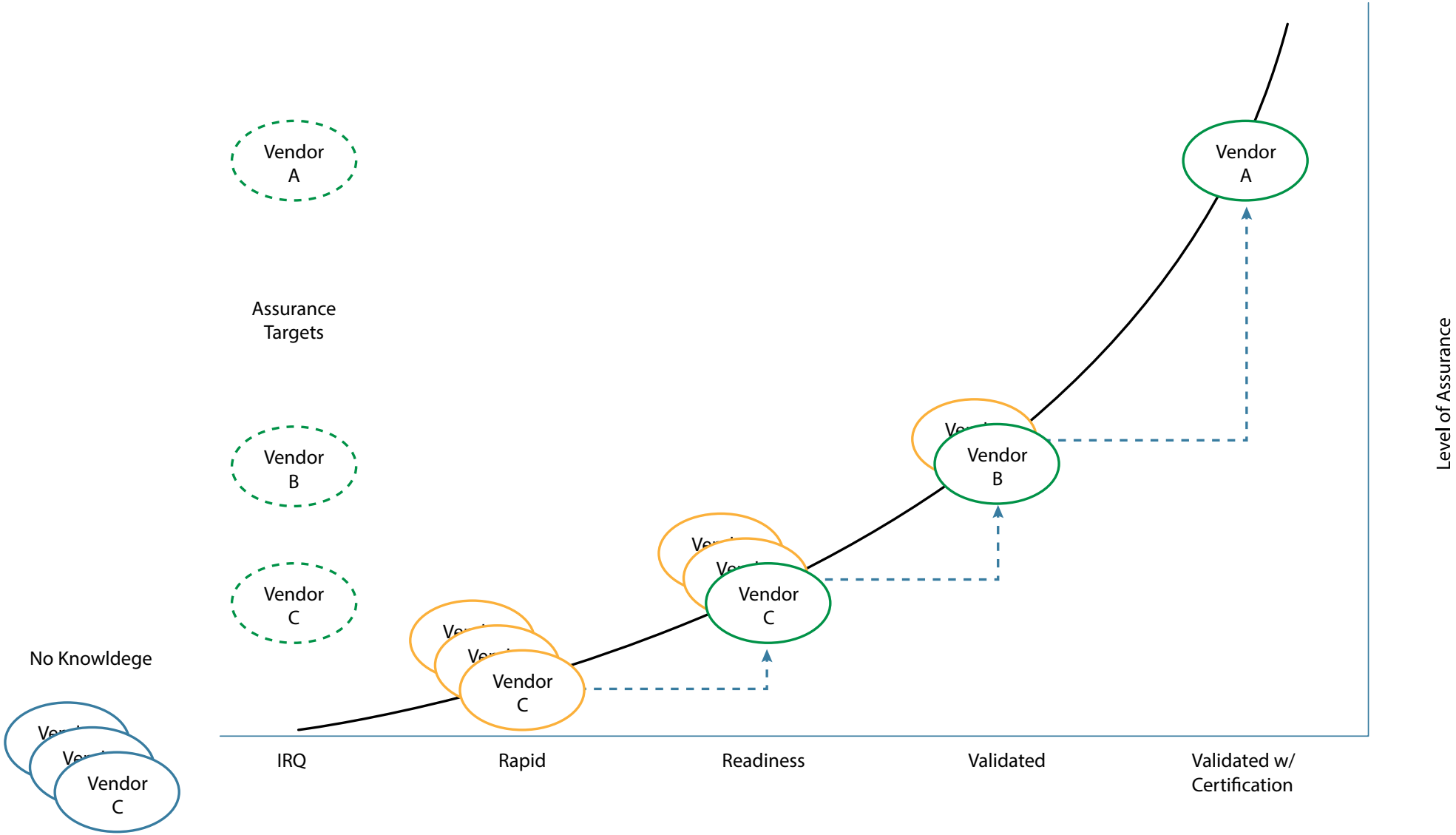
The HITRUST Assessment XChange supports four general types of assessments that provide increasing levels of assurance based on the results of the Inherent Risk Questionnaire.

- HITRUST CSF Rapid Assessment – This self-attested assessment is based on a limited set of 'good security hygiene' requirements derived from the HITRUST CSF, which are assessed using a simplified version[10] of the HITRUST CSF control maturity model. As the name suggests, the Rapid Assessment is used to quickly gauge a third party's security posture, generally within weeks if not days of a PO's request, and nominally serves as the first iterative step in the PO's TPRM process.
- HITRUST CSF Readiness Assessment – Full set of control requirements tailored to the required scope and assessed by the third party using the standard version of the HITRUST CSF control maturity model.[11] No minimum score or corrective action plans (CAPs) are required.
- HITRUST CSF Validated Assessment – Full set of control requirements tailored to the required scope and assessed by a HITRUST Authorized External Assessor using the standard version of the HITRUST CSF control maturity model. No minimum score and CAPs are allowed.
- HITRUST CSF Validated Assessment with Certification – Full set of control requirements tailored to the required scope, assessed by a HITRUST Authorized External Assessor using the standard version of the HITRUST CSF control maturity model, and assessment scores meet HITRUST CSF Certification criteria, at a minimum. Variants of this assessment may include the specification of higher overall scores as well as higher scores for targeted areas, such as access control.

Organizations may also adjust recommended levels of assurance within the HITRUST Assessment XChange (e.g., minimum scores for specific HITRUST CSF Categories, Objectives, Controls, or Control Requirements)[12] to address organizational risk tolerances for specific activities (e.g., outsourcing) or areas of concern (e.g., access control). For example, the risk triage model recommends a HITRUST CSF Validated Assessment with a minimum overall maturity score of 62 for third parties that present a moderate level of inherent risk. However, organizations with a low tolerance for risk presented by subcontractors of a third party or around privileged user access may decide to override this recommendation within the HITRUST Assessment XChange so that all related control requirements must be fully implemented with a minimum score of 75.

While not taking advantage of all the benefits of the HITRUST TPRM Methodology, organizations are also free to leverage the components of HITRUST's comprehensive toolkit available in the HITRUST Assessment XChange to address their specific TPRM requirements. For example, some organizations may wish to leverage the Rapid Assessment for third parties in a broader risk pool or a specific category of third parties to address specific operational needs and subsequently not require these organizations to complete an IRQ.

The figure below depicts the relationship between the various assessments used in the iterative assessment process and the level of assurance they provide. No knowledge of the third party's inherent risk or the controls they may or may not have implemented is assumed (blue ovals), and the target assurance levels ('dashed' green ovals) are produced solely on the information obtained in the Inherent Risk Questionnaire. Third parties then progress through an iterative series of assessments (yellow ovals) until the requisite level of assurance (green ovals) is obtained.



Additional TPRM Support

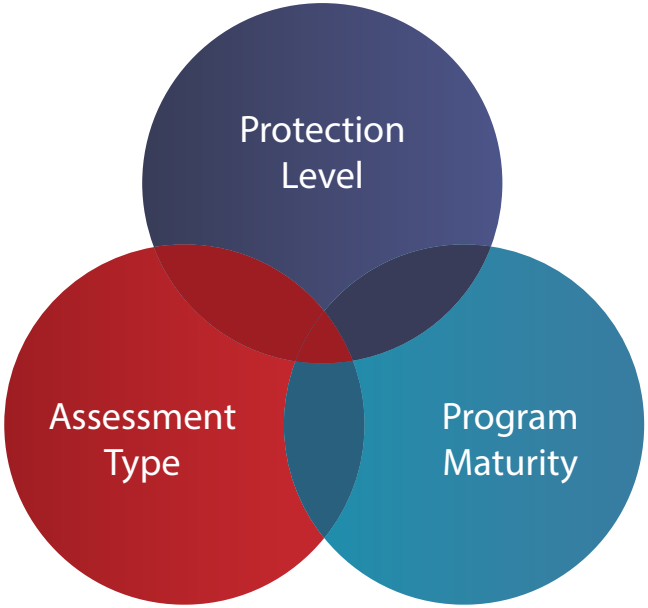
The HITRUST Assessment XChange team also provides additional 'value added' services such as assistance with providing portal training, creation of user accounts and third-party profiles, managing third-party lists, and customizing the Inherent Risk Questionnaire, if needed. In addition, the HITRUST Assessment XChange supports outreach to the third party, facilitates the transmittal and completion of Inherent Risk Questionnaires and HITRUST CSF Rapid Assessments, and monitors general third-party performance including progress towards completing corrective action plans.

Benefits

The HITRUST Assessment XChange provides organizations a simple, open approach to managing third-party risk efficiently and effectively. Unlike other TPRM services, the XChange triages an organization's third parties for the amount of risk inherent to a specific business relationship. This allows organizations to identify an appropriate level of assurance based on a small amount of information that can be readily known.

By leveraging the HITRUST CSF, the XChange allows organizations to specify a reasonable and appropriate set of security and privacy controls that provide an industry-acceptable level of due diligence for the protection of sensitive information. And by leveraging the HITRUST CSF Assurance Program, the XChange allows organizations to specify the type of assessment, the level of independence required, and the maturity that must be demonstrated by the assessment in order to obtain the requisite level of assurance.

The HITRUST Assessment XChange also reduces the need and scope of internal resources required to implement and manage an organization's TPRM program by transferring costs to its third parties. Third parties can see a reduction in cost as well by utilizing HITRUST's *Assess Once, Report Many*™ approach, leveraging the same assessment for multiple stakeholders, even those with disparate reporting requirements.



The HITRUST Approach

HITRUST clearly delivers a comprehensive and unique set of capabilities and services designed to fit into, augment, compliment, or replace various aspects of an organization's current TPRM program. The HITRUST Approach can also be leveraged incrementally, allowing organizations to only use the capabilities and services they need and which are appropriate for their situation.

To learn more about the HITRUST Approach, go to https://hitrustalliance.net/the-hitrust-approach/.

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.

About the HITRUST Assessment XChange

Founded in 2017, HITRUST Assessment Exchange LLC is a wholly-owned subsidiary of HITRUST Services Corp. HITRUST Assessment Exchange LLC ("the XChange") is designed to provide an extension of an organization's third-party risk management program. The HITRUST XChange Manager platform streamlines and simplifies the process of managing and maintaining risk assessment and compliance information from third parties. With the XChange, organizations will maintain constant visibility into their third parties' assessment statuses before, during, and after the assessment process, ensuring organizations effectively manage and understand risk across the third-party ecosystem.

Endnotes

1 Brindley C. (2004). Supply Chain Risk. New York: Routledge, p. 4.

2 NJCCIC (2017, 20 Jul). Supply Chain: Compromise of Third Parties Poses Increasing Risk. Available from https://www.cyber.nj.gov/threat-analysis/

3 For a broader discussion around managing supply chain risk, see, e.g., Trowbridge, M. (2017, 2 Nov). Five Techniques to Manage Supply Chain Risk. In Supply Chain Management Review. Available from https://www.scmr.com/article/five_techniques_to_manage_supply_chain_risk.

4 Protiviti (2019). Insights / 2019 Vendor Risk Management Survey. Available from https://www.protiviti.com/US-en/insights/vendor-risk-management.

5 CSO Online (2016, Aug 4) What's in a security score? Available from https://www.csoonline.com/article/3103293/what-s-in-a-security-score.html.

6 Ibid.

7 Cline, B. (2019). 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. Available from https://hitrustalliance.net/content/uploads/TPRM-Methodology.pdf.

8 HITRUST Assessment XChange (2020). Available from https://hitrustax.com/.

9 HITRUST (2019, 11 Nov). Understanding and Improving the Role of Self-Assessments in Third-Party Risk Management. Available from https://blog.hitrustalliance.net/understanding-improving-role-self-assessments-third-party-risk-management/2/.

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

11 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.

12 For more information on the structure of the HITRUST CSF security and privacy control framework, see Cline, B. (2018, Feb). Risk Analysis Guide for HITRUST Organizations & Assessors, pp. 8-9. Available from https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf.