HITRUST®

HITRUST® Third-Party Risk Management (TPRM) Methodology and HITRUST Assessment XChange™ Enhancements FAQs

FAQs are specific to this webinar. Visit our General FAQs here.

Q: In regard to the HITRUST Trust Score, how would a company that rates itself lower than the validated scores be trust rated?

A: The HITRUST Trust Score is intended to address organizations that overestimate their security postures, regardless of the reason, and is subsequently only based on standard errors of the mean for the left tail of the normal distribution. Organizations that underestimate their security posture will receive the same 'perfect' Trust Score as those that estimate it correctly. For more information on the HITRUST Trust Score, see our blog, *Understanding and Improving the Role of Self Assessments in Third-Party Risk Management*.

Q: How, if at all, is a HITRUST CSF® Assessment much different than a Standardized Information Gathering (SIG) Assessment?

A: HITRUST CSF control requirements are specified for an organization via a framework-based risk analysis and additional tailoring provided by organizational, system, and regulatory risk factors. SIG requirements are not. The assessment of HITRUST CSF control requirements is also done according to a rigorous maturity-based assessment and scoring approach by independent assessor firms that meet stringent quality criteria. SIG assessments are not.

Q: How does your third-party risk management (TPRM) methodology/offering compare to TPRM companies which provide information based on passive monitoring (for example, BitSight)?

A: Rather than employ traditional means of assessment and certification of an organization's information protection program and then sharing the results of such assessments with external stakeholders, some organizations have moved to cybersecurity risk scorecards, or reputational assessment services, which are based on publicly accessible information – what a cyber attacker can see – rather than an in-depth review of internal controls. While useful, such an approach is limited (similar to a narrowly-scoped external penetration test) and is arguably unique for each organization's network.

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

It's further recognized that each scorecard vendor uses a proprietary approach to collecting data as well as proprietary analytics when computing the scores or ratings. In addition to the challenges inherent in their opacity, any changes to these proprietary approaches can change an organization's score, sometimes dramatically, when there has been no discernible change in their actual security posture. This is because the type of evidence collected for these scorecards is circumstantial and statements made about the actual state of the organization's security posture must be inferred rather than directly observed.

Subsequently, while security scorecards based on publicly accessible information can help inform an organization's understanding of its cyber risk, boards and other key stakeholders must recognize the inherent limits of these scores and draw correspondingly limited conclusions regarding a program's effectiveness. Simply put, security scorecards cannot replace the level of assurance provided by a thorough assessment of an organization's information protection program, including its overall approach to risk and risk management as well as detailed reviews of its privacy and security controls.

Q: Our company has our own process for responding to assessment requests. How do we officially opt out of this process so that our customers do not lose time requesting our assessments through the HITRUST Assessment XChange ("the XChange")?

A: A vendor cannot officially opt out of the XChange; vendors should notify their customers of their own internal processes. The customer is then responsible for eliminating those organizations from the list of vendors provided to the XChange.

Q: If an organization is already using a tool to manage third-party risk assessment data, can the HITRUST XChange Manager ("the XChange Manager") platform complement and/or integrate with the organization's existing tool?

A: Yes, the HITRUST Assessment XChange Manager platform does have an open API which organizations can utilize to integrate the XChange Manager platform into other tool(s).

Q: Is there a sample Inherent Risk Questionnaire available for review?

A: The proposed questions to be included in the HITRUST Inherent Risk Questionnaire are included in Appendix A of the whitepaper, *HITRUST Third-Party Risk Management (TPRM) Methodology: The Qualification Process*.

Q: What third-party assurance documentation do the HITRUST MyCSF® and XChange Manager portals have to ensure the exchange of information is done securely?

A: HITRUST and the XChange take the security and privacy of our clients very seriously; the HITRUST MyCSF and XChange Manager platforms have been purposefully built with multiple measures in place to safeguard your organization's sensitive data. For more information, please contact sales@hitrustalliance.net.