HITRUST ASSESSMENT XCHANGE®

Customer FAQs

Q: How do we notify our third parties that they will be managed by the HITRUST Assessment XChange® (the XChange)?
A: Before an XChange Onboarding Specialist reaches out to your third parties, a memo will be sent directly from your organization to the third parties that the XChange will be responsible for managing on your organization's behalf. This memo will serve to notify your third parties that they will soon be contacted by an Onboarding Specialist to communicate requirements on your organizations' behalf.

Q: How are uncooperative third parties handled? (i.e., The third party does not believe the XChange is an extension of the customer, refuses to comply, does not want to share their full report, etc.)
A: When an Onboarding Specialist is met with a third party who questions the validity of the relationship between your organization and the XChange, we start by referencing the memo that was sent out by your organization. In instances where the third party refuses to communicate with us, we contact your organization and ask how you would like us to proceed. These same steps would be taken in instances where third parties are asking for a change in timeframe requirements, including extensions or changes in due dates.

Q: What value does the XChange provide if a third party is not contractually obligated to undergo a HITRUST Assessment?
A: Although a third party may not be contractually obligated to undergo a HITRUST Assessment, they are required to provide adequate information to customers to evaluate the effectiveness of their information privacy and security controls. By requesting that a third party participate in the XChange, your organization is not mandating a new requirement, simply utilizing a more efficient process to obtain the information. An Onboarding Specialist will educate your third parties on the XChange process and the benefits of fulfilling the request, as well as highlight the key benefits of the program, including the "Assess Once, Report Many™" aspect, which allows third parties to address multiple customer requests with one assessment and report.

Q: What information do you need from us as the customer, what role do we play in the process, and what are the expectations?
A: The XChange will need a list of third parties, including details such as the third-party organization's name, address, company website and/or Tax Employer Identification Number (EIN), a valid point of contact's information, and requirement details for each third party. In instances where some of this information may not be available, we work with the customer on a one-off basis. We expect the customer to review and agree upon the terms within the Participation Agreement, provide an initial estimate of when the XChange should expect to receive the list, review and red line all communications between the Onboarding Specialists and third parties in advance, including scripts and third-party memos/letters, establish monthly checkpoint meetings, and ideally copy your assigned Onboarding Specialist when third-party memos/letters are sent out announcing the launch of the program.

Q: How does the XChange ensure that the scope of the report aligns with our needs/expectations?
A: When the Onboarding Specialist reaches out to the third party, they ask whether the organization has an existing HITRUST report and if the third party has an existing report, the Onboarding Specialist will verify that the scope is in line with your organization's requested scope; if it is not, the Onboarding Specialist will inform them that they'll need to complete a new HITRUST assessment with the appropriate scope and reach out to the client with that status update. Should the client like to view the currently held report despite inaccurate scoping for the purposes of identifying overlapping applicable controls, the XChange has the ability to facilitate the delivery of that report, dependent upon the third party's willingness to share that information.

Q: Will details on Corrective Action Plans (CAPs) be included within the report delivered by the XChange, and will periodic updates as to the status of those CAPs be delivered over time?
A: Yes, every report delivered by the XChange will include all CAPs; this data can also be sent electronically as API data elements. Third parties will provide yearly updates concerning CAPs, at a minimum, as assessed entities are required to provide HITRUST with progress updates at the one-year mark after achieving Certification. Should the customer desire more frequent updates on CAP statuses, the XChange will reach out to the third party on an agreed-upon schedule to obtain that data and deliver those status updates back to your organization.

Q: How does our organization know the third parties managed by the XChange are making progress on their HITRUST CSF Assessment(s)?

A: By utilizing the XChange as an extension of your Third-Party Risk Management (TPRM) program, your organization will be provided with reporting updates at an agreed-upon frequency as to the status of the progress being made on requests submitted to the XChange.

Q: What is the Inherent Risk Questionnaire (IRQ)?

A: A new questionnaire to support the risk triage process by assessing the inherent risk within a business relationship and suggesting the appropriate level of assurance.

The questionnaire is comprised of default questions from a HITRUST-managed library. The questionnaire can then be customized by your organization by adding proprietary questions of your their own. The questionnaire is customized and managed directly through the XChange Manager portal. The XChange Manager portal will automatically create an Assessment Report Request (ARR) and recommended assessment type based on the IRQ responses. Your organization also has the ability to review the risk score and determine the level of assurance and next steps for the third party.

Upon request, a sample report is available for review.

Q: What is the HITRUST CSF Rapid Assessment?

A: A new, "pre-qualifying" self-attested assessment that includes a subset of the most critical controls required for HITRUST CSF Certification, more specifically, controls that will give your organization a quick view into the security posture of a third party and can be answered in a minimal amount of time. Your organization has the ability to create customized templates for the various types of risk profiles of your third parties.

The HITRUST CSF Rapid Assessment will be at no cost to the third party, and the responses will be retained so that the data can be re-used by the third party to respond to other levels of assurance of identical scope.

Upon request, a sample report is available for review.

Q: What is the value of the HITRUST TPRM Methodology?

A: The HITRUST TPRM Methodology solves the challenges organizations face today of overcoming inconsistencies when seeking assurances from their third parties by incorporating greater oversight early in the third party selection process in support of informed decision-making, determining an acceptable level of risk, and reducing the likelihood of vulnerabilities being interjected into an organization's environment.

Q: What is the HITRUST Trust Score?

A: A new measure that compares the results of a HITRUST CSF Readiness Assessment with those of a HITRUST CSF Validated Assessment of identical scope, generated later in the qualification process to help encourage accurate self-assessments. The Trust Score will be implemented through the XChange Manager platform. The criteria will be maintained by a HITRUST- dictated algorithm, and the rating would be disclosed to both your organization as well as the third party.

Q: Is there a way to only view pertinent sections of a third party's vendors HITRUST CSF Report?

A: The XChange Manager platform allows for your organization to tailor the report information that you would like to receive through the portal. Filter options include only summary related information such as the assessment type, the assessment's scope, Corrective Action Plans (CAPs), etc. Your organization always has the ability to view third-party reports in their entirety if you desire that level of granularity.

Q: Is there an API available through the HITRUST Assessment XChange? What are the functionalities and limitations associated with the API?

A: The XChange has an open API associated with the HITRUST Assessment XChange Manager platform. Your organization can leverage our robust API to integrate the XChange Manager platform into your own GRC or VRM tools.

Q: Is there a limit on the type and number of questions that can be added to the Inherent Risk Questionnaire?

A: The IRQ is pre-loaded with the minimum number of questions to drive the risk score based on third-party responses. Your organization has the ability the add up to ninety-nine (99) of your own customized questions to the IRQ, as long as they align to the objective of obtaining indicators of risk.

Q: Does my organization need to require a third party to complete an IRQ if we already know the level of assurance we want to receive from our third party?

A: Although the IRQ is the recommend approach for all third parties submitted to the XChange, your organization has the ability to determine whether or not a third party receives an IRQ. A few examples of when an IRQ can be utilized are onboarding due diligence for new third parties, or a stopgap for an active third party while a customer awaits a higher level of assurance.

Q: What determines the amount of time to complete an Inherent Risk Questionnaire or Rapid Assessment?

A: The IRQ and Rapid Assessment are designed to be requests that a third party can respond to in an expedited manner. The response time is dependent on the third party and complexity. The fact that neither requires any type of third-party validation inherently allows both to be completed am accelerated timeframe that is determined by your organization.