HITRUST ASSESSMENT XCHANGE®

HITRUST Assessment XChange™ (The XChange) Use Cases

Inherent Risk Questionnaire Use Cases:

1. When the Inherent Risk Profile of a third party is unknown, (such as a potential new third party being introduced into an organization's environment through the RFP process, on-boarding process, etc.), and an organization needs to assimilate a risk profile for this third party in order to determine the appropriate Level of Assurance that should be requested.

2. A tier has already been assigned to a third party based upon risk, and an organization wants to validate or challenge the current tier and Inherent Risk Profile of the third party against a different metric or methodology, (such as HITRUST Risk Triage), to determine if the current tier and assessment type being requested aligns the Risk Profile and recommended Level of Assurance to HITRUST or the HITRUST Assessment XChange. This validation also helps determine if what is currently being requested is sufficient, or is too much or too little.

3. Compare an organization's understanding of the Inherent Risk Factors relative to a third-party relationship with that of the third party by routing the Inherent Risk Questionnaire questions both internally within an organization and externally to the third party to test the "alignment" of understanding and expectations between an organization and the third party. This helps test and validate the understanding of both internal stakeholders and external third parties relative to the services being contracted.

4. To obtain additional data relative to an organization's third parties that they may not have today, by gaining information from executing an IRQ, including Exposure Score, vendor responses to customized questions, and more.

HITRUST Basic, Current-state (bC) Assessment Use Cases:

1. The Inherent Risk for a third party is low and therefore requesting a comprehensive assessment like a HITRUST i1 or r2 Validated Assessment does not make business sense for the third party, and is considered over-kill, or is too "expensive" or too time-intensive for a third party to complete.

2. When a third party has another type of HITRUST Assessment "In Process" but an organization does not want or cannot wait for that Assessment to be completed and needs some more immediate Level of Assurance from the third party.

3. When a third party has a completed a HITRUST Assessment, but the scope does not fully align with the scope needed by an organization. A bC Assessment can be used as a 'Stop Gap' in the interim while the third party alters the scope or completes a new Assessment with the proper scope for an organization.

4. In instances where an organization may not know the security and privacy posture of a third party, (such as a potential new third party being introduced into an organization's environment, going through an RFP process, or on-boarding process, etc.), but there is a need to assimilate a Level of Assurance for the organization to determine the third party's security and privacy posture.

5. In an emergency, when your organization needs to quickly gain updated assurance(s) in a specific domain, from a third party or third parties.

6. As a fit gap analysis to determine if an organization will engage an existing third party for 'new' services, not currently being utilized because the third party does not have assurances over the new service.