What is the HITRUST Assessment XChange Inherent Risk Questionnaire?
HITRUST Assessment XChange Inherent Risk Questionnaire

Inherent Risk Questionnaire (IRQ) is a questionnaire designed to support the HITRUST Risk Triage Model that is part of the HITRUST Third Party Risk Management Program. The IRQ facilitates assessing the inherent risk associated with a third-party business relationship and determines a suggested appropriate level of assurance to be requested from a third-party based on the risk the relationship presents to the organization. The IRQ is an automated tool that is leveraged through the HITRUST Assessment XChange (the XChange).
What is a HITRUST Assessment XChange Inherent Risk Questionnaire?

The **Inherent Risk Questionnaire** is customizable and delivered through the XChange Manager portal.

- A tool that will enable an organization to properly assess the inherent risk of its entire third-party network
- Pre-loaded with 12 questions designed to gather inherent risk information
- HITRUST CSF Assessment types are recommended based on risk score
- Ability for a customer to add its own custom questions to the questionnaire
- Customer has the ability to override the recommended level of assurance

Note: This sample is a mockup for demonstration purposes only. Not an actual Inherent Risk Questionnaire.
The Inherent Risk Questionnaire at-a-Glance

This view of the Inherent Risk Questionnaire within the XChange Manager portal displays the customer’s ability to assign questions internally or to a third-party.

Both the customer and the third-party may need to respond to ensure both parties agree on the nature of the business relationship.

The view also demonstrates the customer’s ability to add custom questions.

Note: This sample is a mockup for demonstration purposes only. Not an actual Inherent Risk Questionnaire.
Users can build an IRQ template that can be leveraged across the entire third-party population or can choose to build and send individual IRQs.

This view shows the three options a customer has when sending out an IRQ to a third party.

The customer can send IRQs on-demand and schedule them to be sent at a future date.

Note: This sample is a mockup for demonstration purposes only. Not an actual Inherent Risk Questionnaire.
This view shows the five levels of the Inherent Risk Score and the associated recommended level of assurance that should be obtained from a third party based on the IRQ responses.

Note: This sample is a mockup for demonstration purposes only. Not an actual Inherent Risk Questionnaire.
The Inherent Risk Questionnaire Output

This view displays the IRQ Score and corresponding Inherent Risk Rating.

An action plan is automatically generated based off the IRQ Score, which includes one of five recommended levels of assurance to be requested from each third-party. The customer has the option to override the recommendation and determine the level of assurance they want to receive.

Note: This sample is a mockup for demonstration purposes only. Not an actual Inherent Risk Questionnaire.
How to Receive and Review the HITRUST Assessment XChange Inherent Risk Questionnaire

HAX Dashboard Reporting

HAX API
(More detail in appendix)

Export via Excel (.xlsx)
Ready to Simplify and Streamline Your Organization’s Third-Party Risk Management Program?

Call us directly
(214) 618-9300

Email our Support Specialists
getinfo@HITRUSTAX.com

View more resources
HITRUSTAX.com

The HITRUST Assessment XChange is designed to be an extension of an organization’s third-party risk management program, streamlining and simplifying the process of managing and maintaining risk assessment and compliance information from third parties. Integration of the HITRUST MyCSF and HITRUST Assessment XChange platforms makes sharing risk assessment data simple, secure, and efficient.
Inherent Risk Questionnaire Risk Triage Inherent Risk Factor Ratings

An explanation of the ratings used during the Risk Triage Process for each of the inherent risk factors:

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 no 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

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 Requirements**: 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 Requirements**: Relevant laws, regulations, and/or mandatory standards prescribe a comprehensive and prescriptive framework such as the NIST SP 800-53 or the HITRUST CSF
Inherent Risk Questionnaire Risk Triage Inherent Risk Factor Ratings (continued)

- **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 AICPASOC 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
Inherent Risk Questionnaire Risk Triage Inherent Risk Factor Ratings (continued)

- 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
  - N/A: Not used
  - On-premise: Third-party processing is performed with the organization’s data processing facilities and resources
  - 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
Inherent Risk Questionnaire Risk Triage Inherent Risk Factor Ratings (continued)

- **LT2: Type of cloud environment**
  - 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 sensitive information 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 third-party remote access to sensitive information but only through individual user accounts
  - Remote Access (Group): The organization provides the third-party remote access to sensitive information through group or shared user accounts
Inherent Risk Questionnaire Risk Triage Inherent Risk Factor Ratings (continued)

- 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
  - 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
  - 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
# Inherent Risk Questionnaire API Details

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>OPTIONS</th>
<th>CONSTRAINTS</th>
<th>LABEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participating Organization Name</td>
<td>VARYING CHARACTERS</td>
<td>NA</td>
<td>MIN/MAX CHARACTER LENGTH 1 TO 255</td>
<td>PO NAME</td>
</tr>
<tr>
<td>Participating Organization HAX Org ID</td>
<td>INTEGERS</td>
<td>NA</td>
<td>MIN/MAX CHARACTER LENGTH 1 TO 255</td>
<td>PO ORG ID</td>
</tr>
<tr>
<td>Third Party Name</td>
<td>VARYING CHARACTERS</td>
<td>NA</td>
<td>MIN/MAX CHARACTER LENGTH 1 TO 255</td>
<td>THIRD PARTY NAME</td>
</tr>
<tr>
<td>Third Party HAX Org ID</td>
<td>INTEGERS</td>
<td>NA</td>
<td>MIN/MAX CHARACTER LENGTH 1 TO 255</td>
<td>THIRD PARTY ORG ID</td>
</tr>
<tr>
<td>Date Time of Request</td>
<td>DATE TIME</td>
<td>NA</td>
<td>READ ONLY</td>
<td>DATE TIME IRQ SENT</td>
</tr>
<tr>
<td>Date Time of Completion</td>
<td>DATE TIME</td>
<td>NA</td>
<td>READ ONLY</td>
<td>DATE TIME IRQ COMPLETED</td>
</tr>
<tr>
<td>Inherent Risk Questionnaire Title</td>
<td>VARYING CHARACTERS</td>
<td>NA</td>
<td>MIN/MAX CHARACTER LENGTH 1 TO 255</td>
<td>IRQ TITLE</td>
</tr>
<tr>
<td>Participating Organization Responses</td>
<td>SELECTION</td>
<td>CHOICE 1</td>
<td>READ ONLY</td>
<td>PO RESPONSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHOICE 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHOICE 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHOICE 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHOICE 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third Party Responses</td>
<td>SELECTION</td>
<td>CHOICE 1</td>
<td>READ ONLY</td>
<td>THIRD-PARTY RESPONSE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHOICE 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHOICE 3</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHOICE 4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CHOICE 5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Response Status</td>
<td>SELECTION</td>
<td>NOT STARTED</td>
<td>READ ONLY</td>
<td>STATUS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>INCOMPLETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>COMPLETE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Score</td>
<td>SELECTION</td>
<td>0 - VERY LOW LEVEL OF ASSURANCE</td>
<td>REQUIRED FIELD</td>
<td>SCORE</td>
</tr>
</tbody>
</table>