HITRUST Assessment XChange™

Streamlining the Process of Third-Party and Vendor Risk Management

HITRUST ASSESSMENT XCHANGE™

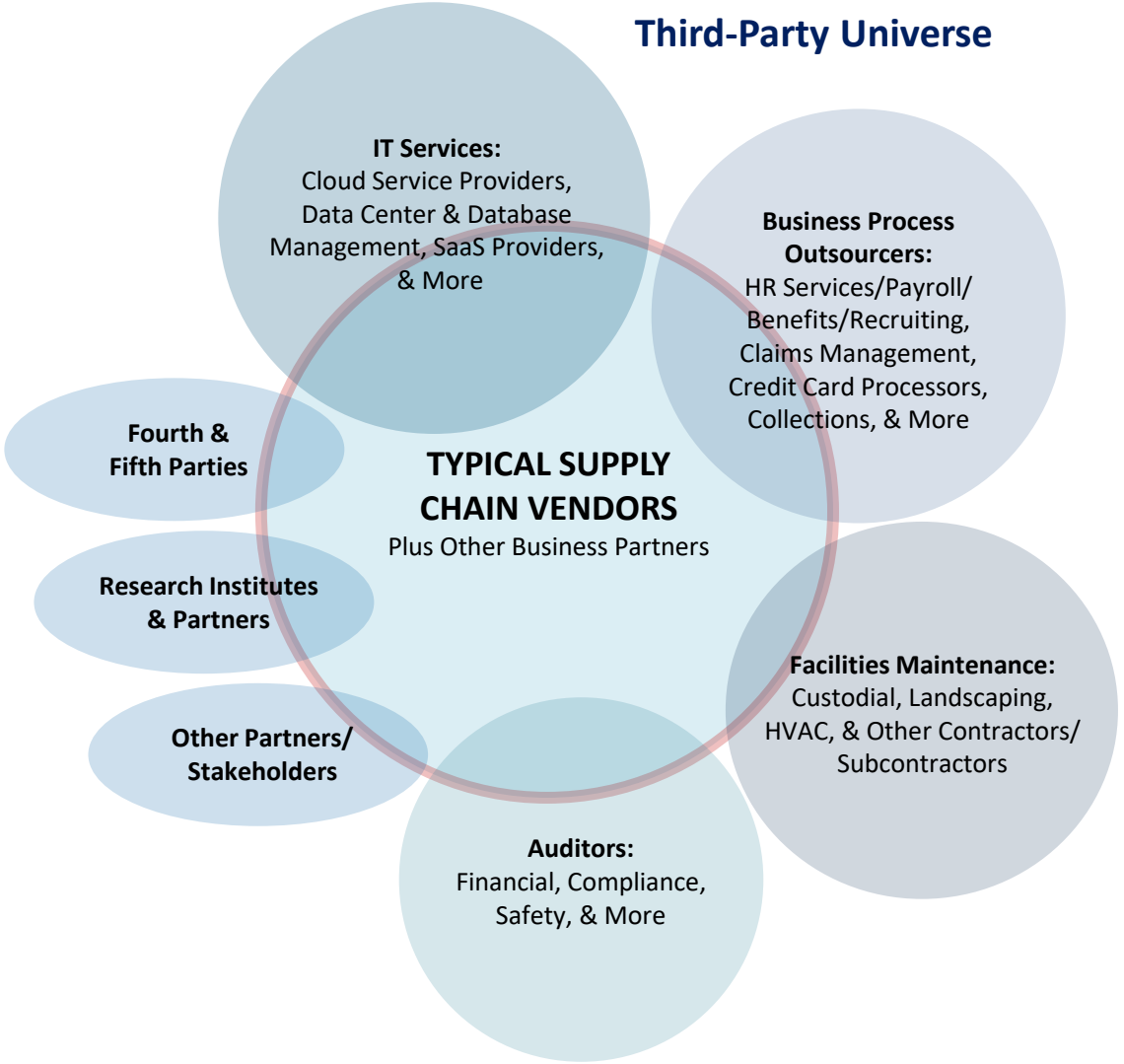
Business Challenges Your Organization Needs to Resolve:

1. We need to better understand the security and privacy risk posed by our entire third-party population and then obtain appropriate, comprehensive, and transparent assurances to address those risks
2. We must ensure we are assessing the risk across our entire population of third parties, and not just a small subset
3. We don't have enough resources to efficiently vet and assess third parties so we can add them to our ecosystem with confidence
4. Our current TPRM processes are manually intensive and distract our risk managers from higher value functions that better help our organization make better informed risk decisions
5. Adding internal resources would require significant cost
6. Adding program automation would be expensive to build in-house – and we don't have the expertise

Defining Your Risk Management Third-Party Population

The Third-Party Universe is far greater than many risk managers realize – consider:

- All vendors are “Third Parties” but not all Third Parties are vendors.
- Third Parties can be any enterprise with which an organization exchanges data or connects to a shared network (including internet portals).
- Most organizations focus primarily on “Accounts Payable” suppliers and those vendors they consider Critical, High-Risk, or High-Volume.
- Third Parties who can put information security and privacy at risk extend well beyond Supply Chain Vendors to include other Business and Ecosystem Partners …



HITRUST Assessment XChange: Strategic Value and Tactical Benefits

IT'S A FACT: Over half of organizations have experienced a data breach caused by third parties that led to the misuse of sensitive or confidential information."

Source: "A Crisis in Third-Party Remote Access Security," report conducted by Ponemon Institute

The HITRUST Assessment XChange is a comprehensive TPRM Managed Service that includes:

- Vendor due diligence and vetting. New vendor onboarding. Continuous monitoring and updating of vendor population.
- Dedicated HITRUST Team supports Participating Organizations (POs) throughout the TPRM administration process, freeing internal staff for more strategic initiatives.
- Customized online platform provides one central repository with significant automation to obtain, store, and report vendor risk data.
- Proven end-to-end HITRUST methodologies and programs effectively assess risk against more than 40 Authoritative Sources.
- Scalable program offers multiple levels of assurance to align to the varying risk profiles of each vendor.
- Automated inherent risk module that segments third parties and recommends action based on level of risk.
- The XChange helps achieve TPRM information security compliance for multiple regulations and the HITRUST CSF framework itself.
- Program is one pre-set annual subscription fee with no variable costs.

A HITRUST XChange Subscription *is a fraction of what a full-time, internal third-party risk manager would cost!*

Leveraging Existing Solutions and ROI Considerations

- **Leverage Infrastructure and Network Already in Place**
  - Don't invest in building a program on your own; leverage the investment already made by others
  - Thousands of assessments already exist and are shared within The HITRUST XChange
  - Utilize output from other stakeholder requests

- **Leverage Globally-Recognized Methodologies**
  - A proven Risk Triage model is built into program
  - Multiple assessment types offered that can scale according to specific relationship risk
  - Assessment scope and requirements also provide fourth-party (and even fifth-party) insight

- **Justify Return on Investment for TPRM**
  - An average internal TPRM resource costs $120K USD per year
  - 50% of a Third-Party Risk Manager's time is spent on administrative and non-value add activities
  - TP risk managers execute 60 to 80 vendor reviews per year at average cost of $1,700 USD per review
  - Most organizations have 150-200 vendors (on average), many have far more
  - Rather than expanding internal risk management programs with expensive internal resources, leverage the value of The XChange to free up your staff for other critical activities

The Need for Third-Party Risk Management (TPRM)

Organizations across all industries rely on third parties.

Organizations need to **efficiently** and **effectively** evaluate and manage the risk they incur by sharing sensitive information with third parties. These organizations must rely on non-validated assurances from their supply chain that **sensitive data is protected**, and the organization **complies with multiple Authoritative Sources including frameworks, regulations, and more.**

CUSTOMER

"We need to ensure our sensitive information is protected."

THIRD PARTY

"Do you really need us to complete a proprietary questionnaire and undergo another privacy and security assessment?"

CUSTOMER

"We need to find a more efficient way to evaluate the effectiveness of our third parties' privacy and security controls."

THIRD PARTY

"How can we leverage a single privacy and security assessment to satisfy all our customers?"

The Current State of TPRM

Many organizations managing third-party risk face these challenges:

- Inaccurate and/or incomplete third-party information, unknown risk profiles
- Organizational resource drain and assessment fatigue managing third parties
- Lack of training and communication for third parties on expectations
- Absence of transparency within third-party environments
- Inability to "quickly" vet and onboard third parties
- Multiple and disparate questionnaires and assessment approaches
- Inappropriate or inconsistent level of assurances
- Assessment scope misaligned with organizations' expectations

TPRM solutions today are inconsistent, generally inefficient (if not ineffective), and unaffordable at scale.

The Partner for Your Third-Party Risk Management Program

The HITRUST Assessment XChange (The XChange) is an integrated yet modular program designed to *streamline and simplify third-party risk management.*

In addition to being the leader in providing organizations with the methodologies, tools, and services needed to efficiently and effectively qualify third parties for potential business relationships …

The XChange also provides a common approach that can be used across all industries for third-party risk management:

1. **Offers proven managed services supported by highly-qualified people, processes, and technologies**
2. **Provides reliable validation of third-party information assurances with continuous updates**
3. **Delivers implementation and application of a streamlined inherent risk tiering and scoring methodology**
4. **Facilitates automated classifications of third parties with recommended levels of assurance to request**

What Makes the HITRUST Assessment XChange Unique?

The HITRUST Assessment XChange Provides all **3 Key Components** of Effective Third-Party Risk Management:

01

People – Professional Services

The XChange is driven by a dedicated team of customer-focused Onboarding Specialists – experts dedicated to ensuring a positive experience for your third parties, as well as transparent and comprehensive results for your organization, providing you with a highly-cost-effective managed service.

02

Process - Industry Agnostic Methodology

The foundation of the XChange is the *HITRUST Third-Party Risk Management Qualification Methodology* – a groundbreaking approach for organizations in ALL industries to minimize risk from third-party relationships – established by HITRUST, a global leader in information risk management and compliance.

03

Technology - Innovative XChange Manager Portal

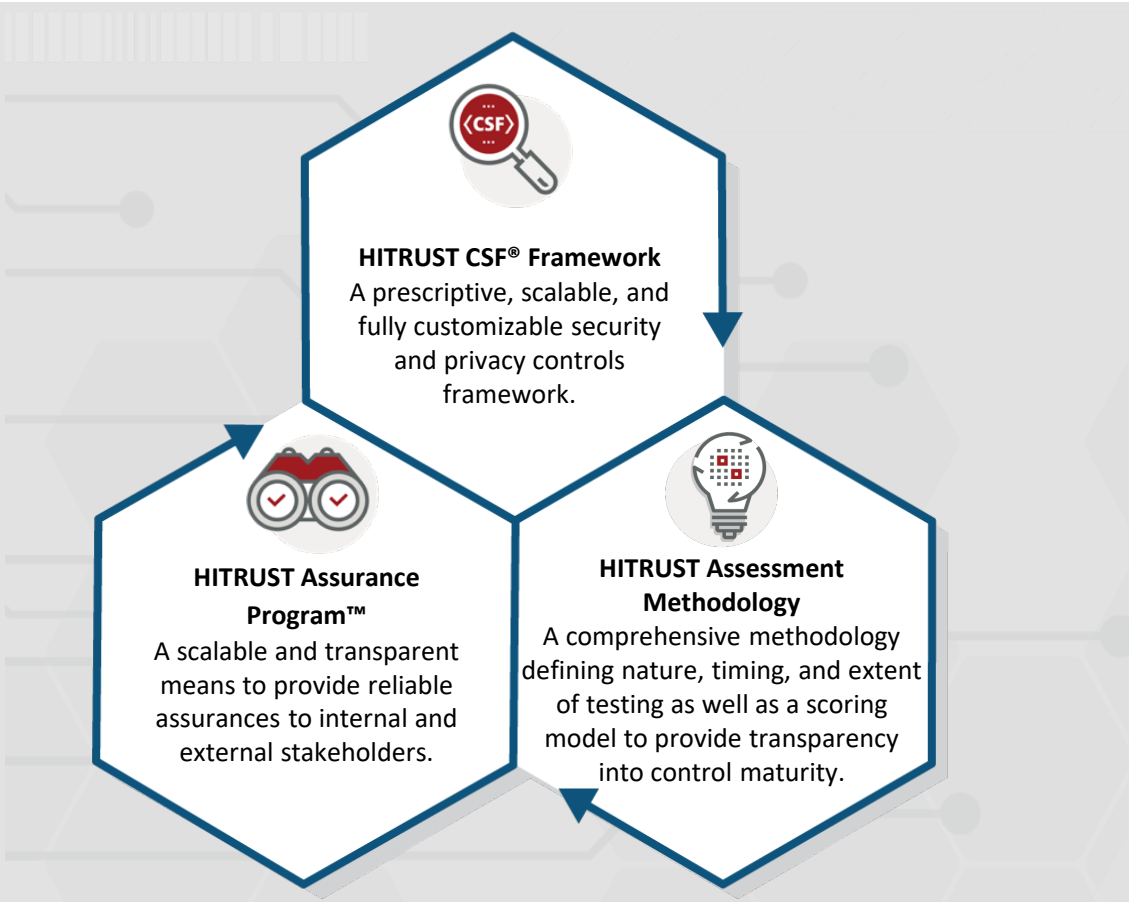
Powering everything is the user-friendly XChange Manager portal – a secure SaaS designed to automate the TPRM qualification process, simplify communications, and streamline everything needed, in one convenient location.

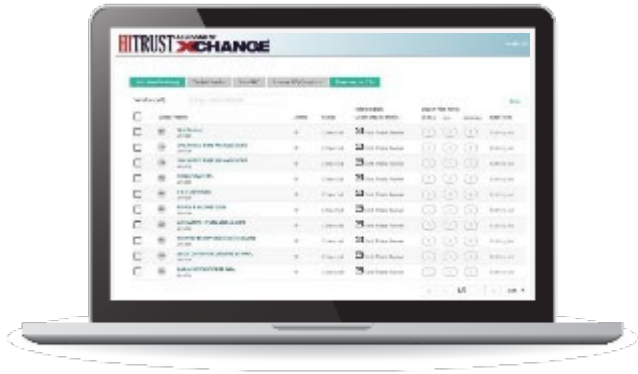
The XChange is a turnkey solution for your organization to manage all third parties, at all levels of risk exposure.

HITRUST ASSESSMENT XCHANGE™

HITRUST Third-Party Risk Management Methodology

Founded on the Core Components of HITRUST®—Enabled by the HITRUST Assessment XChange™





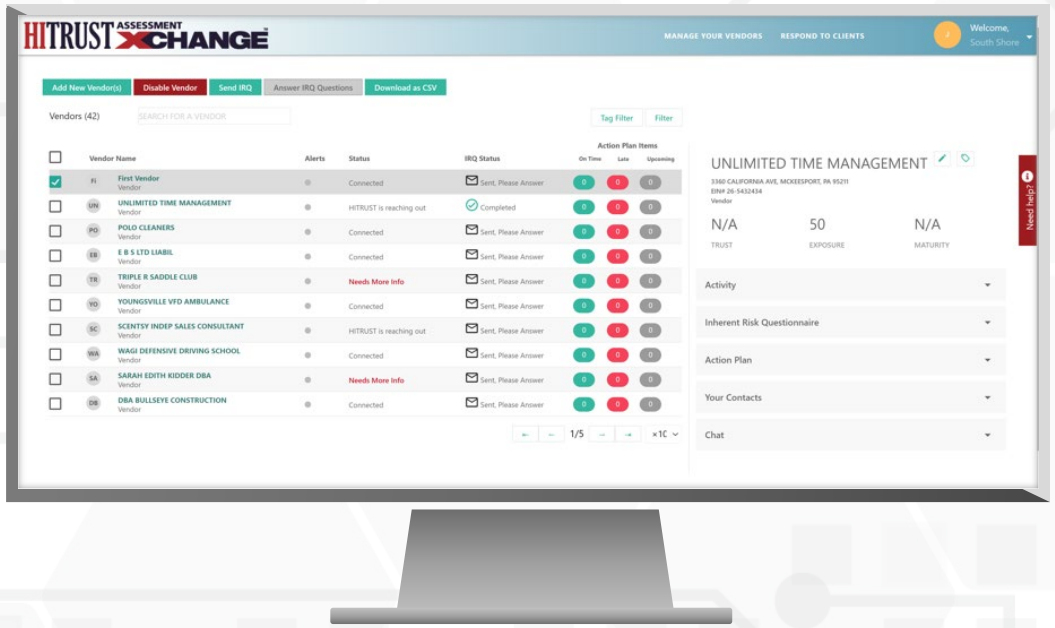
HITRUST Assessment XChange

An innovative and modular program designed to streamline and simplify third-party risk management coupled with an SaaS platform that operationalizes the HITRUST TPRM Program.

HITRUST ASSESSMENT XCHANGE™

Powered by the XChange Manager Portal

The HITRUST Assessment XChange Manager Portal provides access to an online interactive status dashboard with intuitive data analytics.



- ✓ Streamlined, secure communication and information exchange between your organization and all your third parties in one centralized location
- ✓ The ability to deploy Inherent Risk Questionnaires and Assessment Report Requests internally and externally
- ✓ User-friendly filters to quickly view only the pertinent sections of assessment reports
- ✓ Securely access assessment progress details, HITRUST Reports, interim assessments, corrective action plan information, scoring metrics, and more*

** Future enhancements in development*

HITRUST ASSESSMENT XCHANGE™

HITRUST TPRM Methodology

Powered by the HITRUST Assessment XChange

An effective and efficient approach to third-party risk management, consisting of a six-step process:

1. **Initiate:** Formal start of the TPRM process
2. **Collect:** Gathering of information needed to determine risk of a specific business relationship
3. **Qualify:** Formal evaluation of risk due to a specific business relationship
4. **Accept:** Formal acceptance of risk
5. **Select:** Selection of a third party (e.g., a vendor) for a specific business relationship or decision to continue with a third party
6. **Monitor:** Ongoing monitoring of risk

Satisfies HITRUST CSF framework requirements for TPRM.

HITRUST ASSESSMENT XCHANGE™

Inherent Risk Module: Effectively Determines Risk Profiles

Uses the HITRUST Third-Party Risk Triage Model to assess inherent risk with a third-party business relationship.

Provides an Inherent Risk Score to assign a tier/bucket to third parties based on criticality.

Recommends the appropriate level of assurance to request from a third party.

Customizable and delivered through the XChange Manager Portal.

The HITRUST Inherent Risk Questionnaire Offers Key TPRM Benefits:

- ✓ Enables an organization to **properly** and easily assess the inherent risk of its entire third-party network
- ✓ Recommends the right HITRUST Assessment based on the results of a third party's responses
- ✓ Allows customers to determine the required level of assurance based off the recommendation provided
- ✓ Adapts to customer needs with the ability to add customized questions to the standard questionnaire
- ✓ Routes internally and externally to identify misalignment in service understanding between an organization and third party

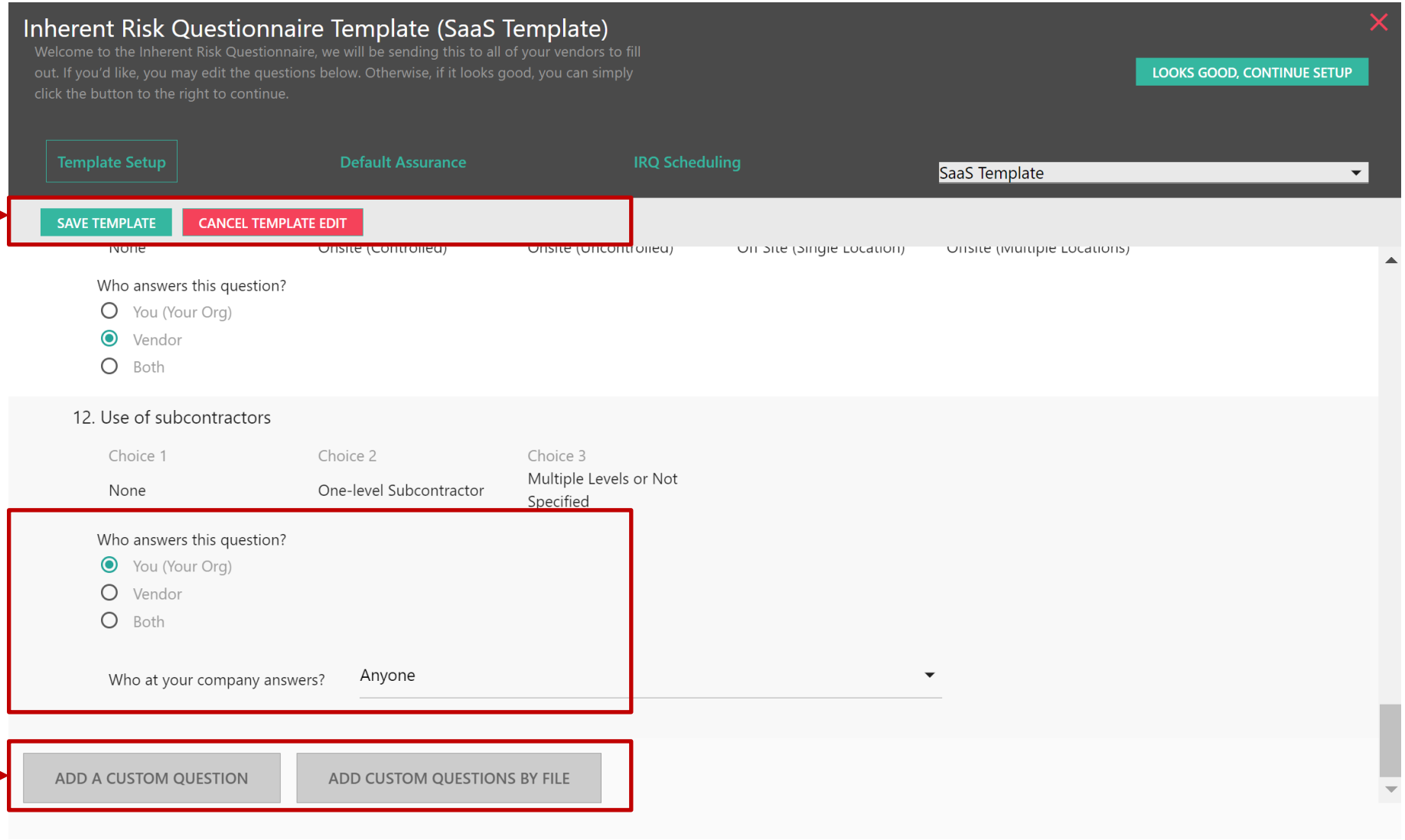
HITRUST ASSESSMENT XCHANGE™

Inherent Risk Module - continued

Multiple IRQ templates available

Ability to route individual questions to different stakeholders

Ability to add customized questions

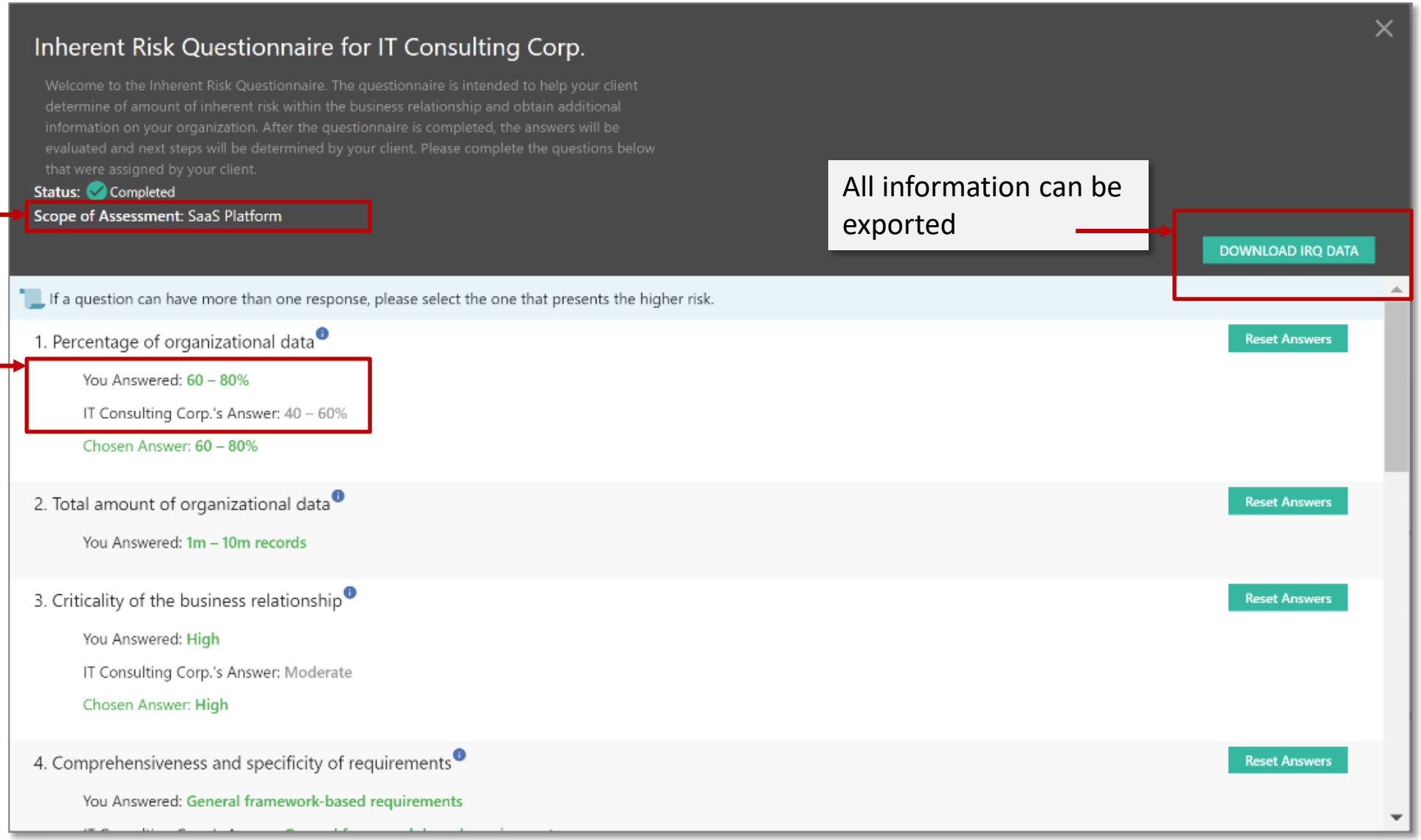


HITRUST ASSESSMENT XCHANGE™

Inherent Risk Module - continued

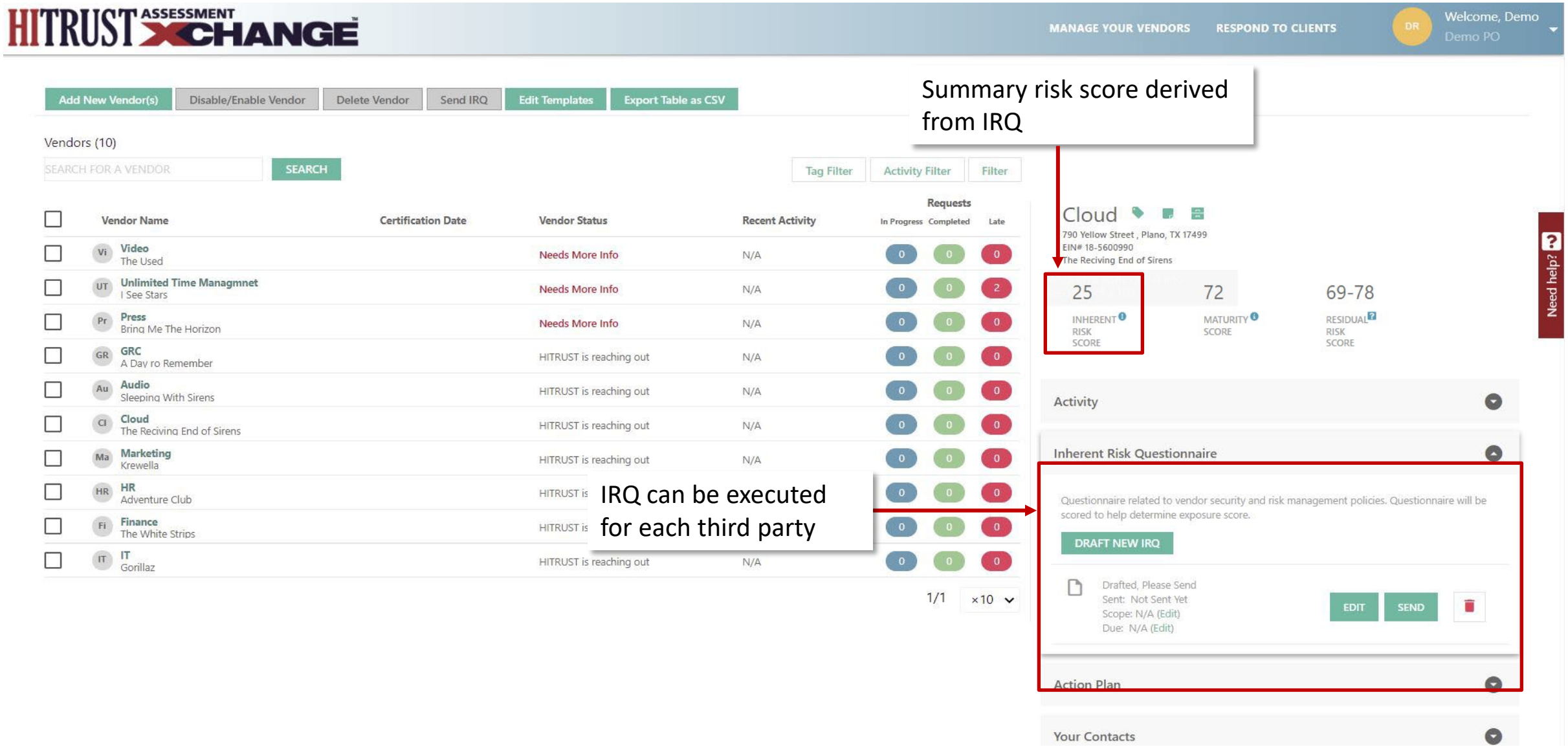
The scope of each IRQ can be defined by the customer

Questions can be addressed by both your organization and third parties



HITRUST ASSESSMENT XCHANGE™

Inherent Risk Module



HITRUST ASSESSMENT XCHANGE

Inherent Risk Module – The Inherent Risk Questionnaire (IRQ)

As part of our Risk Triage Methodology, the HITRUST XChange, sends out an Inherent Risk Questionnaire (IRQ) for your vendor(s) to fill out. IRQ scoring helps determine appropriate HITRUST Assessment level.

	RISK LEVEL	LEVEL OF ASSURANCE	ASSESSMENT RECOMMENDATION PO Can Override	DESCRIPTION	REQUESTED ARR TIMELINE PO Can Modify
6 SCORING TIERS/BUCKETS	0	No Assurance Required	None	N/A	N/A
	1	Low	bC Self-assessment	Good hygiene, fast, low effort, no-cost self-assessment preset with 71 control requirements. No Corrective Action Plans required.	1 month
	2	Moderate	i1 Validated Assessment submitted (does not require Certification)	Best practices, Implemented, 1-Year Validated Assessment (i1) with over 200 preset control requirements. Threat-adaptive control set evolves over time to deliver continuous cyber security relevance. Requires external assessor firm and HITRUST QA. No minimum score. Corrective Action Plans allowed.	6 months
	3	Moderate (Higher)	i1 Validated Assessment (which meets Certification)	Must meet established scoring thresholds during HITRUST QA to earn Certification.	12 months
	4	High	r2 Validated Assessment submitted (does not require Certification)	Risk-based, 2-Year (r2) Validated Assessment with 2000+ possible control requirements (360 average in scope of assessments). Allows customized tailoring to meet selected risk factors, authoritative sources, and regulatory compliance. Requires external assessor firm and HITRUST QA. No minimum score. Corrective Action Plans allowed.	9 months
	5	Very High	r2 Validated Assessment (which meets Certification)	Must meet established scoring thresholds during HITRUST QA to earn Certification. Considered gold standard in information protection assurances.	18 months

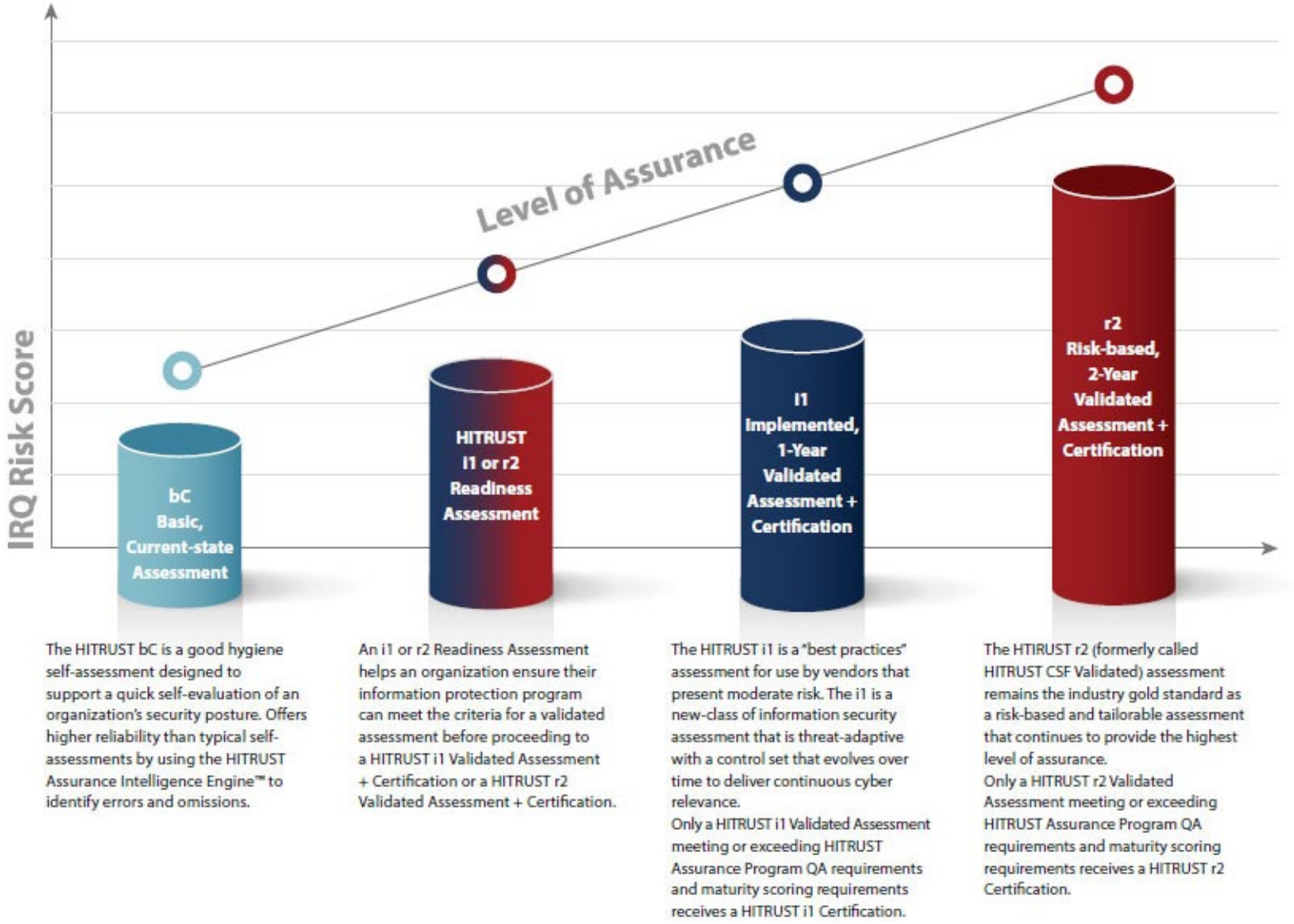
HITRUST ASSESSMENT XCHANGE™

Expanded Assessment Portfolio for the XChange

HITRUST Assessment XChange™ will offer several new options for obtaining assurances related to the security and privacy posture of each of your third parties.

The HITRUST Third-Party Risk Management Methodology, offered through the HITRUST Assessment XChange™, delivers optimal flexibility that allows for:

1. A stand-alone, individual assessment approach.
2. An iterative process in which each step is designed to support progressively increasing levels of assurance.

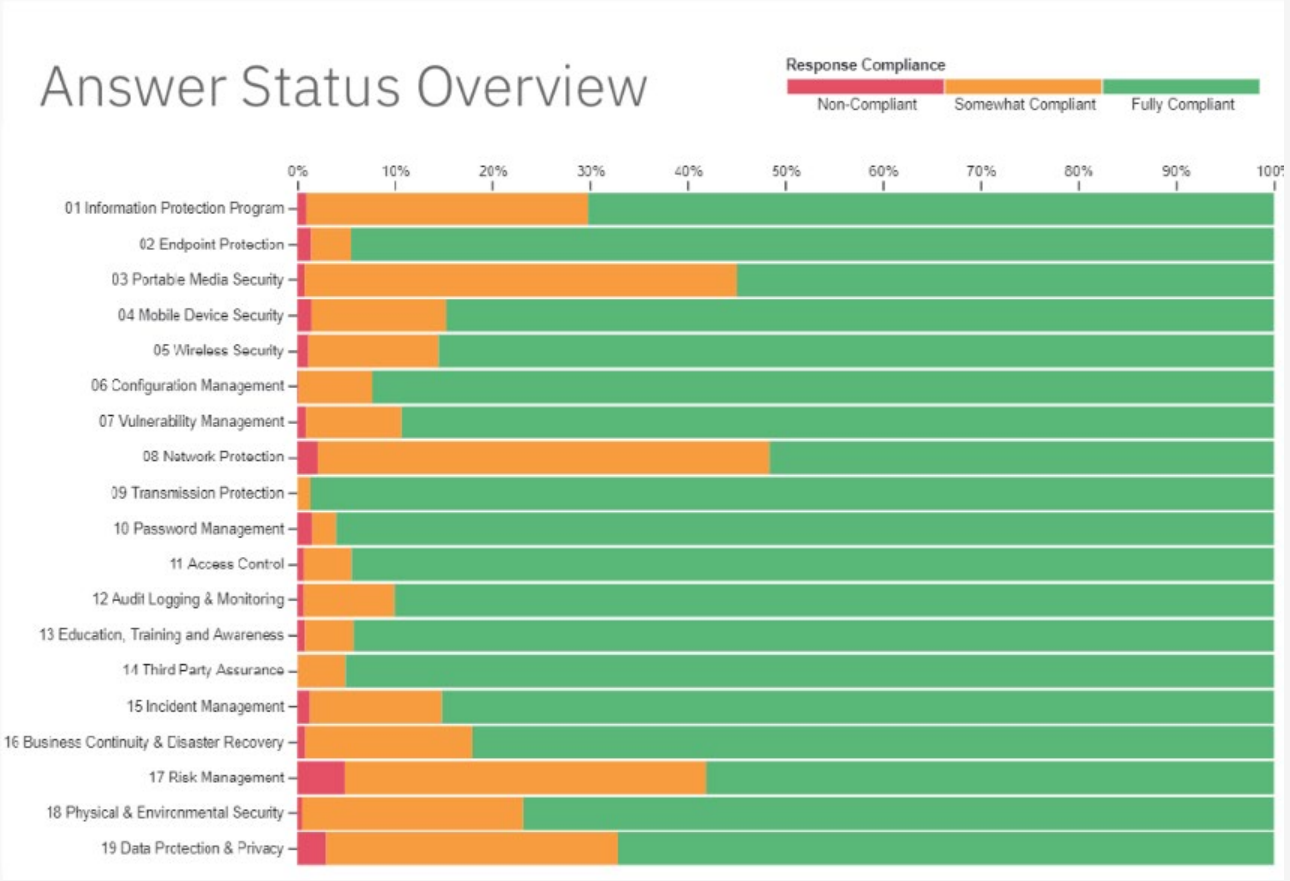


The Basic Assessment At-A-Glance

The Assessment XChange Manager provides a heat map illustrating the results of the HITRUST bC Self-assessment and what percentage of the questions were answered as:

- Noncompliant (NC)
- Somewhat Compliant (SC)
- Fully Compliant (FC)

Potential compliance deficiencies are easy to identify at a glance.



Note: This sample is a mockup for demonstration purposes only. Not an actual Basic Assessment report.

The Basic Assessment At-a-Glance — Continued

The XChange Manager Portal

Reporting screen provides a more detailed view of each bC Self-assessment response.

Clearly identifies any deficiencies.

Deficiencies

Filter

Domain	Statement	Compliance
01 Information Protection Program	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.	Somewhat Compliant
02 Endpoint Protection	Protection against malicious code is based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.	Non-Compliant
02 Endpoint Protection	The status and location of unencrypted covered information is maintained and monitored.	Somewhat Compliant
04 Mobile Device Security	If it is determined that encryption is not reasonable and appropriate, the organization documents its rationale and acceptance of risk.	Somewhat Compliant
05 Wireless Security	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc orci lorem, viverra in augue ut, tempus aliquet sem. Praesent fermentum orci ac tellus tempus, et.	Non-Compliant
06 Configuration Management	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc orci lorem, viverra in augue ut, tempus aliquet sem. Praesent fermentum orci ac tellus tempus, et.	Somewhat Compliant
07 Vulnerability Management	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc orci lorem, viverra in augue ut, tempus aliquet sem. Praesent fermentum orci ac tellus tempus, et.	Somewhat Compliant
08 Network Protection	Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nunc orci lorem, viverra in augue ut, tempus aliquet sem. Praesent fermentum orci ac tellus tempus, et.	Somewhat Compliant

Note: This sample is a mockup for demonstration purposes only. Not an actual Basic Assessment report.

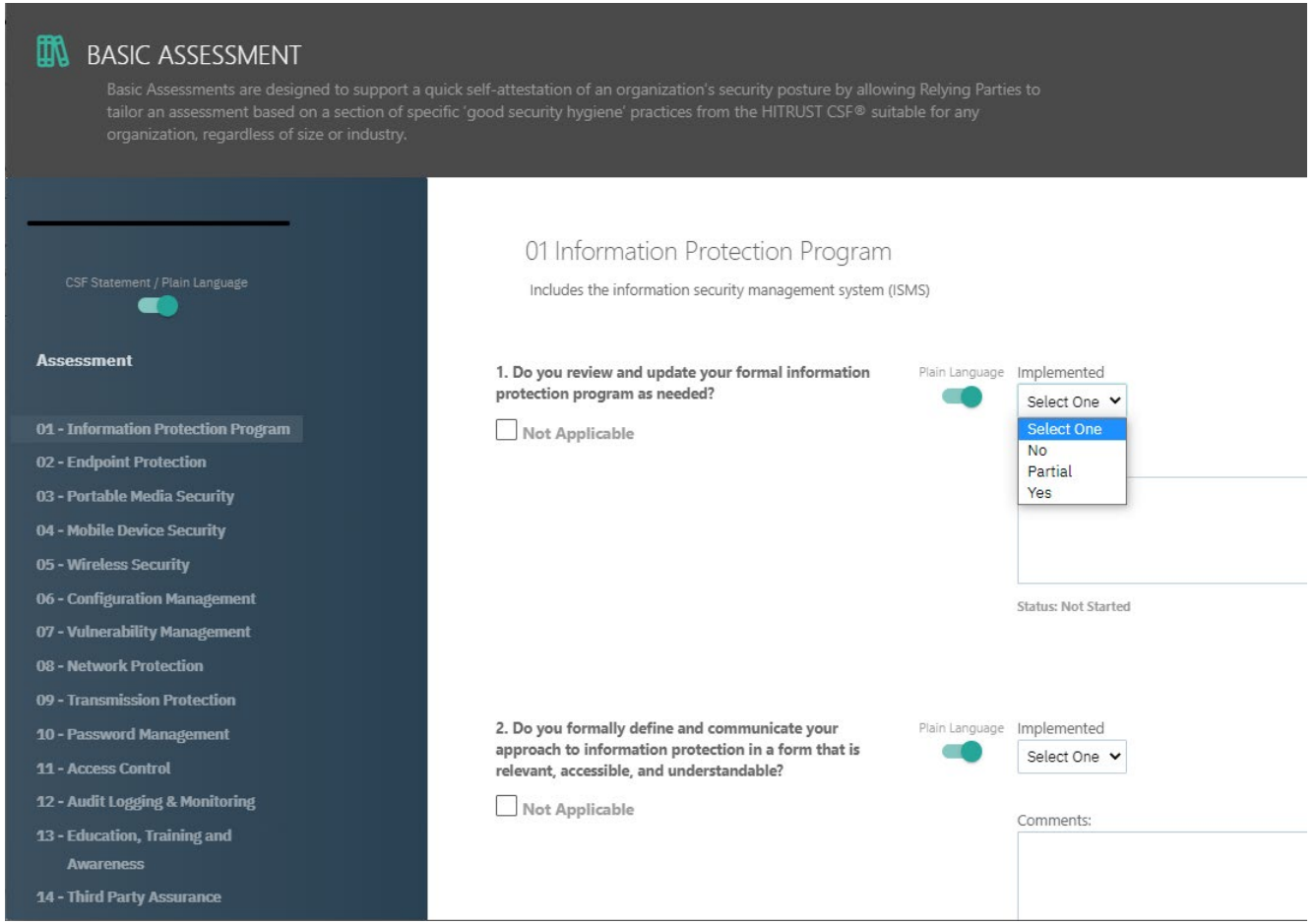
HITRUST bC Assessment

Example: Information Protection Program Questions

Access to user-friendly portal is established for each of your third parties, which allows them to respond to IRQs or bC Self-assessments.

This free, centralized portal allows every vendor to conveniently:

- Articulate responses to each control
- Score against each requirement
- Describe any documentation in place as evidence to each response



Note: This sample is a mockup for demonstration purposes only. Not an actual bC Assessment report.

HX-012-01

Who is Leveraging The XChange?

Large Healthcare System

10,000+ employees; 1,000+ third parties

Utilizes the XChange to store and track all third-party assessments in one place

Insurance Provider

5,000+ employees; 500+ third parties

Utilizes the XChange to obtain required assurances from third parties and monitor corrective action plans

Major University

10,000+ employees; 200+ third parties

Utilizes the XChange to better understand the inherent risk profile of each third party

Small Software Company

50 employees; 30+ third parties

Utilizes the XChange as an extension of their internal risk management team

Luxury Hospitality Brand

8,000+ employees; 300+ third parties

Utilizes the XChange to streamline vetting and onboarding of new vendors

Additional Sectors

Enterprises, Organizations, and Agencies of any size that need to:

Utilize the XChange to better identify and mitigate third-party information risk

HITRUST ASSESSMENT XCHANGE™

HITRUST®

Thank You!

www.HITRUSTAlliance.net

Appendix A

HITRUST ASSESSMENT XCHANGE

HITRUST Readiness Assessment

HITRUST Readiness Assessment

- A self-attested assessment used to determine current security posture and any potential remediation efforts
- Often used in preparation for a future HITRUST i1 or r2 Validated Assessment (+ Certification).
- Though a HITRUST-Certified External Assessor is not required, many organizations choose to leverage our network and obtain consulting services to assist with their Readiness Assessment.
- HITRUST prepares and issues HITRUST Readiness Assessment Reports.

HITRUST Validated Assessment

HITRUST Validated Assessment

- A third-party validated assessment, performed in partnership with an Authorized External Assessor organization then submitted to HITRUST for quality assurance review and issuance of a HITRUST Validated Assessment Report.
- A HITRUST Validated Assessment (+ Certification) is available for both a HITRUST Implemented, 1-Year (i1) Assessment and a HITRUST Risk-based, 2-Year (r2) Assessment.
- HITRUST Certifications may be issued in conjunction with HITRUST Validated Assessment Reports that meet scoring requirements.
- HITRUST Validated Assessment Reports that do not meet HITRUST Certification standards are valid for one year.
- A HITRUST i1 Certification is are valid for one year.
- A HITRUST r2 Certification is valid for two years, pending completion of a HITRUST r2 Interim Assessment at the one-year mark.

HITRUST Assessment Portfolio

HITRUST Basic, Current-state (bC) Self-assessment

Lowest Level of Effort, Lowest Level of Assurance

- A good hygiene assessment that offers higher reliability than other self-assessments and questionnaires.
- Delivers relatively easy-to-obtain results when speed is essential, or when a third party poses a low level of risk.

HITRUST Implemented, 1-Year (i1) Validated Assessment + Certification

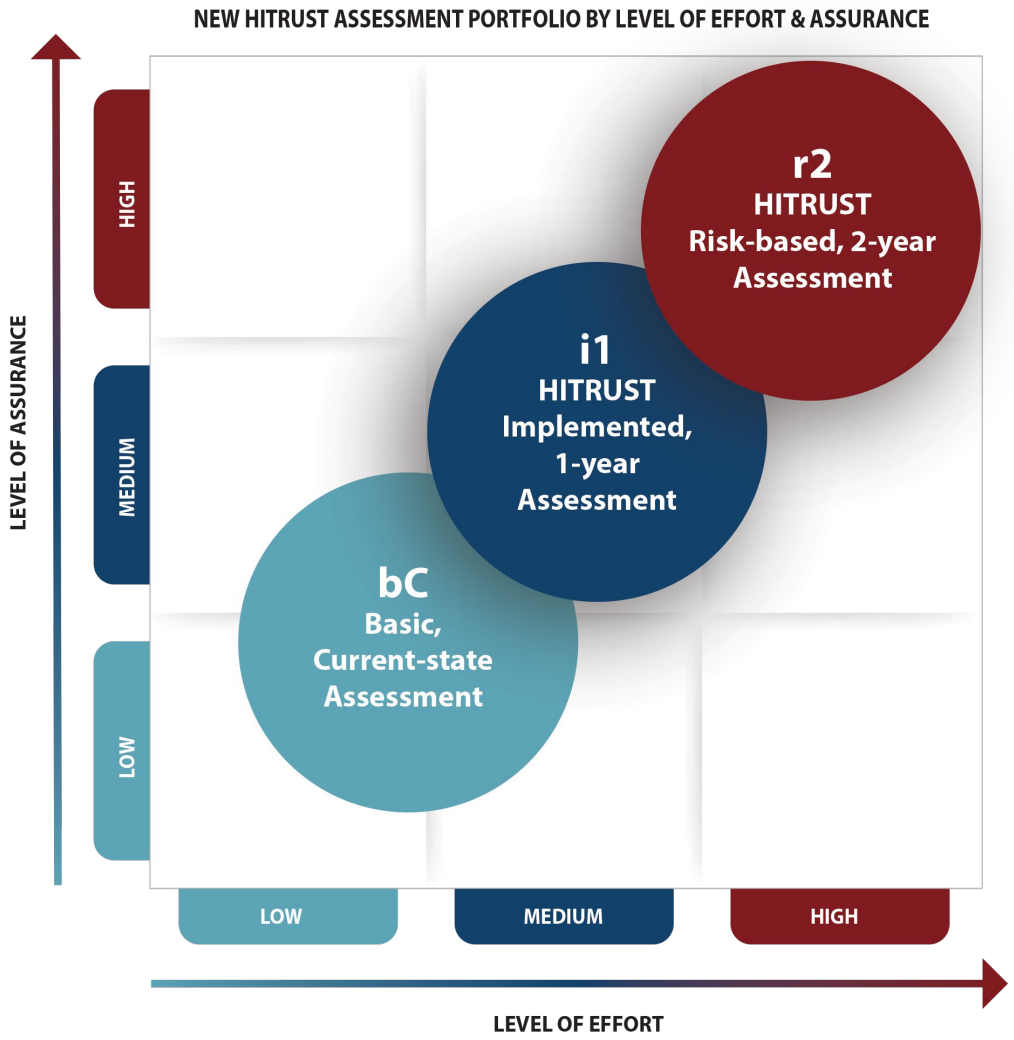
Moderate Level of Effort, Moderate Level of Assurance

- A new-class of information security assessment that is threat-adaptive with a control set that evolves over time to deliver continuous cyber relevance and keep pace with the latest cyberattack threats.
- A best practices assessment recommended for vendors that present moderate risk.

HITRUST Risk-based, 2-Year (r2) Validated Assessment + Certification

Highest Level of Effort, Highest Level of Assurance

- Formerly named the HITRUST CSF Validated Assessment, the r2 remains the industry gold standard as a risk-based and tailorable assessment that continues to provide the highest level of assurance.
- Use for vendors that present the greatest risk exposure due to data volumes, regulatory compliance, or other demanding risk factors.



HITRUST Basic, Current-state (bC) Self-assessment

bC Assessment Features

A good hygiene information security assessment that offers better consistency, improved accuracy, and more flexibility than other types of self-assessments.

- Fast, low-effort tool that is ideal for providing basic assurances from service providers, vendors, supply chain partners, and other third-party business partners
- Requires no control selection, scoring, validation, or quality assurance by external assessor(s)
- Offers no certification

bC Assessment Use Cases

1. When the Inherent Risk for a third party is low and it does not make business sense to request a more comprehensive assessment from the third party
2. When an organization does not know the security and privacy posture of a third party that is going through an RFP or on-boarding process
3. When a third party has another type of HITRUST Assessment underway, but an organization needs immediate assurances
4. As a stop-gap when a third party has a completed a HITRUST Assessment, but the scope does not fully align with the scope needed
5. When an organization needs to quickly gain updated third-party assurance(s) in a specific domain

HITRUST Implemented, 1-Year i1 Validated Assessment

i1 Assessment Features

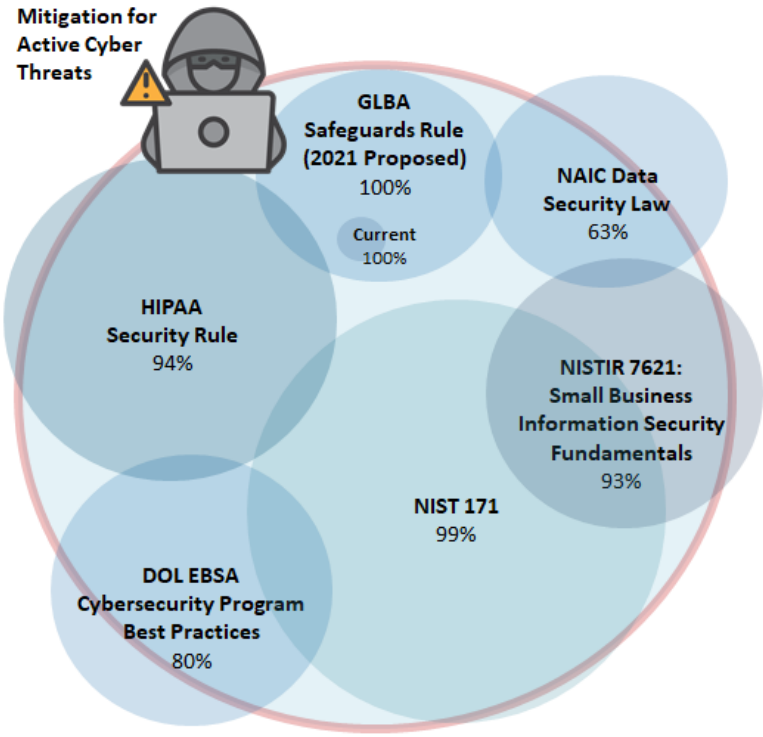
Delivers next-generation assurances by leveraging ongoing threat intelligence data and the MITRE ATT&CK Framework to address the latest cyberattack threats.

- Moves security assessments beyond a check-list model to a more dynamic approach that ensures control selection is continuously relevant in defending against the latest threats and cyberattack techniques, including ransomware and phishing
- Focuses on Implementation for greater assurance that control requirements are in place and operating as intended
- Assessment and testing through a highly qualified HITRUST Authorized External Assessor and the comprehensive HITRUST QA process for Validation and Certification (if earned)
- 1-year Certification

i1 Assessment Use Cases

1. Use for third parties that present moderate levels of information security risk to your organization
2. The Implemented, 1-year i1 Assessment falls between the HITRUST bC Self-assessment and the more rigorous HITRUST Risk-based 2-year (r2) Assessment in terms of effort and assurance levels
3. Leverages good security hygiene and leading practices that substantially cover authoritative sources, such as: NIST SP 800-171, HIPAA Security Rule, GLBA Safeguards Rule, U.S. Department of Labor EBSA Cybersecurity Program Best Practices, Health Industry Cybersecurity Practices (HICP).
4. Since some organizations choose an i1 Assessment based on speed-to-completion, HITRUST has established a 45 business days (or less) post-submission Service Level Agreement to complete QA on Validated i1 Assessments.
   (Note: Validated i1 Assessment submissions that enter escalated QA due to quality concerns are exempted from this SLA.)

HITRUST CSF Requirements in an i1 Assessment



HITRUST Risk-based, 2-Year r2 Validated Assessment

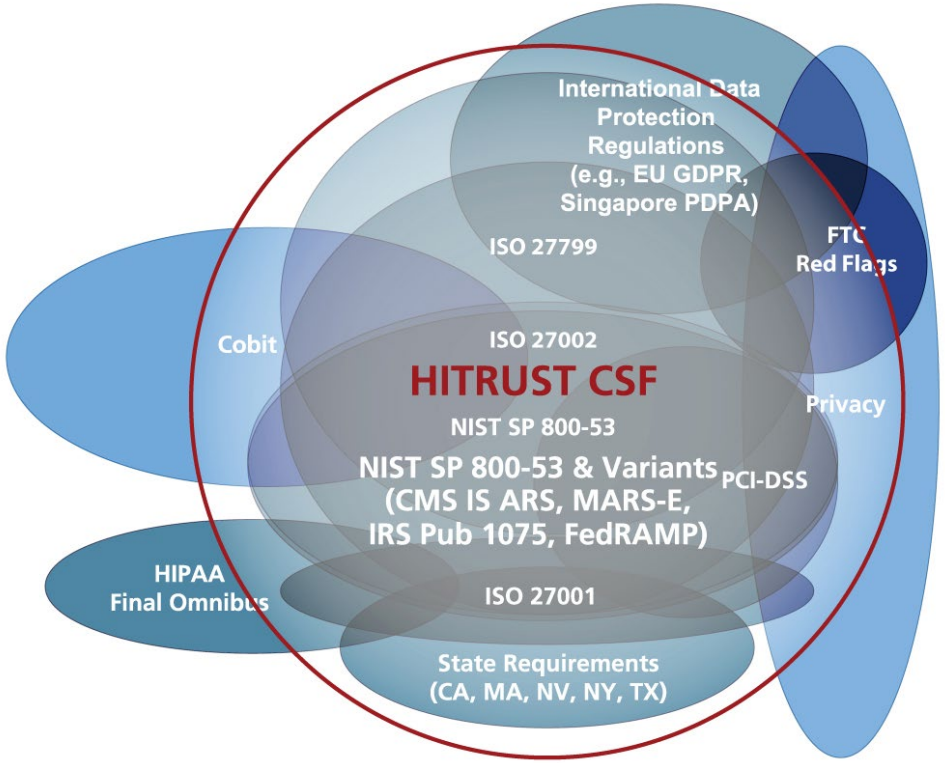
r2 Assessment Features

The industry-recognized gold standard for providing the highest level of information protection and compliance assurance.

- Uses a risk-based approach so vendors with the greatest risk potential assess against the most demanding security and data protection challenges
- A tailorable assessment that focuses on comprehensive, prescriptive, risk-based controls specification
- Can be customized to include up to 2000 control requirements, which allows your assessed entity to select and evaluate against whichever risk factors, authoritative sources, and compliance factors your organization requires
- Assessment and testing through a highly qualified HITRUST Authorized External Assessor and the comprehensive HITRUST QA process for Validation and Certification (if earned)
- 2-year Certification

r2 Assessment Use Cases

1. For service providers and other vendors that handle PII, ePHI, and other sensitive data that requires the highest levels of assurance
2. For third-parties who present high levels of risk due to data volumes, regulatory compliance, or other risk factors
3. A properly scoped r2 Assessment offers coverage against: NIST SP 800-53, NIST CSF, ISO 27001, HIPAA, FedRAMP, FISMA, FTC Red Flags Rule Compliance, MARS-E Requirements, PCI DSS, CCPA, GDPR, AICPA Trust Services Criteria for Security, Confidentiality and Availability, plus more than 30 other industry-recognized frameworks, standards, and authoritative sources
4. When demonstrable assurances are need to show full compliance with HIPAA Security, Breach, and Privacy Rules – or any other specific authoritative source
5. The r2 Assessment provides a separate NIST CSF Report, so is ideal when a NIST Cybersecurity Framework evaluation is needed



Appendix B

HITRUST ASSESSMENT XCHANGE

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

Inherent Risk Questionnaire Risk Triage Inherent Risk Factor Ratings (continued)

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

° Compliance Risk Factor Type

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 AICPA SOC 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

Appendix C

HITRUST ASSESSMENT XCHANGE

HITRUST Basic, Current-state (bC) Self-assessment Requirements

Domain Name	HITRUST CSF Requirement Statement
01 Information Protection Program	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.
	Information security objectives, approach, scope, importance, goals, and principles for the organization's security program are formally identified, communicated throughout the organization to users in a form that is relevant, accessible, and understandable to the intended reader; and supported by a controls framework that considers legislative, regulatory, contractual requirements, and other policy-related requirements.
	The security policies are regularly reviewed and updated to ensure they reflect leading practices (e.g., for systems and services development and acquisition), and are communicated throughout the organization.
	Verification checks take into account all relevant privacy, protection of covered data and/or employment-based legislation, and, where permitted and appropriate, include satisfactory character references; a check of the applicant's curriculum vitae; confirmation of claimed academic and professional qualifications; verification of eligibility to work in the U.S.; and an independent identity check (e.g., passport or similar document) prior to granting access to covered information.
02 Endpoint Protection	Anti-virus and anti-spyware are installed, operating and updated on all end-user devices to conduct periodic scans of the systems to identify and remove unauthorized software. Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software are addressed via a network-based malware detection (NBMD) solution.
	Audit logs of the scans are maintained.
	Centrally-managed, up-to-date anti-spam and anti-malware protection is implemented at information system entry/exit points for the network and on all devices.
03 Portable Media Security	The organization, based on the data classification level, registers media (including laptops) prior to use, places reasonable restrictions on how such media are used, and provides an appropriate level of physical and logical protection (including encryption) for media containing covered and/or confidential information until properly destroyed or sanitized.
04 Mobile Device Security	Mobile computing devices are protected at all times by access controls, usage restrictions, connection requirements, encryption, virus protections, host-based firewalls, or equivalent functionality, secure configurations, and physical protections.
	Teleworking activities are only authorized if security arrangements and controls that comply with relevant security policies and organizational requirements are in place.
	The organization ensures that mobile devices connecting to corporate networks, or storing and accessing company information, allow for remote wipe.
05 Wireless Security	Vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point.
	Wireless access points are configured with strong encryption (AES WPA2 at a minimum).

HITRUST Basic, Current-state (bC) Self-assessment Requirements

Domain Name	HITRUST CSF Requirement Statement
06 Configuration Management	Only authorized administrators are allowed to implement approved upgrades to software, applications, and program libraries, based on business requirements and the security implications of the release.
	Changes to equipment, software, and procedures are strictly and consistently managed.
	The organization minimizes any testing on production systems; and, when testing is performed, a test plan is developed that documents all changes to the system and the procedures for undoing any changes made to the system.
	The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse. Vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of web browsers on operational systems to take advantage of the latest security functions in the application.
	If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, the organization is able to provide evidence of a formal migration plan approved by management to replace the system or system components.
	Where development is outsourced, change control procedures to address security are included in the contract(s) and specifically require the developer to track security flaws and flaw resolution within the system, component, or service and report findings to organization-defined personnel or roles.
	The operating system has in place supporting technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of its baseline.
07 Vulnerability Management	An inventory of assets and services is maintained.
	Technical vulnerabilities are identified, evaluated for risk, and corrected in a timely manner.
	The organization centrally manages the flaw remediation process and installs software updates automatically where possible.
08 Network Protection	The organization's security gateways (e.g., firewalls) enforce security policies; are configured to filter traffic between domains; block unauthorized access; are used to maintain segregation between internal wired, internal wireless, and external network segments (e.g., the Internet), including DMZs; and, enforce access control policies for each of the domains.
	Requirements for network routing control are based on the access control policy, including positive source and destination checking mechanisms, such as firewall validation of source/destination addresses, and the hiding of internal directory services and IP addresses. The organization designed and implemented network perimeters so that all outgoing network traffic to the Internet passes through at least one application layer filtering proxy server. The proxy supports decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a blacklist, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. The organization forces outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.

HITRUST Basic, Current-state (bC) Self-assessment Requirements

Domain Name	HITRUST CSF Requirement Statement
09 Transmission Protection	Encryption keys and the equipment to generate, store, and archive keys are protected against modification, loss, destruction, and disclosure.
	Strong cryptography protocols are used to safeguard covered and/or confidential information during transmission over less trusted/open public networks.
	Stronger controls are implemented to protect certain electronic messages, and electronic messages are protected throughout the duration of its end-to-end transport path, using cryptographic mechanisms unless protected by alternative measures.
10 Password Management	Before deploying any new devices in a networked environment, the organization changes all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
	The organization requires quality passwords that are easy to remember, not based on anything somebody else could easily guess or obtain using person-related information (e.g., names, telephone numbers, and dates of birth etc.), not vulnerable to dictionary attack (do not consist of words included in dictionaries), and free of consecutive identical characters.
11 Access Control	Access authorization (e.g., access requests, approvals and provisioning) is segregated among multiple individuals or groups.
	User identities are verified prior to establishing accounts.
	Default and unnecessary system accounts are removed, disabled, or otherwise secured (e.g., the passwords are changed and privileges are reduced to the lowest levels of access).
	User registration and deregistration, at a minimum: communicates relevant policies to users and require acknowledgement (e.g., signed or captured electronically); checks authorization and minimum level of access necessary prior to granting access; ensures access is appropriate to the business needs (consistent with sensitivity/risk and does not violate segregation of duties requirements); addresses termination and transfer; ensures default accounts are removed and/or renamed; removes or blocks critical access rights of users who have changed roles or jobs; and automatically removes or disables inactive accounts.
	The organization has implemented secure log-on procedures, which include: a warning notice; limits the number of unsuccessful attempts to six and enforces a delay of 30 minutes, without specific authorization from an administrator; records the number of unsuccessful and successful attempts; and does not display the password when being entered.
	The organization ensures that redundant user IDs are not issued to other users and that all users are uniquely identified and authenticated for both local and remote access to information systems.
	A time-out mechanism (e.g., a screen saver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed; or, if the system cannot be modified, a limited form of time-out that clears the screen but does not close down the application or network sessions is used.
	Logical and physical access authorizations to systems and equipment are reviewed, updated or revoked when there is any change in responsibility or employment.

HITRUST Basic, Current-state (bC) Self-assessment Requirements

Domain Name	HITRUST CSF Requirement Statement
11 Access Control (cont.)	The organization maintains a current listing of all workforce members (individuals, contractors, vendors, business partners, etc.) with access to sensitive information (e.g., PII).
	Acceptable use agreements are signed by all employees before being allowed access to information assets.
	The organization restricts access to privileged functions and all security-relevant information.
	The organization reviews critical system accounts and privileged access rights every 60 days; all other accounts, including user access and changes to access authorizations, are reviewed every 90 days.
12 Audit Logging & Monitoring	Auditing is always available while the system is active and tracks key events, success/failed data access, system security configuration changes, privileged or utility use, any alarms raised, activation and de-activation of protection systems (e.g., A/V and IDS), activation and deactivation of identification and authentication mechanisms, and creation and deletion of system-level objects.
	The organization specifies how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required.
	Retention for audit logs are specified by the organization and the logs retained accordingly.
	The organization identifies duties that require separation and defines information system access authorizations to support separation of duties; and incompatible duties are segregated across multiple users to minimize the opportunity for misuse or fraud.
13 Education, Training and Awareness	Employees and contractors receive documented initial (as part of their onboarding within 60 days of hire), annual, and ongoing training on their roles related to security and privacy.
	The organization defines rules to describe user responsibilities and acceptable behavior for information system usage, including at a minimum, rules for email, Internet, mobile devices, social media and facility usage.
	The organization prohibits users from installing unauthorized software, including data and software from external networks, and ensures users are made aware and trained on these requirements.
	The organization provides incident response and contingency training to information system users consistent with assigned roles and responsibilities within 90 days of assuming an incident response role or responsibility; when required by information system changes; and within every 365 days thereafter.
	Employees, contractors and third-party system users are aware of the limits existing for their use of the organization's information and assets associated with information processing facilities and resources; and they are responsible for their use of any information resource and of any use carried out under their responsibility.

HITRUST Basic, Current-state (bC) Self-assessment Requirements

Domain Name	HITRUST CSF Requirement Statement
14 Third Party Assurance	Access to the organization's information and systems by external parties is not permitted until due diligence has been conducted, the appropriate controls have been implemented, and a contract/agreement reflecting the security requirements is signed acknowledging they understand and accept their obligations.
	The organization ensures a screening process is carried out for contractors and third-party users, and, where contractors are provided through an organization, the contract with the organization clearly specifies the organization's responsibilities for screening and the notification procedures they need to follow if screening has not been completed, or if the results give cause for doubt or concern; and, all responsibilities and notification procedures for screening.
15 Incident Management	The security incident response program accounts for and prepares the organization for a variety of incidents.
16 Business Continuity & Disaster Recovery	The organization can recover and restore business operations and establish an availability of information in the time frame required by the business objectives and without a deterioration of the security measures.
	The contingency program addresses required capacity, identifies critical missions and business functions, defines recovery objectives and priorities, and identifies roles and responsibilities.
	Backup copies of information and software are made, and tests of the media and restoration procedures are regularly tested at appropriate intervals.
	A formal definition of the level of backup required for each system is defined and documented including how each system will be restored, the scope of data to be imaged, frequency of imaging, and duration of retention based on relevant contractual, legal, regulatory and business requirements.
	The backups are stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site, and reasonable physical and environmental controls are in place to ensure their protection at the remote location.
	The organization brings together specific key information security elements of business continuity management, which include: (i) identifying all the assets involved in critical business processes; (ii) considering the purchase of suitable insurance, which may form part of the overall business continuity process, as well as being part of operational risk management; (iii) ensuring the safety of personnel and the protection of information assets and organizational property; and, (iv) formulating and documenting business continuity plans addressing information security requirements in line with the agreed business continuity strategy.

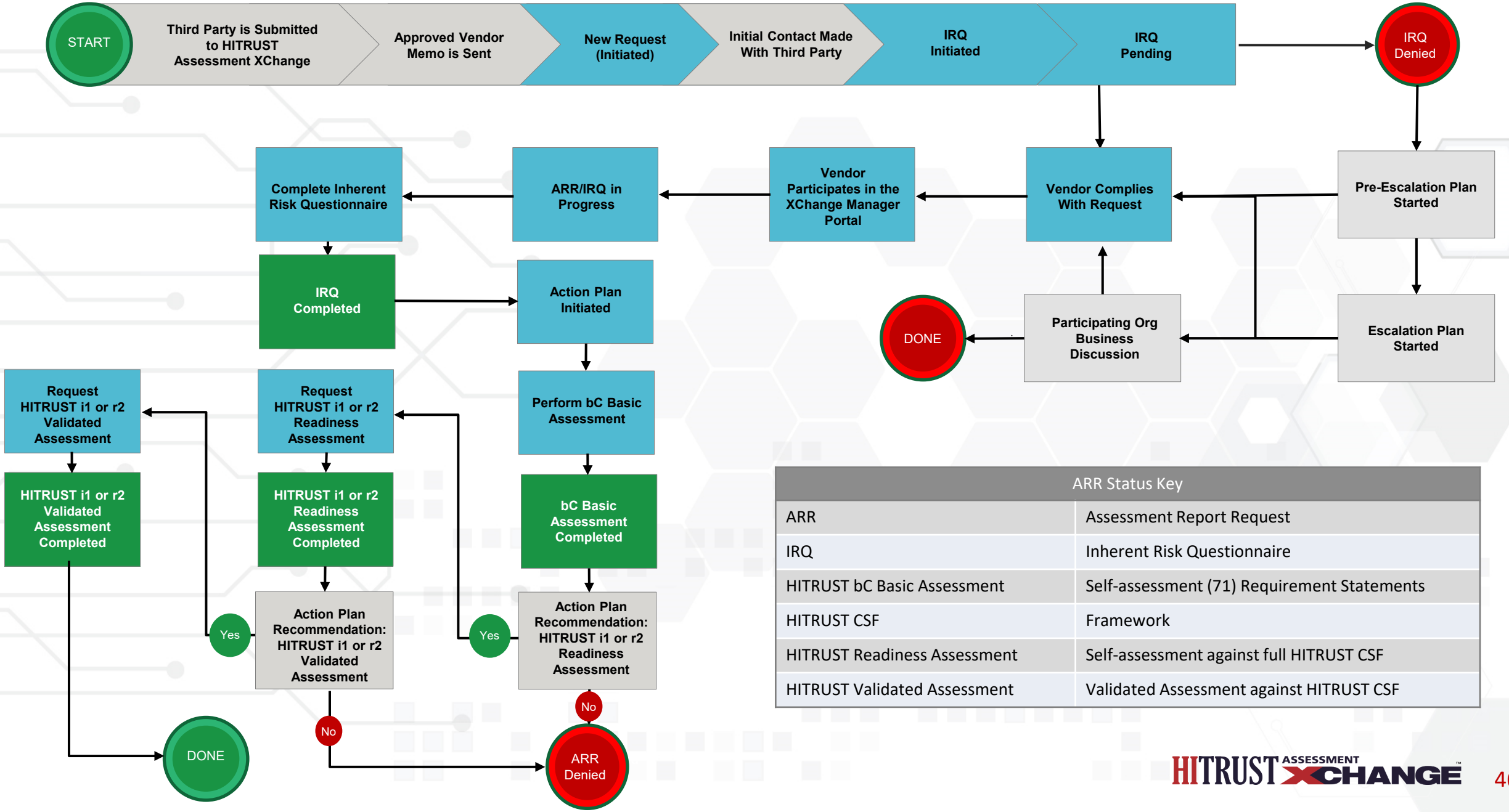
HITRUST Basic, Current-state (bC) Self-assessment Requirements

Domain Name	HITRUST CSF Requirement Statement
17 Risk Management	The organization maintains and updates a formal, comprehensive program to manage the risk associated with the use of information assets.
	The organization performs risk assessments in a consistent way and at planned intervals, or when there are major changes to the organization's environment and reviews the risk assessment results annually.
18 Physical & Environmental Security	Areas where sensitive information (e.g., covered information, payment card data) is stored or processed are controlled and restricted to authorized individuals only.
	Visible identification that clearly identifies the individual is required to be worn by employees, visitors, contractors and third-parties.
	The organization monitors and controls non-local maintenance and diagnostic activities; and prohibits non-local system maintenance unless explicitly authorized, in writing, by the CIO or his/her designated representative.
	Electronic and physical media containing covered and/or confidential information is securely sanitized prior to reuse, or if it cannot be sanitized, is destroyed prior to disposal.
	The organization securely disposes of media containing sensitive information.
	Lightning protection is applied to all buildings, and lightning protection filters (e.g., surge protectors) are fitted to all incoming power and communications lines.
	Information assets handling covered and/or confidential information are positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage devices are secured to avoid unauthorized access.
	An uninterruptable power supply (UPS) is used for equipment supporting critical business operations to support orderly shutdown or continuous running (transition to long-term alternate power); UPS equipment and generators are regularly checked to ensure they have adequate capacity and are tested in accordance with the manufacturer's recommendations; and power contingency plans cover the action to be taken should the UPS fail.
19 Data Protection & Privacy	Personnel developing and testing system code do not have access to production libraries.

Appendix D

HITRUST ASSESSMENT XCHANGE

HITRUST ASSESSMENT XCHANGE REQUEST WORKFLOW



ARR Status Key	
ARR	Assessment Report Request
IRQ	Inherent Risk Questionnaire
HITRUST bC Basic Assessment	Self-assessment (71) Requirement Statements
HITRUST CSF	Framework
HITRUST Readiness Assessment	Self-assessment against full HITRUST CSF
HITRUST Validated Assessment	Validated Assessment against HITRUST CSF

HITRUST ASSESSMENT XCHANGE™