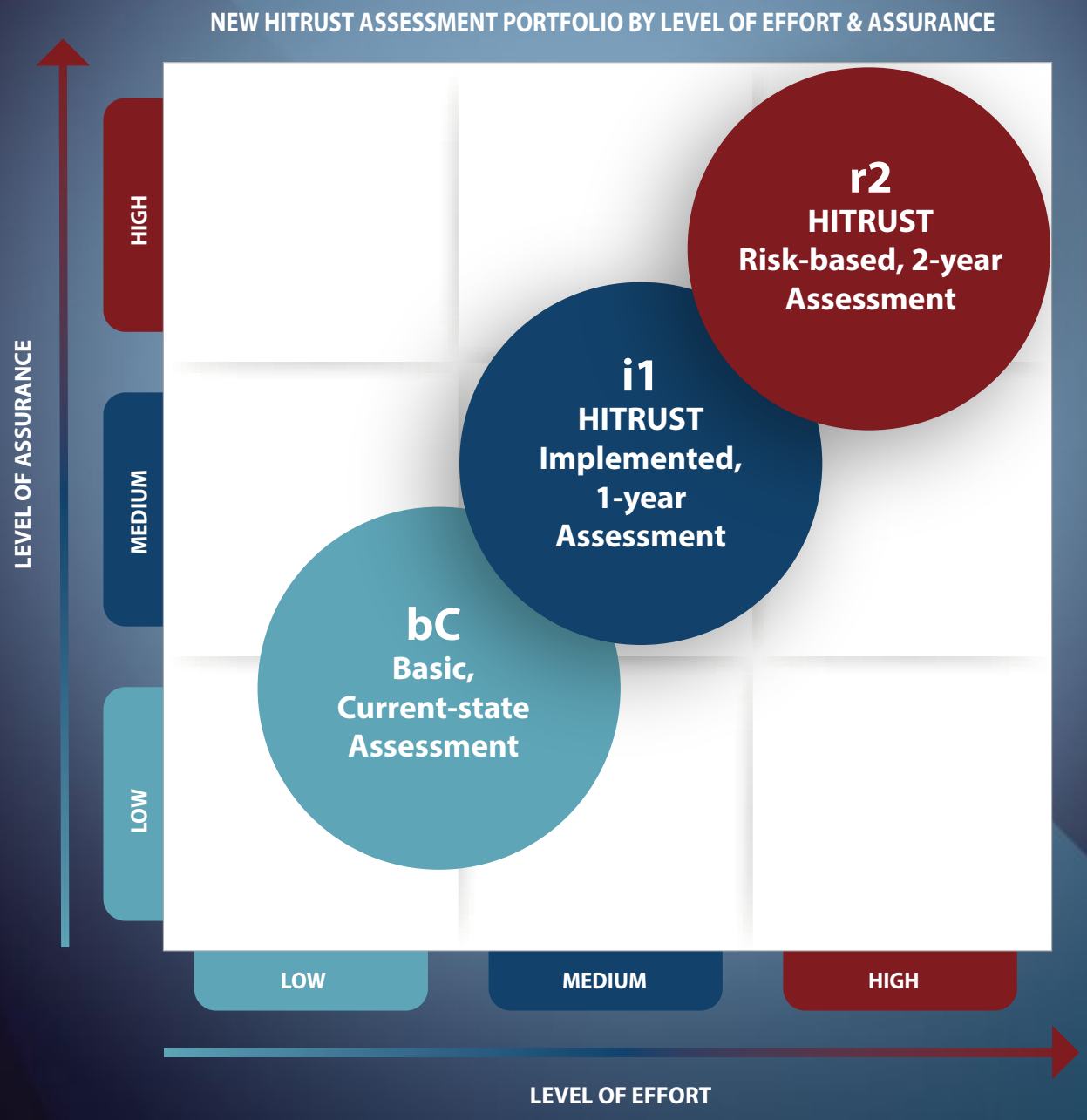
HITRUST

New HITRUST Assessment Portfolio Meets Varying Levels of Assurance with Better Quality and Reliability.

The HITRUST bC, i1, and r2 Assessments Offer a Full Range of Assurance Options to Meet Any Organizational Need.



>>>

Organizations perform information protection assessments for a variety of reasons. Usually, they have a need to assure internal or external stakeholders that their organization has effectively mitigated the risk of a data breach or other cyber event to adequately protect the organization's sensitive information or that of a relying third party.

Balancing the Needs of Ecosystem Assurances

The ecosystem of relying parties can include internal management, board of directors, customers, regulators, investors, or cyber insurers, just to name a few. They all need assurances they can trust and understand, which requires a transparent, impartial, and consistent evaluation of an organization's information protection controls.

In the absence of an objective and independent quality assurance report, relying parties will often ask their vendors to fill out proprietary questionnaires that are time-consuming and inefficient for both parties. And questionnaires only provide a low level of assurance since they are merely self-attestations.

Assessed entities must balance the needs of their stakeholders to provide more reliable assurances within the entity's acceptable parameters of time, cost, and effort to complete the assessment. Ideally, they need a single assessment that can satisfy multiple stakeholders and eliminate the need to fill out questionnaires.

ASSESSED ENTITIES NEED...

To provide **credible and reliable** information risk management assurances to internal and external stakeholders or relying parties

To **stop wasting time** performing duplicative assessments or **filling out proprietary questionnaires they receive from customers**

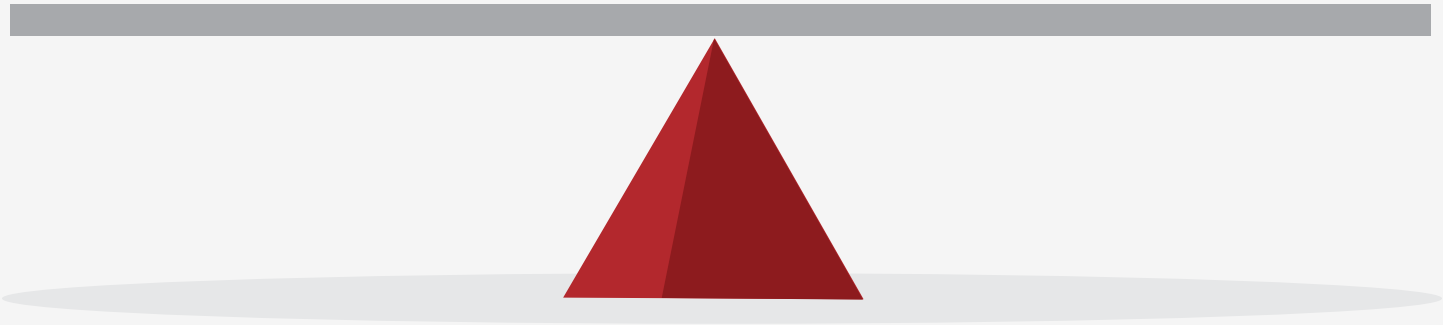
An industry recognized assessment mechanism that is appropriately rigorous to their level of risk allowing them to **"assess once, report many"**

RELYING PARTIES NEED...

Third-party assurance results they can trust to provide

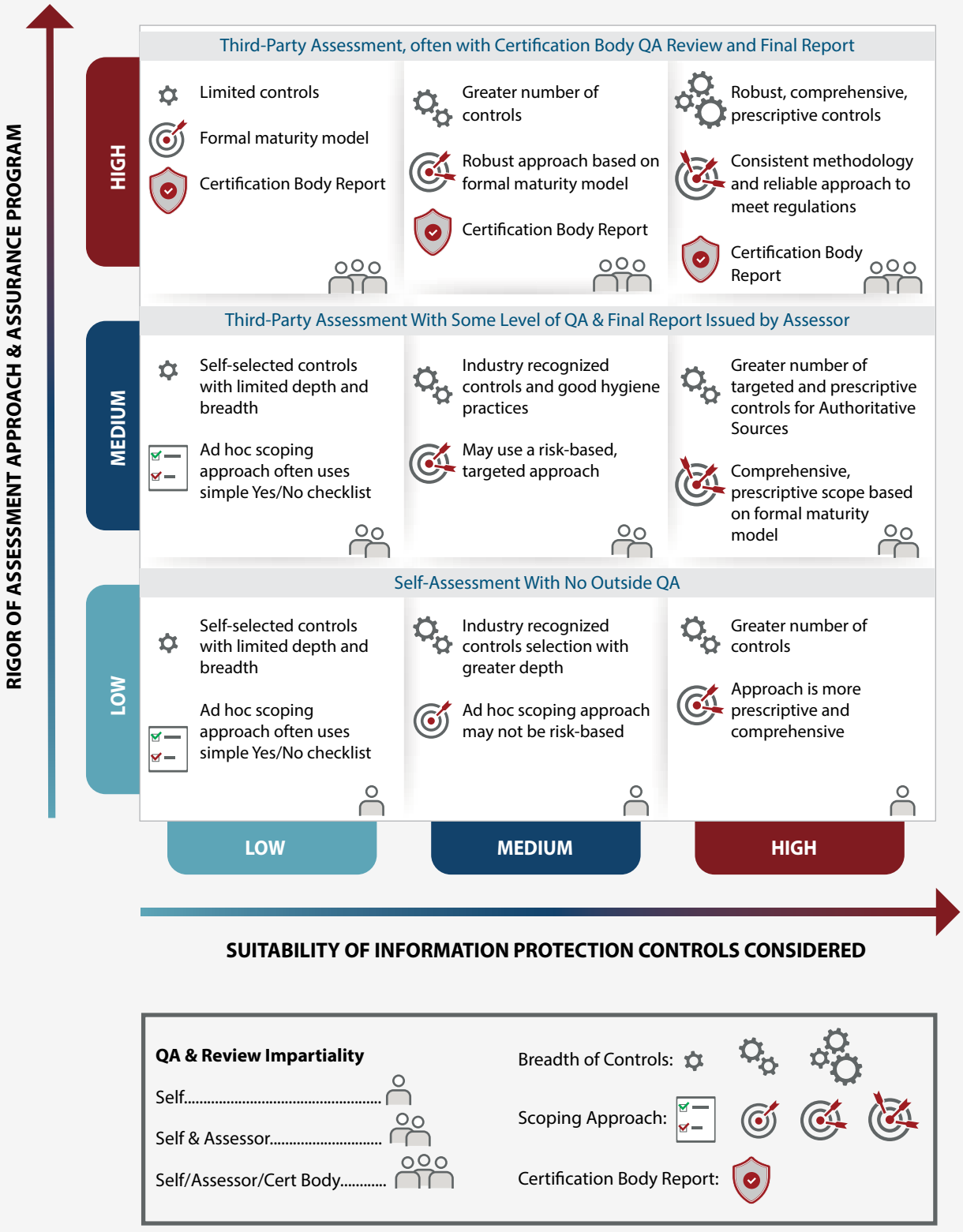
- Understanding of the **suitability** of the controls
- Full **transparency** on how the controls were selected and scored
- **Consistency** in assessor testing and evaluation methods
- An evaluation free of subjectivity or variability to bring more **integrity** to the report
- Increased levels of **impartiality,** ideally through a centralized quality assurance program and certification body

To effectively **manage third-party risk** across hundreds or thousands of vendors in the most efficient way



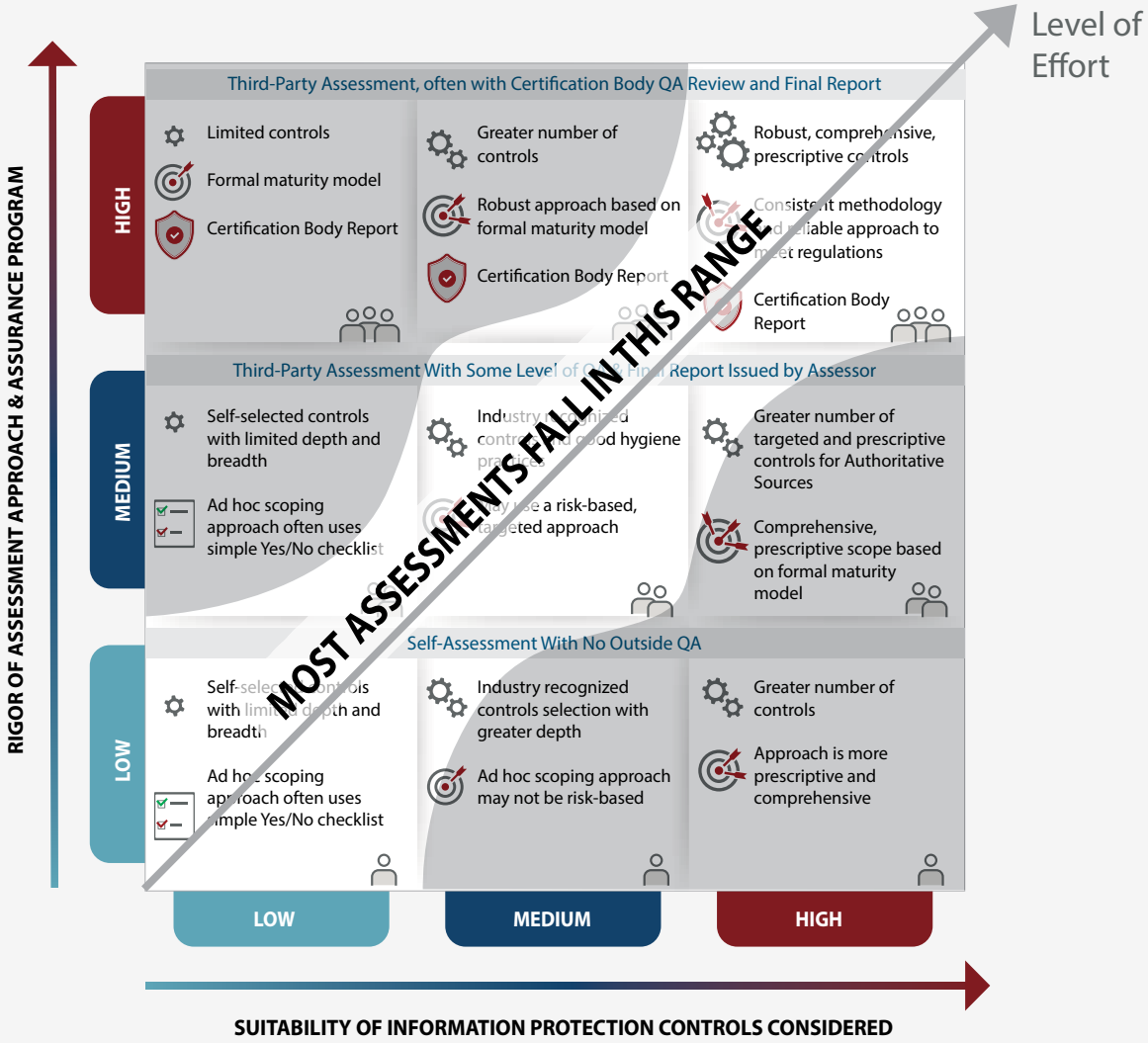
The Landscape of Information Protection Assessments

Existing information protection assessments deliver varying levels of assurance based on the suitability of incorporated information protection controls and the rigor of the assessment approach and assurance program. The control requirements range from limited to industry-recognized to comprehensive risk-based; and the level of rigor is largely driven by the breadth and level of third-party validation and quality assurance.



Level of Assurance is Highly Correlated with Level of Effort and Rigor

Most information protection assessments and certifications fall into a range of low-to-high levels of assurance which are highly correlated with the level of effort required to provide them. Low levels of assurance are usually characterized as having self-selected controls with limited depth and breadth and a basic approach that is self-attested. Moderate levels of assurance typically include industry-recognized, targeted control requirements that are tested and validated by an external assessor to provide general assurance of an organization's information control posture. Higher levels of assurance are attained when control requirements are more robust, comprehensive, and prescriptive, leveraging a formal risk-based maturity model that is validated through a centralized and consistent assurance program that includes validation and QA by both a third-party assessor and a recognized certification body.



The Need for Varying Levels of Assurance with Higher Reliability

Effectively managing information risk requires an understanding of potential risks and residual risk. HITRUST historically has focused on addressing gaps in the information assessment market–specifically by offering an assessment that is reliable, with high assurance, meaningful residual risk score, and that meets regulatory compliance requirements, such as HIPAA. The HITRUST Risk-Based, 2-year (r2) Validated Assessment (formerly the HITRUST CSF Validated Assessment) is widely recognized as the gold standard for reliable assurances.

It is generally known that most low- and moderate-level assurance assessments in the market have gaps, deficiencies, and inefficiencies that impact their reliability and usefulness. These gaps and deficiencies exist in the effectiveness and transparency of control requirements, consistency of evidence review, and integrity of the process.

The growing need for lower or moderate assurances is driven by considerations of purpose, time, and budget. Relying parties recognize that not every partner or vendor relationship warrants the level of assurance, or time and effort, to get an r2 Validated Assessment. However, they do require transparency, consistency, and integrity commensurate to the level of risk.

To meet these needs, HITRUST has added two new assessment options for low and moderate risk levels that will deliver a more Rely-Able™ assessment report than comparable options on the market. The new assessments will also improve efficiency by reducing the time and effort required to complete them. Effectively, HITRUST® is raising the bar on quality over the existing low and moderate assurance mechanisms in the market.

New HITRUST Assessment Portfolio: Better Quality and Reliability Across Every Assurance Level

All HITRUST assessments – new and existing – leverage a single assurance methodology, framework, assessment platform, and the Results Distribution System (RDS). This ensures consistency and efficiency across the assessment portfolio and makes it easier for assessed entities to transition to higher levels of assurance as their program matures. All HITRUST assessments aid in understanding the effectiveness of an organization's cyber preparedness and resilience.

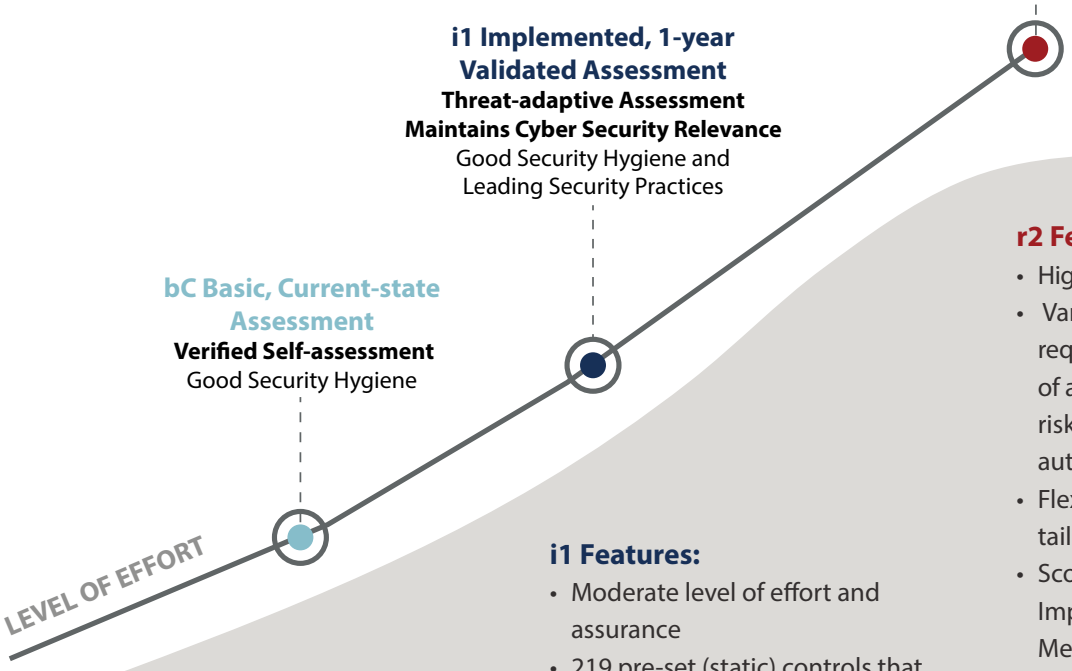
- **New! HITRUST Basic, Current-state (bC) Assessment** is a good hygiene self assessment and offers higher reliability than other self-assessments and questionnaires by utilizing the HITRUST Assurance Intelligence Engine™ (AI Engine) to identify errors, omissions, and potential deceit.
- **New! HITRUST Implemented 1-Year (i1) Validated Assessment** is a "best practices" assessment recommended for situations that present moderate risk. The i1 is a new-class of information security assessment that is threat-adaptive with a control set that evolves over time to deliver continuous cyber relevance. The i1 is designed to provide higher levels of transparency, integrity, and reliability over existing moderate assurance reports, with comparable levels of time, effort, and cost. **HITRUST i1 Readiness Assessment available.**
- **HITRUST Risk-based, 2-Year (r2) Validated Assessment** (formerly the HITRUST CSF Validated Assessment) remains the industry gold standard as a risk-based and tailorable assessment that continues to provide the highest level of assurance for situations with greater risk exposure due to data volumes, regulatory compliance, or other risk factors. **HITRUST r2 Readiness, Interim, and Bridge Assessments available.**

The i1 and r2 Assessments provide higher levels of assurance than the bC due to the transparency and consistency of how the controls are selected, scored, and validated by qualified external assessors and the HITRUST Assurance and Quality teams. The level of effort required for an i1 Certification is significantly less than an r2 Certification due to fewer control requirement statements, maturity levels (Implementation only), and evaluative elements.

HITRUST ASSESSMENT ATTRIBUTES

Higher Quality and Reliability at Every Level of Assurance

Guide to Selecting the Right HITRUST Assessment for Your Organization's Needs:



bC Features:

- Low level of effort and assurance
- Self-assessment only; verified by HITRUST Assurance Intelligence Engine
- 71 HITRUST CSF requirements
- 1 maturity level (Implemented)
- Targeted Coverage*: NISTIR 7621: Small Business Information Security Fundamentals

i1 Features:

- Moderate level of effort and assurance
- 219 pre-set (static) controls that leverage security best practices and threat intelligence
- Targeted Coverage*: 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)
- 1 maturity level (Implemented)
- Uses an external assessor's annual evaluation of control implementation along with HITRUST review and QA
- i1 Readiness Assessment available

r2 Features:

- High level of effort and assurance
- Varies from 198 – 2000 requirements (360 average in scope of assessments), based on inherent risk factors and included authoritative sources (optional)
- Flexible controls selection allows tailoring
- Scores: Policies, Procedures, Implemented, (and optionally) Measured, and Managed
- Full 5x5 PRISMA evaluation using a comprehensive scoring rubric
- Targeted Coverage*:
- NIST SP 800-53, HIPAA, FedRAMP, NIST CSF, AICPA TSC, PCI DSS, GDPR, and 37 others
- 2-year certification
- r2 Readiness, Interim, and Bridge Assessments available

**Targeted Coverage means substantial coverage is intended.*

Each HITRUST CSF Assessment Offers Unique, Industry-Leading Advantages, Including:

- Single HITRUST CSF Control Framework and One Control Library
- Best in Class MyCSF® SaaS Assessment Platform
- Consistent Approach
- Common Assurance Methodology
- Standard Report Formatting
- Supports Inheritance
- HITRUST Assurance Intelligence Engine™ (AIE) identifies errors, omissions, and potential fraud
- HITRUST Results Distribution System (RDS) shares assessment results with relying parties *(Coming Q2 2022)*
- And More...

HITRUST Results Distribution System (RDS): The Most Efficient Way to Share, Consume, and Utilize Third-Party Assessment Results *(Coming Q2 2022)*

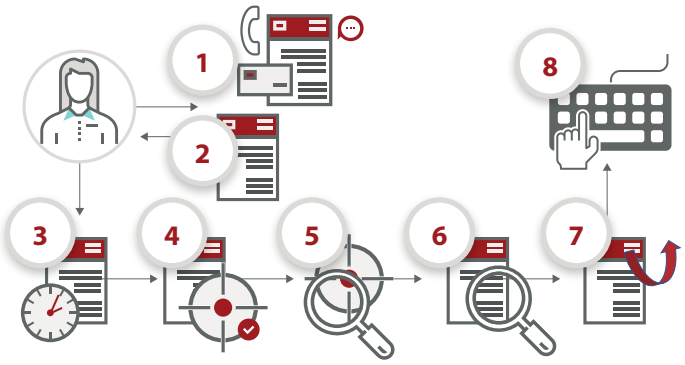
Those who manage risk know the current process of obtaining, interpreting, and analyzing assessment results from third parties is both time-consuming and highly inefficient. Today, third-party attested security and privacy assessment reports are delivered to the assessed entity in PDF format. In many cases, the assessed entity is asked to share their assessment report with a relying party (such as a customer, trading partner, or regulator) who then must manually review the report to identify the relevant information they need to make better-informed decisions about the risk an assessed entity presents to their organization.

At a minimum, the relying party wants to review the scope, scoring, and details on specific controls of interest. In many cases, they post or upload the entire report as documentation in a vendor risk management system for compliance purposes and then repeat this process annually with each vendor. This process is very time-consuming and labor-intensive, and it often prevents risk management professionals from identifying and focusing on those vendors that pose the greatest residual risk (risk left after controls are put in place and assessed).

The HITRUST Results Distribution System (RDS) addresses the highly inefficient process of obtaining, interpreting, and analyzing assessment results from third-party vendors

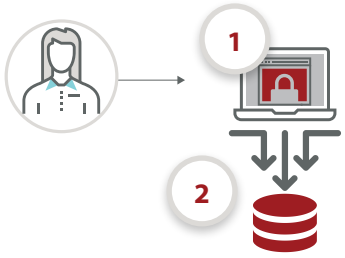
RDS allows assessed entities to share assessment results through a secure web portal or API so that relying parties can quickly and easily find and leverage the information they need to make better-informed decisions. *(Coming Q2 2022)*

EXISTING ASSURANCE EXCHANGE PROCESS



1. Request Third-Party Assurance Report
2. Receive Report
3. Validate Report is Current
4. Review Assessment Scope
5. Confirm Assessment Scope Meets Expectations
6. Analyze Assessment Findings and Conclusions
7. Manually Extract Relevant Data
8. Manually Enter Data into a Tracking System or Spreadsheet

PROCESS WITH THE HITRUST RESULTS DISTRIBUTION SYSTEM (RDS)



1. Review Dashboard Showing Predetermined Data of Interest
2. RDS Integrates with Vendor Risk Management (VRM) Systems and Governance, Risk and Compliance (GRC) Systems for Automated Tracking

Along with the HITRUST Results Distribution System, the expanded HITRUST Assessment Portfolio offers the highest levels of reliability to organizations across every industry by delivering impartial and consistent information security and privacy audits to organizations that interact with or rely upon sensitive information. No other assessments on the market bring together a centralized platform capable of securely distributing results to relying parties; a Quality Assurance (QA) function that helps ensure consistent results; plus, an innovative maturity model that effectively evaluates information protection.

New HITRUST Assessment Portfolio, Assurance Program, and Results Distribution System Provide Significant Benefits to Assessed Entities and Relying Parties

Benefits for Assessed Entities

- One framework, one assurance program, and one assessment tool to meet the information assurance needs of an entire enterprise
- HITRUST r2 Certification has been a competitive advantage with customers, as it provides significant assurances that can be relied upon by all stakeholders (e.g., Customers, Regulators, Cyber Insurance Underwriters)– and HITRUST expects the i1 Certification to achieve a similar status
- The HITRUST CSF® covers control requirements from more than 40 authoritative sources, such as ISO 27001, NIST 800-53, 800-171, HIPAA, GDPR, and more. To meet HITRUST's goal to "Assess Once, Report Many," the CSF can satisfy multiple stakeholders with one assessment and reduce the unnecessary efforts required to respond to third-party proprietary questionnaires.
- HITRUST Assessments allow for both internal and external inheritance to reduce the time and cost of testing with External Assessors
- Differentiates your organization relative to security and privacy posture and can facilitate potential new business partnerships with other organizations who require in-depth, third-party validated assurances
- Allows organizations to start with bC Assessment, and easily leverage that assessment when ready to move to the next level i1 as their Information Risk Management program matures
- Every assessment leverages the HITRUST Results Distribution System *(coming Q2 2022)*, which allows assessed entities to electronically share their assessment results with the stakeholders that they designate and eliminates all the back and forth to get the required information that customers' relying parties need
- Can minimize cyber insurance premiums

Benefits for Relying Parties

- **The most Rely-Able™ assurance reports due to suitability of controls, the rigor of the assurance program, and centralized oversight – HITRUST QAs 100% of the assessments.**
  - Ensures suitability of the controls
  - Transparency in how controls were evaluated and scored
  - Better accuracy based on a quasi-quantitative, rather than "qualitative" scoring
  - Consistency in how controls are evaluated
  - Integrity in the report with over 50 automated checks and 6 levels of independent and objective quality assurance reviews by HITRUST
- **Able to Run your Entire Security and Privacy Third-Party Risk Management Program through HITRUST**
  - Portfolio of Assessments to meet the needs of all vendors, regardless of risk level, company size, or purpose
  - No reason NOT to use HITRUST
  - Assurance framework to support more organizations on their assurance continuum journey
  - Receive all HITRUST assessment results electronically through the HITRUST Results Distribution System to radically improve efficiency over the outdated process of authenticating, requesting, sharing, and analyzing assessment results *(Coming Q2 2022)*

For more information, visit the HITRUST Assessments web page:
www.hitrustalliance.net/product-tool/hitrust-assessments/, call 855-448-7878, or contact sales@hitrustalliance.net