HITRUST® i1 Assessments

BARR ADVISORY

Table of Contents

3 Everything You Need to Know About the HITRUST i1 Assessment

4 What Is the HITRUST i1 Assessment?

4 Who Needs a HITRUST i1 Assessment?

5 The Difference Between i1 and r2 Assessments

6 BARR's Proven Process

7 Industry Coverage

7 Why Use BARR for HITRUST i1 Assessments

8 About BARR Advisory

8 Our Services

Everything You Need to Know About the HITRUST i1 Assessment

The demand for HITRUST certifications is at an all-time high. According to Health IT Security, since the founding of HITRUST in 2007, more than 80% of hospitals and health systems leverage HITRUST within their security practice. Recently, HITRUST announced the addition of the i1 Assessment, which adds another level of compliance solutions for healthcare organizations.

There's a reason for a majority of healthcare systems relying on HITRUST—it's considered the gold standard of frameworks. The framework is measurable, and includes more than 40 authoritative sources. If your company uses healthcare data, hosts ePHI in your system, or tests against HIPAA controls, you can feel confident in your organization's data security by obtaining a HITRUST certification.

What Is the HITRUST i1 Assessment?

The HITRUST i1 Assessment is a new one-year assessment designed to address the constantly developing threat landscape. The assessment is designed to be threat-adaptive—as the threat landscape evolves, the i1 requirements will also be updated to address future risks as they emerge. This ensures security controls are proactively adjusted on a regular basis to prevent cyberattacks, including ransomware and phishing.

The HITRUST i1 Assessment is valid for one year from its issuance date. Because the control set evolves over time, vendors will obtain the i1 on an annual basis. (Note: Entities with i1 assessments underway and those with a valid i1 Certification, will not be affected by i1 control selection updates until their next HITRUST assessment.

Who Needs a HITRUST i1 Assessment?

The HITRUST i1 Assessment is a good choice for any vendor looking to provide a moderate level of assurance on transparency, accuracy, consistency, and integrity. According to a press release from the Provider Third-Party Risk Management Council (PTPRM), some of the largest healthcare organizations and hospitals will require moderate risk vendors to obtain a HITRUST i1 Assessment.

The PTPRM is comprised of prominent chief information security officers (CISOs) from leading health systems throughout the United States, including Allegheny Health Network, Cleveland Clinic, University of Rochester Medical Center, Tufts Medicine, Shriner's Hospitals for Children, and Mayo Clinic. Members of the Council will instruct moderate risk vendors to provide assurances through the HITRUST i1 certification in place of other compliance mechanisms like a SOC 2 report.

This move expanded the Council's previous third party assurance guidance beyond highrisk vendors with protected health information (PHI) to now include moderate risk vendors with personally identifiable and confidential information. According to spokespersons from PTPRM, this new requirement aims to simplify and standardize the assurance process for both vendors and healthcare organizations.

The Difference Between i1 and r2 Assessments

The HITRUST r2 Assessment is a risk-based two-year assessment that offers a high level of assurance. It requires a higher level of effort and is a good choice for organizations with a significant volume of sensitive data that requires maximum assurance. In comparison, the i1 Assessment is a good choice for organizations with only a moderate level of risk to be tested against best practices for security.

The r2 Assessment addresses five key areas:

- Policy
- Procedures
- Implementation
- Measurement
- Management

Think of the HITRUST i1 Assessment as a scaled down version of the r2 Assessment.

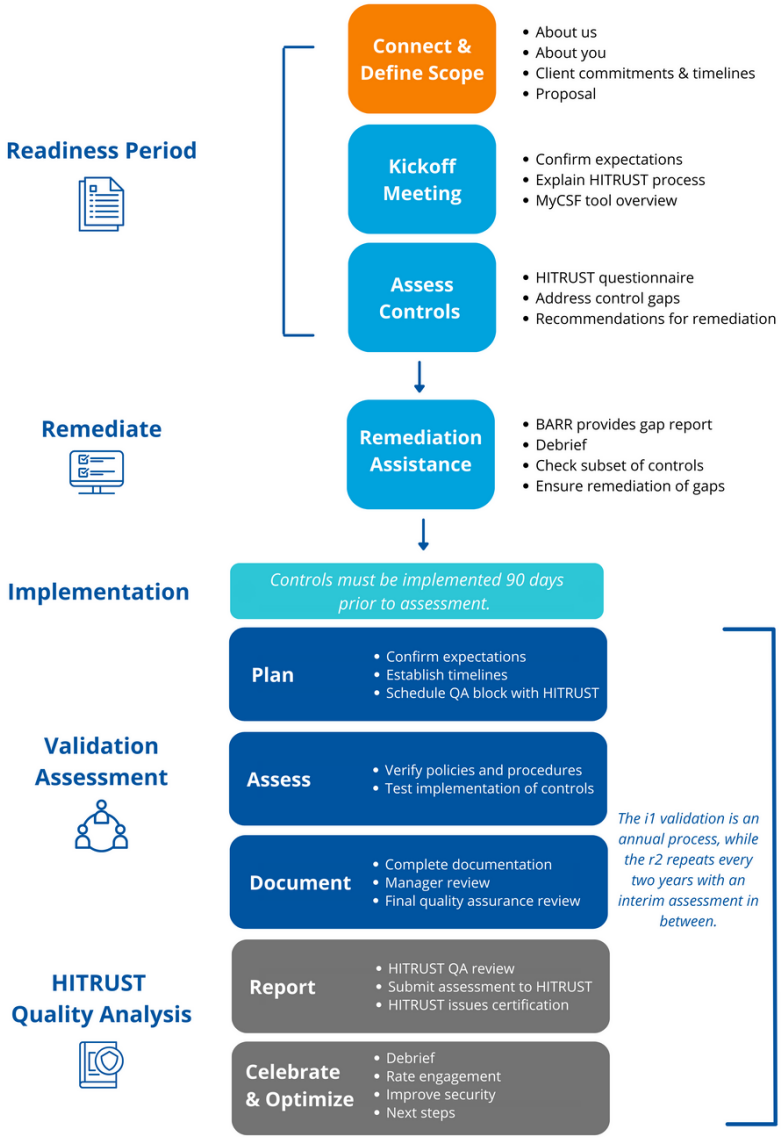
Instead of focusing on all five areas, the i1 Assessment hones in on implementation of each control alone. It's a smaller undertaking, and allows small to medium-sized organizations with less support staff to obtain a moderate level of assurance through HITRUST.

Organizations should choose an i1 over and r2 when they need to become HITRUST certified, but don't yet have a team dedicated to the implementation of a big project such as the r2. The i1 serves as a perfect stepping stone for organizations that want to implement a set of foundational controls, become HITRUST certified, and look into the future for tackling an r2 Assessment.

BARR's Proven Process

BARR's proven process helps organizations simplify the HITRUST i1 Assessment with a three-step process:

- **Readiness Phase:** BARR tests your environment against the i1 controls and establishes a baseline.
- **Remediation Phase:** BARR provides simple and actionable steps for your organization to close identified gaps.
- **Validation/Certification Phase:** Once your organization is ready, BARR tests your environment against the HITRUST controls and submits the assessment to HITRUST for certification.



Industry Coverage

The HITRUST i1 Assessment provides provides targeted coverage for a number of industry standards including:

- NIST 800-171
- GLBA Safeguard Rule
- HIPAA Security Rule
- Health Industry Cybersecurity Practices (HICP)
- U.S. Department of Labor EBSA Cybersecurity Program Best Practices

Why Use BARR for HITRUST i1 Assessments

When it comes to HITRUST i1 Assessments, BARR has the experience and knowledge to get the job done. Companies that handle the most sensitive data trust BARR to successfully guide them through the HITRUST i1 Assessment.

What sets BARR apart?

We Care
As your security partner, we take the time to listen and understand so you can achieve lasting cyber resilience.

We Keep it Simple
We take the complexity out of compliance without compromising quality.

We're Approachable
Our expertise is matched only by our accessibility.

About BARR Advisory

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

Our Services

- **SOC Examinations**
  [SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]
- **Healthcare Services**
  [HIPAA/HITRUST]
- **ISO 27001 Assessments**
- **FedRAMP Security Assessments**
- **PCI DSS Assessment Services**
- **Penetration Testing and Vulnerability Assessments**
- **Virtual CISO Services**
- **Compliance Program Assistance**

Connect with BARR

Want to learn more about the HITRUST i1 Assessment and how it can benefit your organization?

Contact us today, or join us for an Open House every Tuesday from 11 a.m. to noon CST for an Q&A and discussion of the process and benefits of obtaining HITRUST certification.