SIMPLIFYING HEALTHCARE COMPLIANCE

Essential Facts for Achieving HITRUST Certification

BARR ADVISORY

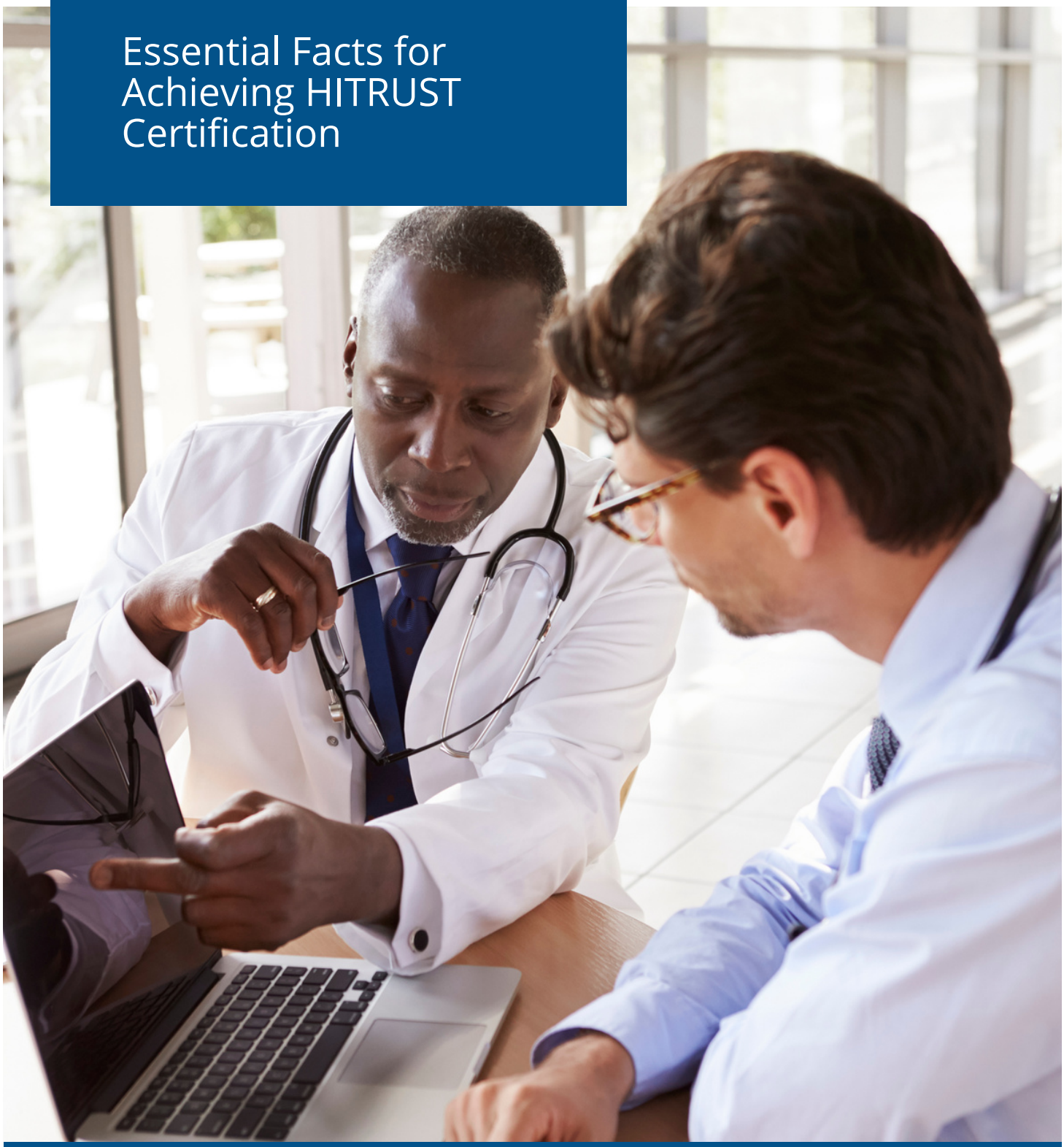

Table of Contents

3 Introduction

4 HITRUST Assessment Levels

5 HITRUST Risk Management Solutions

6 HITRUST Traversable Assessment Portfolio

7 Notable Statistics and Facts about HITRUST

8 About BARR Advisory

Introduction

The HITRUST Alliance recently released a new resource titled HITRUST: Did You Know?—a comprehensive guide outlining ten essential HITRUST facts. The guide is designed to be a resource that provides organizations with the knowledge and insights necessary to successfully navigate the HITRUST certification process.

As the healthcare industry's most widely adopted security framework, HITRUST CSF provides a prescriptive approach to simplifying security requirements. Benefits of a HITRUST certification include protecting patient data and other sensitive information, access to ongoing improvement plans, and a way to differentiate your organization from the rest.

While navigating healthcare compliance might seem like a challenge, BARR is here to help simplify the process and provide expert guidance. Let's dive into the facts covered in the HITRUST: Did You Know? guide so you can feel confident in moving forward to achieve your HITRUST goals.

HITRUST Assessment Levels

The HITRUST portfolio includes three cybersecurity certification options based on an organization's complexity, risk profile, and needs:

The HITRUST Essentials (e1) Validated Assessment
Addresses foundational cybersecurity hygiene.

The HITRUST Implemented (i1) Validated Assessment
Offers a more comprehensive level of assurance than the e1, with more controls in scope.

The HITRUST Risk-Based (r2) Validated Assessment
The most comprehensive assessment in the HITRUST portfolio.

The three levels of assurance offered by the HITRUST assessment portfolio build on a common framework, so you can begin with a less comprehensive assessment and move up to a more comprehensive one without starting over.

For example, if your organization begins with the e1 Assessment, you can upgrade to the more comprehensive i1 Assessment or r2 Assessment without losing the time and effort invested in obtaining the e1.

The e1 Assessment is designed to cover basic foundational cybersecurity practices based on 44 controls. It incorporates HITRUST cyber threat adaptive methodology to ensure relevancy and acts as an entry-level assessment.

> *The e1 Assessment is designed for faster cybersecurity certification, enabling some organizations to complete the assessment in less than a month.*

Additionally, different vendors can opt for different types of assessments:

- The e1 is ideal for startups and organizations with limited risk profiles.
- The i1 can be a good fit for mid-level vendors demonstrating leading security practices.
- The r2 is best suited for vendors needing expanded control tailoring or regulatory compliance with authoritative sources.

HITRUST Risk Management Solutions

To ensure HITRUST assessments remain relevant as the cyber threat landscape evolves, HITRUST regularly evaluates cyber threat intelligence for effective risk management. It identifies potential gaps in control coverage in its assurance portfolio and regularly publishes updates to keep up with the changing needs of organizations.

Unlike other standards and risk management frameworks, HITRUST assessments are cyber threat-adaptive. This means they regularly stay current on relevant risks, avoiding the need for organizations to distribute security questionnaires.

With the HITRUST Results Distribution System (RDS), organizations save time and effort by eliminating mundane tasks like locating assessment results and manually entering a limited data set in their Third-Party Risk Management (TPRM) solution. RDS can post electronic assessment details into TPRM solutions promptly and efficiently, enabling better compliance and analytics.

At at-a-glance benefits of the HITRUST RDS:

- Reduces the inefficiencies in current approaches by **sharing assurance results** more efficiently
- **Works within your TPRM** system to improve data access, security, and storage
- Unlocks the **power of analytics** by locating and extracting essential information faster
- Helps **automate TPRM** and vendor management activities
- **Enables electronic delivery** of assessment results to specific individuals or organizations via the HITRUST Application or API interface
- Allows recipients to **set alerts** based on various assessment thresholds

HITRUST Traversable Assessment Portfolio

HITRUST CSF can be tailored to an organization's requirements based on specific organizational, technical, and compliance risk factors. One HITRUST assessment can be used to satisfy many reporting requirements, saving organizations time and money.

One HITRUST certification can include the integration of requirements from many authoritative sources like:

Organizations can also use HITRUST effectively across any industry—not just healthcare. The level of integration and prescriptiveness provided by the framework, make the HITRUST CSF the easy choice for organizations in any industry.

HITRUST protects all types of data and information, including:

- Electronic protected health information (ePHI)
- Personally identifiable information (PII)
- Payment card data
- Proprietary information
- Other sensitive information

BARR's Audit Once, Report Many Approach

BARR offers an audit once, report many approach to security and compliance—meaning your organization can achieve multiple reports with just one audit. For example, HITRUST can serve as a risk assessment for the ISO 27001 audit. If your organization has HITRUST in place, BARR can provide expert guidance and feedback on how to close any identified gaps prior to an ISO 27001 audit.

Additionally, a HITRUST certification can help satisfy the requirements of a SOC 2 report. The AICPA's trust services criteria align with the CSF criteria, which allows us to issue SOC 2 plus HITRUST in a collaborative reporting model.

Notable Statistics and Facts about HITRUST

HITRUST CSF has many benefits for organizations of all sizes and across industries. Take a look at some of the most notable statistics and facts that demonstrate BARR and HITRUST's' commitment to a simplified and effective certification process.

One of only a handful of firms

BARR is one of only a handful of firms in the U.S. eligible to perform audits against all three highest-regarded standards—HITRUST, ISO 27001, and SOC 2.

Reduce time and effort by up to 85%

Organizations can reduce the time and effort needed to obtain a HITRUST certification by up to 85% with the HITRUST Shared Responsibility and Inheritance Program.

Dozens of security and privacy regulations

The HITRUST CSF integrates and harmonizes dozens of privacy and security regulations and standards to ensure complete coverage of controls.

2,000+ control requirements

As one certifiable framework, HITRUST includes 2,000+ control requirements in a fully tailorable and flexible control library, which is harmonized and mapped to each authoritative source.

Considered the "gold standard"

Because of their comprehensive approach, HITRUST certifications are broadly considered the "gold standard" in providing assurance of risk management and compliance.

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**
- **Cybersecurity Consulting and vCISO Services**
- **Compliance Program Assistance**

Connect with BARR

Contact us to speak with a HITRUST specialist and learn more about how BARR can help your organization begin or continue your HITRUST certification journey.