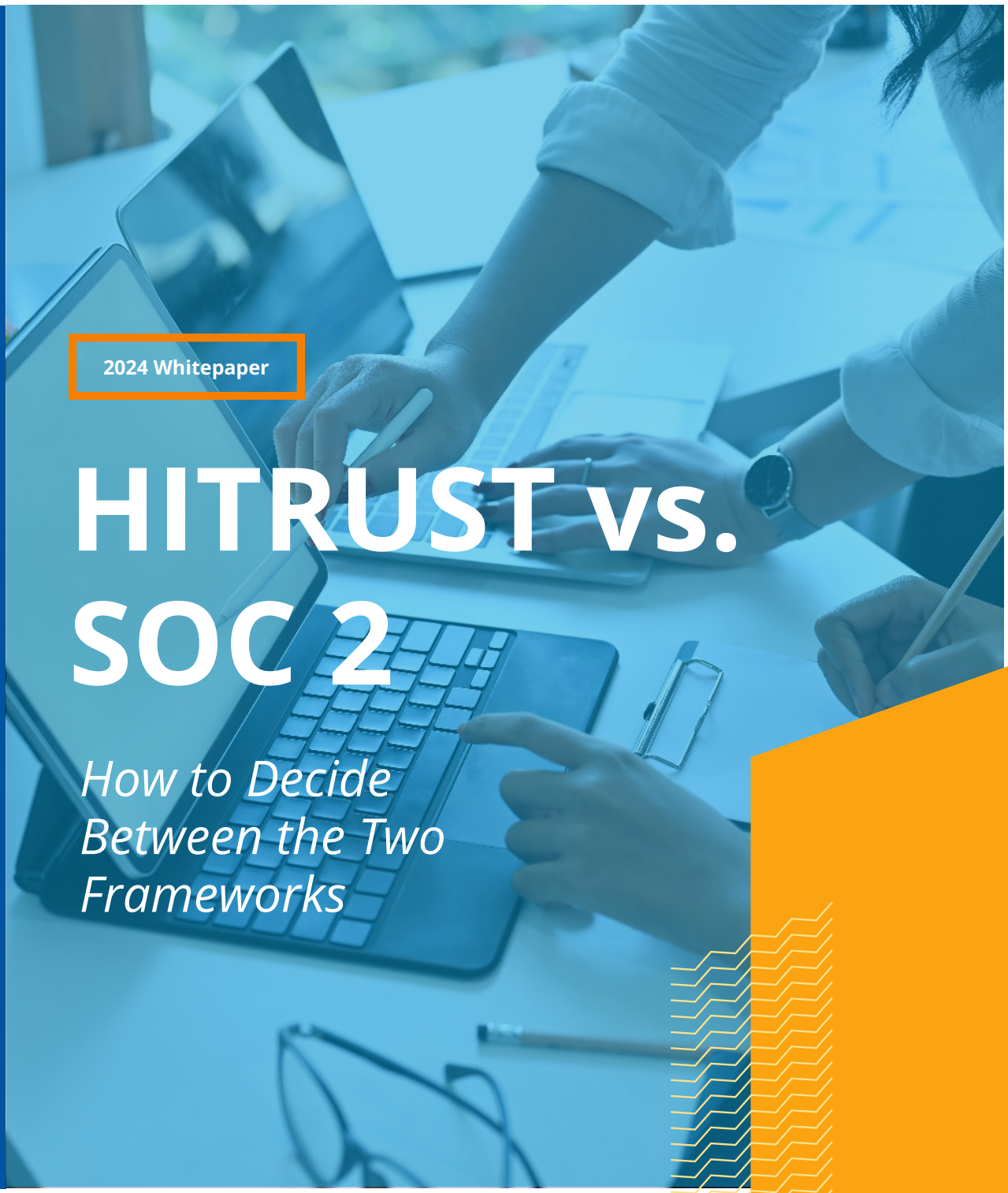
BARR ADVISORY



2024 Whitepaper

HITRUST vs. SOC 2

How to Decide Between the Two Frameworks

Table of Contents

Introduction

In the rapidly evolving landscape of data security, organizations are increasingly challenged to establish and maintain robust compliance frameworks that safeguard sensitive information. HITRUST and SOC 2 have emerged as essential compliance frameworks to help organizations communicate their security and compliance posture with key stakeholders.

As industries strive to meet the growing demands of stakeholders and regulators, understanding the nuances between HITRUST and SOC 2 becomes imperative. While both frameworks share common objectives in enhancing data protection and risk management, they can differ significantly in their scopes, degree of effort required to obtain compliance, and applicability.

> ***When deciding between HITRUST and SOC 2, you need to ask yourself: What are your stakeholders looking for? What level of effort are you willing to put into security to provide that trust to your customers?***
>
> **Steve Ryan, Head of Healthcare and Attest Services Manager**

This whitepaper aims to provide a comprehensive examination of the distinctions between HITRUST and SOC 2, arming organizations seeking clarity on the most suitable framework with the information necessary to make an informed decision.

The Key Differences

SOC 2 reports and HITRUST certifications aren't the same regarding control suitability, consistency, integrity, and transparency. It's a common misconception that SOC 2 is a certification. SOC 2 is an attestation resulting in a report, while HITRUST is a certification that provides reliability, quality, and transparency.

SOC 2: Following an audit over the AICPA's trust services criteria, a third-party firm issues a SOC 2 report that contains its opinion.

HITRUST: A HITRUST certification is based on a framework of authoritative sources, offering reliable assurances.

Every HITRUST assessment is based on the HITRUST CSF, an objective and quantitative cybersecurity framework. The HITRUST CSF maps each control to multiple authoritative sources, including HIPAA and GDPR. HITRUST can be mapped to SOC 2, too.

The effort and resources needed to achieve these frameworks can vary. With the addition of the e1 assessment to the HITRUST portfolio, the time, talent, and financial resources required to become HITRUST certified is comparable to getting a SOC 2. A HITRUST i1 or r2 Assessment can be a considerable effort over a SOC 2.

Read on to find out more about each of these frameworks.

"HITRUST i1 and r2 Assessments are a considerable effort over the SOC 2 but allow for much more trust and reliability over the SOC 2 attestation report. With these HITRUST Assessments, you're getting a certification over an attestation report, which is therefore much more rigorous."
– Steve Ryan

HITRUST: An In-Depth Look

HITRUST Overview

The HITRUST Common Security Framework (CSF) was developed in collaboration with healthcare and information security professionals to provide a prescriptive framework to simplify security requirements. It is the most widely adopted security framework in the U.S. healthcare industry. HITRUST offers a readiness assessment and a validated assessment against the CSF. A validated assessment is conducted by a HITRUST Authorized External Assessor, like BARR, and is the only assessment that produces a validated certification report. With extensive experience in healthcare audit services, we'll help your organization through the HITRUST CSF assessment process. There are a few different types of HITRUST certifications you can choose to pursue. Let's take a closer look at the e1, i1, and r2 Assessments and how they can benefit your organization.

HITRUST e1 Assessment

The HITRUST Essentials, 1-year (e1) Assessment is a low-effort yet reliable assessment that helps organizations focus on foundational cybersecurity controls and prepares them for the most critical cybersecurity threats.

The e1 Assessment can serve as a stepping stone to more comprehensive and higher-effort assessments such as the HITRUST i1 Assessment or r2 Assessment. With only 44 controls, it is significantly more attainable than other cybersecurity assessments. Similar to other HITRUST assessments, the e1 Assessment is threat-adaptive, which means that as the threat landscape evolves, the requirements will also proactively shift to address risks as they emerge.

The e1 Assessment is valid for one year from its issuance date. After that year, BARR experts recommend building on the established cybersecurity foundation with a higher level assessment.

Who Needs the e1 Assessment?

As the minimum level of cybersecurity assurance in the HITRUST framework, the e1 Assessment is an excellent first step for any organization looking for validation of essential cybersecurity controls that plans to progress to more robust assessments in the future. BARR experts recommend the e1 Assessment to startups or other organizations that are just getting started in their cybersecurity journey.

While the e1 Assessment reliably demonstrates an organization's commitment to the basics, it doesn't provide coverage of compliance related to laws like HIPAA or other leading cybersecurity practices.

HITRUST: An In-Depth Look

HITRUST i1 Assessment

The HITRUST Implemented, 1-year (i1) Assessment is designed to address the constantly developing threat landscape. As a threat-adaptive assessment, the i1 requirements will also be updated to address future risks as they emerge.

The Provider Third Party Risk Management Council, which is composed of prominent chief information security officers from leading health systems and provider organizations, announced that any moderate-risk vendors that want to work with them must obtain the HITRUST i1 Certification. The Council's governing organizations include Cleveland Clinic, Mayo Clinic, and Tufts Medicine.

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. With the new HITRUST v11 updates, the i1 Assessment decreased controls from 219 to 182, which helps accelerate the time it takes to complete certification. It's important to note the level of effort to achieve and maintain HITRUST i1 Certification can be reduced up to 45% over the course of two years.

Who Needs the 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. It allows smaller organizations with less support staff to become HITRUST certified. The reason for this is the i1 only addresses the implementation of each control, as opposed to the r2, which requires a policy, procedure, and the actual implementation of the control.

Did You Know?

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, you can begin with the HITRUST e1 Assessment that covers foundational cybersecurity hygiene practices and move to the more comprehensive HITRUST i1 Assessment or r2 Assessment without losing the time and effort invested in obtaining the e1.

HITRUST: An In-Depth Look

HITRUST r2 Assessment

The HITRUST Risk-based, 2-year (r2) Assessment offers the highest level of assurance and requires significantly more effort than the e1 and i1. Within the updated v11 HITRUST CSF framework, i1 Assessments now serve as the baseline for the r2 Assessments, which has reduced the number of controls in scope considerably.

The r2 Assessment is valid for two years with an interim period in between and addresses five key areas—policy, procedures, implementation, measurement, and management—and over 200 controls.

Who Needs the r2 Assessment?

The r2 is the right assessment for established organizations that obtain a significant volume of sensitive data and protected health information (PHI) to keep secure. As the most comprehensive of the HITRUST assessments, the r2 is key for organizations that need high-level assurance and have the necessary resources and team dedicated to complete a larger, more complex assessment.

Take a look at this overview of key features of each assessment to decide which one is right for you.

e1 Assessment

- Takes 3 months to obtain
- Less expensive
- Only 44 controls
- Provides low assurance
- Stepping stone to other assessments

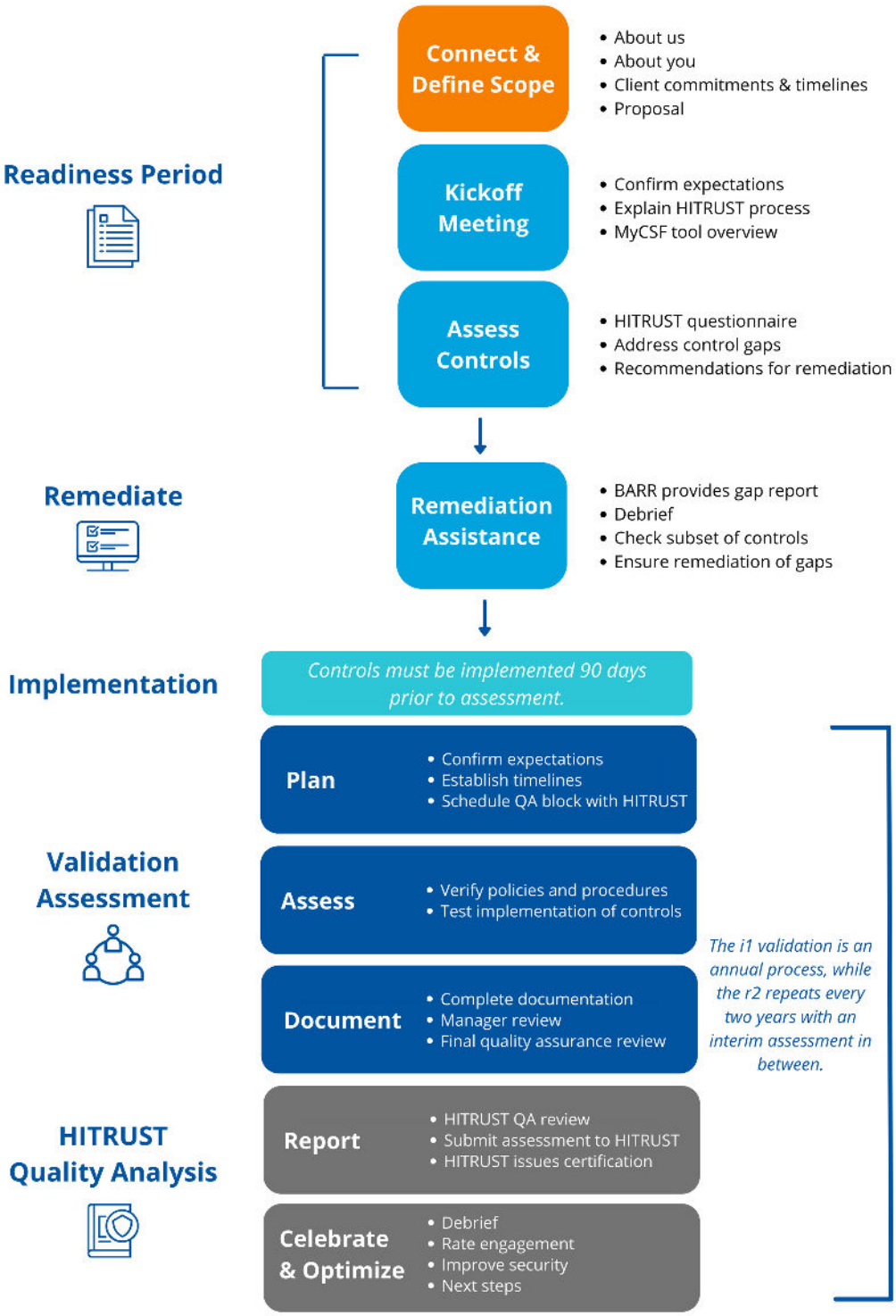
i1 Assessment

- Takes 6-12 months to obtain
- 182 controls
- Provides moderate assurance
- Smaller undertaking than the r2 Assessment

r2 Assessment

- Takes 18-24 months to obtain
- Over 200 controls
- Provides highest level of assurance

The HITRUST Proven Process



SOC 2: Everything You Need to Know

An Overview of SOC 2

The System and Organization Control (SOC) 2 examination reports on one or any combination of the AICPA's trust services criteria including security, availability, processing Integrity, confidentiality, and privacy.

It demonstrates an organization's commitment to its customer requirements and cybersecurity best practices.

The SOC 2 report is intended to meet the needs of a broad range of users who need detailed information and assurance about the controls at a service organization. The report can play an important role in oversight of the organization, vendor management programs, and internal corporate governance and risk management processes.

The report can be distributed to an organization's stakeholders including user entities, CPAs providing services to such user entities, regulators, and business partners.

Trust Services Critera

Organizations have the ability to choose one or a combination of the five AICPA Trust Services Criteria depending upon their customer needs:

- **Security:** The system is protected against unauthorized physical and logical access.
- **Availability:** The system is available for operation and used as agreed upon.
- **Processing Integrity:** System processing is complete, accurate, timely and authorized.
- **Confidentiality:** Information designated as confidential is protected as agreed upon.
- **Privacy:** Personal information is collected, used, retained, disclosed, and/or destroyed in accordance with established standards.

SOC 2: Everything You Need to Know

Types of SOC Reports

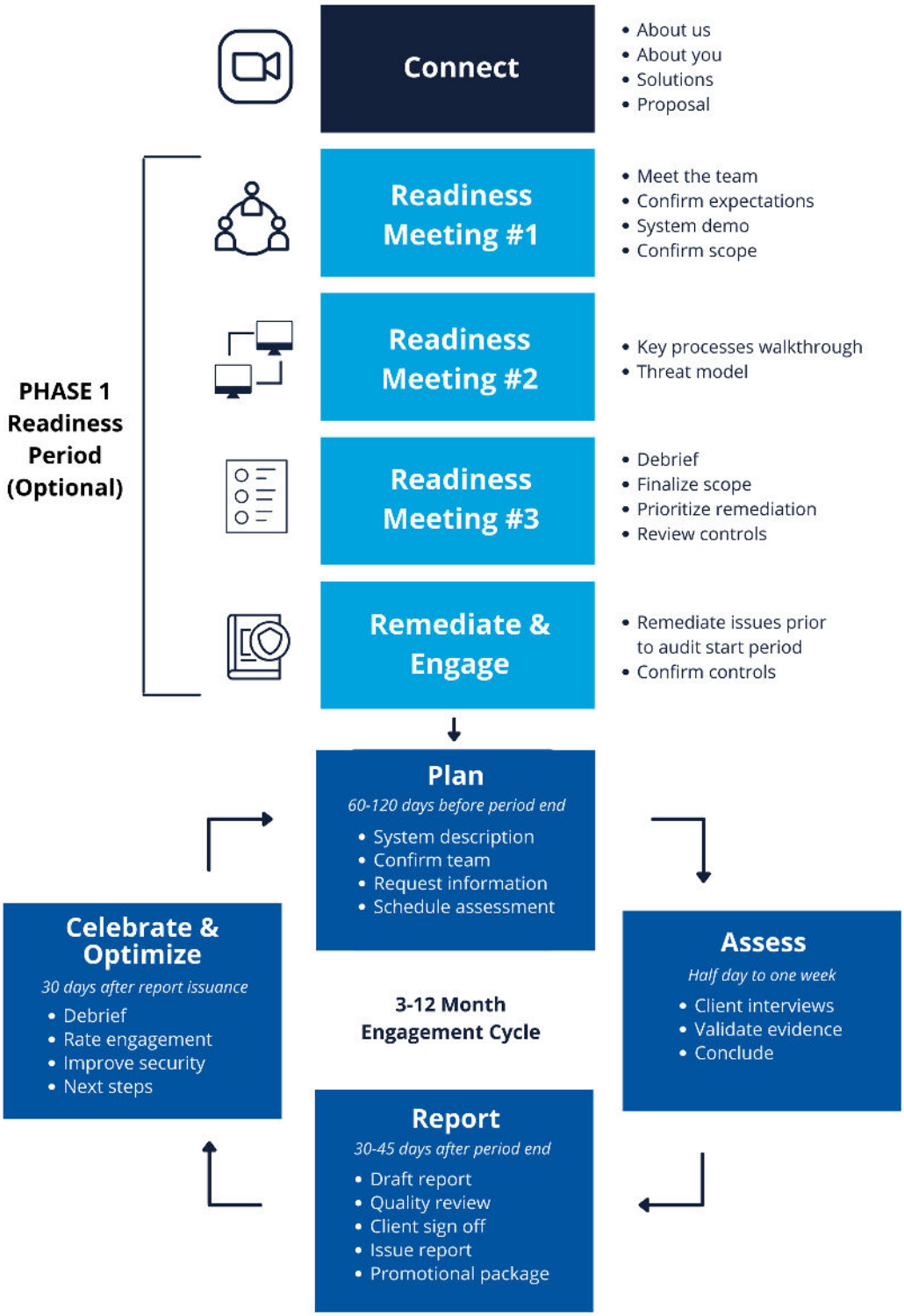
There are two types of SOC 2 reports:

SOC 2 Type 1: The SOC 2 Type 1 Report (referred to as a point-in-time report), includes an opinion over the suitability of the design of controls at the service organization at a specific point in time. An initial Type 1 report often serves as the starting point for subsequent Type 2 reviews.

SOC 2 Type 2: The SOC 2 Type 2 Report (referred to as a period-of-time report) includes an opinion over the suitability of the design of controls at the service organization and the operating effectiveness of the controls throughout a specified period of time. This type of report is often issued annually.

No matter what type of SOC 2 report you are working toward, we are committed to guiding you through every stage of your SOC 2 audit from kickoff to final deliverable and everything in between. Read on to learn more about our proven process to see how we do it.

The SOC 2 Proven Process



The Case for Both

Test Once, Report Many

Depending on the needs of your stakeholders, some organizations may benefit from pursuing both HITRUST and SOC 2. Having both a HITRUST certification and SOC 2 report not only increases consumer trust, it also enhances your brand value. You'll stand out as an organization that takes security seriously, while instilling the most confidence in your customers and stakeholders.

That's where we come in—BARR is proud to be one of only a handful of firms in the country that is certified to perform all three of the highest-regarded security audits: ISO 27001, HITRUST, and SOC 2.

With a test once, report many approach, BARR can help your organization achieve both SOC 2 and HITRUST seamlessly.

As an external assessor, BARR can complete all the necessary tasks and data collection processes for HITRUST and SOC 2 audits at the same time. If an organization has already achieved a HITRUST certification, it's easy to map the controls that are already in place to SOC 2 requirements, especially when the assessment data already exists and is immediately available in the MyCSF portal. That way, the organization's compliance team doesn't need to go through redundant activities or conversations.

Since the AICPA's trust services criteria align with the HITRUST CSF criteria, BARR is able to issue SOC 2 plus HITRUST in a collaborative reporting model.

"With BARR's test once, report many approach to auditing, organizations can obtain both a SOC 2 report and HITRUST certification easily. They can feel like they're only being audited once while getting two different reports with different values."
– Steve Ryan

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

Want to learn more about our SOC 2 and HITRUST services? Contact us today.