AUDIT ONCE, REPORT MANY:

BARR IS ELIGIBLE TO PERFORM AUDITS FOR ISO 27001, HITRUST, AND SOC 2

At BARR Advisory, we exist to create a world of trust through cyber resilience. One of the ways we do that is by taking an ***audit once, report many*** approach to our attestations to add real value to our clients' experience. By mapping to multiple controls across frameworks like ISO 27001, SOC 2, and HITRUST, we create efficiencies that help organizations achieve compliance faster and easier.

In fact, BARR is one of only a handful of firms in the country that are certified to perform all three of the highest-regarded security audits: **ISO 27001, HITRUST, and SOC 2**.

Let's dive into what that means:

In 2021, BARR Certifications (the certification arm of BARR Advisory) earned the prestigious ISO/IEC 17021-1 accreditation for certification to ISO/IEC 27001 from the ANSI National Accreditation Board (ANAB). Accreditation by the ANAB—the largest multidisciplinary accreditation body in North America—validates BARR's competence and independence in assessing the people, processes, and technology within a service organization's ISMS.

Together, BARR Certifications and BARR Advisory are one of only a handful of firms in the nation that meet requirements of the ANAB and the American Institute of Certified Public Accountants (AICPA) to issue ISO/IEC 27001 certifications with a SOC 2 audit report and HITRUST certification.

HOW DO THESE THREE FRAMEWORKS BENEFIT ORGANIZATIONS?

All of these three frameworks ultimately help organizations improve their security posture. However, they each differ a little bit through the engagement process and in their final deliverables:

ISO 27001

ISO/IEC 27001 is the globally-accepted standard that defines the requirements of an Information Security Management System (ISMS). ISO/IEC 27001 certification from an accredited certification body means an organization has demonstrated adherence to those requirements.

SOC 2

The SOC 2 exam 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 consumer requirements and cybersecurity best practices.

HITRUST

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.

AUDIT ONCE, REPORT MANY: WHAT IT REALLY MEANS

As an external assessor, BARR can complete all the necessary tasks and data collection processes for HITRUST, SOC 2, and ISO 27001 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 ISO 27001 requirements, especially when the assessment data already exists and is immediately available in the MyCSF portal.

Since ISO 27001 auditors cannot provide guidance on how to fix issues or mitigate gaps, HITRUST CSF can serve as a risk assessment for the ISO 27001 audit. If your organization has HITRUST in place, your external assessor can help by providing expert guidance and feedback on how to close any identified gaps ahead of time. This can help avoid potential nonconformities during your ISO 27001 audit.

When all of the information and data needed for an ISO 27001 audit is readily available in the HITRUST MyCSF platform, the organization's compliance team doesn't need to go through redundant activities or conversations. In addition to ISO 27001, a HITRUST certification can help satisfy the requirements of other assessments like SOC 2. With SOC 2, for example, 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.

Similarly, BARR can leverage your SOC 2 report to include ISO controls, and vice-versa. This means that organizations seeking ISO/IEC 27001 certification and a SOC 2 audit now have a unified team of auditors to perform both assessments.

WHAT ARE THE BENEFITS OF OBTAINING MULTIPLE REPORTS?

Now that you understand how the audit once, report many process works, you may be thinking "Why would I need more than one of these reports?"

The answer depends on the unique needs of your organization. For example, having both an ISO certification and SOC 2 report not only increases consumer trust, it also enhances your brand value. You'll stand out as an organization who takes security seriously, while instilling the most confidence in your customers and stakeholders.

Working to obtain these reports simultaneously also significantly reduces the time and resources required to achieve compliance. According to BARR experts, organizations can save up to **90% of the time** needed to achieve two reports with the *audit once, report many* process.

BENEFITS OF AUDIT ONCE, REPORT MANY:

- **Save up to 90% of the time**
- **Significantly reduces cost**
- **Enhances brand value**

GETTING STARTED

A trusted partner like BARR can help you determine which frameworks are right for your organization. To get started, your organization can determine what compliance certifications or reports you may need based on your stakeholders and contractual obligations. Contacting BARR is a great place to start! We will help you through the process and understand how you can reach your potential through your established security and compliance achievements and processes that are already in place.

BARR ADVISORY

Contact Us

Interested in learning more about finding the right compliance framework for your organization? Contact BARR today.

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 the ***audit once, report many*** process at BARR?

Contact us today to speak to a specialist and find the right framework for your organization.