TWO FRAMEWORKS, ONE AUDIT

Leveraging an ISO 27001 Certification for a SOC 2 Report

BARR ADVISORY

Table of Contents

Introduction

If your organization works with clients in and outside of the U.S., you might be considering the benefits of a compliance strategy that meets both national and international requirements. ISO 27001 and SOC 2 are two compliance standards that help organizations comply with ongoing regulations and keep customer data from around the world safe.

BARR Advisory is proud to say we're one of only a small number of firms in the nation that meet the requirements of the ANSI National Accreditation Board (ANAB) and the American Institute of Certified Public Accountants (AICPA) to issue both ISO 27001 certifications and SOC 2 reports.

> *We are very proud to be among the small number of firms who can offer both ISO 27001 certifications and SOC 2 audit reports. It's a vote of confidence from the ANAB and AICPA that affirms the dedication and hard work our team has put into providing exceptional value to our clients.*

Brad Thies
BARR's Founder and President

BARR auditors use our *test once, report many* approach to help you achieve an ISO 27001 certification and a SOC 2 report through the same audit.

This guide explores the differences between an ISO 27001 certification and a SOC 2 report and the benefits of obtaining both. You'll learn how BARR serves as your partner, guiding you through the process to adhere to two of the highest-regarded standards in cybersecurity.

ISO 27001 vs. SOC 2—What's the Difference?

Both ISO 27001 and SOC 2 provide organizations with a strategic framework to implement and measure security controls. ISO 27001 is a set of standards and requirements for an information security management system (ISMS). As an internationally accepted standard, ISO 27001 is an excellent choice for organizations that serve clients abroad. SOC 2 uses the U.S.-based AICPA Trust Services Criteria to meet the needs of a broad range of users that require detailed assurance of the controls of service organizations.

While the two frameworks cover similar topics, one big difference between ISO 27001 and SOC 2 is that specific standards can be certified under the ISO 27001 series. SOC 2 audits result in an attestation report rather than certification.

ISO 27001

- Compliance with global industry standards
- Successful engagements result in certification
- Includes specific requirements around documentation and policy
- Contains 93 Annex A control recommendations
- Is flexible to meet your organization's specific environment
- Keeps your Information Security Management System (ISMS) up-to-date

SOC 2

- More common for consumers that live in the U.S.
- Successful engagements result in a report
- Can be obtained as a Type 1 or Type 2 report
- Uses AICPA criteria to test controls
- Reports can be distributed to your organization's stakeholders
- Ensures controls are appropriately designed to mitigate risks

The ISO 27001 and SOC 2 Audits

ISO 27001 Certification

The ISO 27000 series is a family of information security management standards that can be combined to provide a globally recognized framework for best-practice information security management. At the core of ISO 27000 is the ISO 27001 framework, which contains 93 Annex A controls categorized into four overarching groups—organizational, people, physical, and technological.

ISO 27001 focuses on the ISMS following ISO 27002 control implementation guidance. It helps your organization manage the security of your services, data, intellectual property, or any information entrusted to you by a third party.

Certification to ISO 27001 consists of two stages that include walkthroughs, nonconformities review, and a remediation plan. The first stage involves walkthroughs of ISO clauses 4-10, while the second stage looks at Annex A controls.

Following preparation for the two-stage ISO audit, stage one generally takes two to three days to complete. Stage two can be achieved for most organizations within one to two weeks. BARR will then issue an internal report and public-facing certification, suitable for three years with surveillance audits.

ISO 27001 certification process »

ISO 27001 Stage One
This stage generally takes two to three days to complete.

ISO 27001 Stage Two
This stage can be achieved for most organizations within one to two weeks.

The ISO 27001 and SOC 2 Audits

SOC 2 Reporting

The 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 consumer requirements and cybersecurity best practices.

SOC 2 reports meet the needs of a broad range of users that require detailed information and assurance about the controls at a service organization. The report can be essential in the oversight of the organization, vendor management programs and internal corporate governance and risk management processes.

The duration for SOC 2 reporting depends on the type of report. If your organization has previously documented your controls through an automation partner, Type 1 reports may be performed immediately. Type 1 reports offer a point-in-time report, testing your design on a specific date. Type 2 reports are generally audited throughout a three to 12-month period.

SOC 2 Report Options »

SOC 2 Type 1

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

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.

Leveraging ISO 27001 for SOC 2—How it Works

So, how does it work to audit against two frameworks through one engagement? BARR serves as a unified team of auditors to perform both assessments for organizations seeking an ISO 27001 certification and a SOC 2 report*.

BARR's ISO 27001 + SOC 2 audit approach. »

Map ISO 27001 to SOC 2 controls.

While certifying toward ISO 27001 takes a certain amount of initial planning and time with your auditor, its flexibility means most ISO 27001 requirements will map over seamlessly with SOC 2 controls.

Combine SOC 2 and ISO 27001 meetings.

BARR's team of experts will leverage our resources to map SOC 2 control requirements *during* your ISO 27001 meetings.

Save countless hours.

You'll bypass additional walkthroughs to obtain a SOC 2 Type 2 report simultaneously, saving you countless hours to achieve two of the highest levels of security.

Though they are two completely separate audits, working with SOC 2 auditors who are also certified ISO Lead Auditors can make the process feel more like one and a half audits.

Marc Gold, **Attest Services Manager at BARR**

*ISO 17001 certifications are issued by BARR Certifications, the certification body of BARR Advisory.

Benefits of ISO 27001 + SOC 2

Having an ISO 27001 certification and a SOC 2 report under your belt increases consumer trust, and you'll stand out as an organization that takes security seriously while instilling the most confidence in your clients.

Benefits to a combined ISO 27001 + SOC 2 engagement »

- **Save time and resources** to achieve compliance.
- Increase your **customer trust**.
- Enhance organizational **brand value**.
- **Avoid fines** and penalties.
- **Remain transparent** with stakeholders.
- Assure that controls are **operating effectively**.
- **Keep up-to-date** with regular requirements.

Benefits of ISO 27001 + SOC 2

What Our Clients Are Saying

Clients who've completed an ISO 27001 certification and SOC 2 report with BARR not only adhere to two of the highest-regarded cybersecurity frameworks, but they've indicated results like:

- **Improved compliance processes**
- **Simplified evidence collection**
- **Decreased time spent on audits**
- **Gained a true audit partner**

> *We initially chose BARR because they could perform both ISO 27001 and SOC 2 audits simultaneously. We've stayed with BARR because* ***they are all-around an excellent organization to partner with****.*
> —Codat

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 completing both an ISO 27001 certification and a SOC 2 report in the same audit? Contact us today.