

2026 Whitepaper

One Team, Total Assurance

*BARR's Proven Process
for Coordinated Audits*

TABLE OF CONTENTS

- 2 | Introduction**
- 3 | One Team, Total Assurance**
- 4 | BARR's Proven Process**
- 7 | Today's Compliance Landscape**
- 8 | About BARR Advisory**



INTRODUCTION

We live in an era when technology is changing rapidly—and with those changes come new and increasingly stringent compliance requirements and regulations for businesses across all industries.

Especially for fast-growing organizations, juggling these requirements can be challenging. That's why our team has developed a [coordinated audit approach](#) that empowers organizations to work with one team to achieve total assurance across multiple cybersecurity frameworks.

Let's dive in.



ONE TEAM, TOTAL ASSURANCE

With a dedicated certification body, BARR is among a small group of U.S. auditing firms qualified to audit against all of the highest-regarded security frameworks and industry standards, including SOC 2, ISO 27001, HITRUST, PCI DSS, CMMC, CSA STAR, and more. This allows us to take a unique approach to auditing that provides organizations with a more holistic view of the compliance landscape as well as existing gaps in their security postures.

Unlike traditional firms that treat each audit separately, BARR can integrate multiple compliance frameworks into a single, coordinated process, reducing redundancies and saving you time and resources.

By leveraging BARR's coordinated audit approach, you and your team will achieve your compliance goals in less time and with less friction by:

- Reducing the risk of discrepancies and inconsistencies;
- Eliminating the need to balance multiple checklists and audit schedules;
- Streamlining communication with a consistent point of contact who understands your business and compliance needs; and,
- Minimizing disruptions to your daily operations by consolidating audit activities into a clear, unified process.

Working with experts who specialize in each framework can also help you identify and address broader cybersecurity and compliance risks, strengthening your overall security posture. For organizations aiming to mature their compliance programs, our experts can provide a clearer picture of the next steps to achieve your goals.



BARR'S PROVEN PROCESS

Leveraging the BARR team's deep expertise and experience across a wide range of frameworks, we've developed a simple, proven process to help organizations achieve ISO 27001 certifications, SOC 2 reports, HITRUST certifications, HIPAA Security Rule and PCI DSS compliance reports, CMMC certifications, CSA STAR attestations, and more through a coordinated audit process.



SOC 2

System and Organization Controls (SOC) 2 reports were developed by the American Institute of CPAs (AICPA) to assess a service organization's controls related to five trust service criteria: security, availability, processing integrity, confidentiality, and privacy. In addition to sharing commonalities with frameworks like ISO 27001 and HITRUST in areas like access control, data protection, and security incident response, SOC 2 reports can also include a section attesting to an organization's compliance with the [HIPAA Security Rule](#). This overlap makes a SOC 2 report a smart first step for fast-growing organizations aiming to build and mature their compliance programs.

The time it takes to complete a SOC 2 engagement depends on the type of report you're seeking. If your organization has previously documented your controls through an automation partner, Type 1 examinations may be performed immediately. Type 1 reports offer a point-in-time service, testing your design on a specific date. Type 2 reports, on the other hand, generally cover a period between three and 12 months.

BARR can also attest to an organization's compliance with [frameworks](#) like SOC 1, SOC 3, and SOC for Cybersecurity.



ISO 27001

ISO/IEC 27001:2022—often shortened to ISO 27001—is an international standard for establishing and maintaining an information security management system (ISMS). Certification to ISO 27001 is a multi-stage process that for most organizations can be completed in just a few months.

During [Stage 1](#), your auditor will test the design of your organization's ISMS, including reviewing documentation, identifying potential nonconformities, and evaluating the organization's plan to remediate any issues. Organizations that successfully complete Stage 1 then move on to [Stage 2](#), where your auditor tests the effectiveness of your ISMS, including ensuring areas of concern have been remediated.

At the conclusion of both stages, the auditor reviews the results of their assessments and makes a final decision on certification. ISO 27001 certifications are valid for three years, with required annual surveillance audits in the interim.

While achieving ISO 27001 certification requires a certain number of days with your auditor, BARR can improve efficiency by combining it with other frameworks, like SOC 2 and HITRUST. For instance, leveraging our dedicated certification body, BARR's team of experts can map SOC 2 control requirements during your ISO 27001 meetings. This allows your organization to bypass additional walkthroughs to obtain a SOC 2 Type 2 report simultaneously with an ISO 27001 certification.

This is particularly valuable for organizations that do business in the U.S. and abroad; because SOC 2 is [most common](#) in North America, ISO 27001 certification can serve as a powerful differentiator that underscores your team's global commitment to data security.

BARR can also audit against a number of [extensions to the ISO 27001 framework](#), including:

- **ISO 27701**, which outlines requirements for establishing, implementing, maintaining, and continually improving an organization's privacy information management system (PIMS).
- **ISO 27017**, which places an enhanced focus on cloud security.
- **ISO 27018**, which adds 24 new security controls related to protecting personally identifiable information (PII) in the cloud.



HITRUST

Known internationally as the gold standard for security, the HITRUST Common Security Framework (CSF) was designed to help organizations demonstrate their adherence to the highest standards in information security.

The amount of time it takes to achieve HITRUST certification varies depending on the level of assurance an organization requires. For organizations in low-risk environments, the HITRUST e1 assessment serves as a stepping stone to the more complex i1 and r2 assessments, which offer greater levels of assurance.

As a HITRUST Authorized External Assessor, BARR can help your team achieve HITRUST certification while taking steps toward compliance against other frameworks. For instance, because HITRUST CSF is built on a foundation that includes ISO 27001, many of the controls and requirements [overlap](#), allowing auditors to efficiently map existing controls to ISO 27001 requirements.

What's more, since ISO 27001 auditors cannot provide guidance on how to fix issues or mitigate gaps, HITRUST can serve as a risk assessment for the ISO 27001 audit, allowing your team to address potential nonconformities before you begin the ISO 27001 certification process.

HITRUST can also satisfy requirements for other assessments, like SOC 2. The AICPA's trust service criteria, which underpin SOC 2, align closely with HITRUST CSF criteria. This alignment allows BARR to offer a collaborative reporting model, issuing both SOC 2 reports and HITRUST certifications in a unified process.



PCI DSS

Typically required for businesses that store, process, or transmit credit card data, the Payment Card Industry Data Security Standard (PCI DSS) lays out a set of foundational security standards to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

As a PCI Qualified Security Assessor firm, BARR can assist organizations with a self-assessment questionnaire or a formal [report on compliance](#) in tandem with other attestations. For instance, PCI DSS shares its focus on network security, encryption, and vulnerability management with frameworks like ISO 27001 and HITRUST, which allows our team to more easily map controls from one framework to another.

Utilizing BARR's proven process for PCI DSS engagements, organizations can expect to complete a report on compliance within three to six months.



CMMC

As an [authorized C3PAO](#), BARR can evaluate your organization's compliance with the Cybersecurity Maturity Model Certification (CMMC) requirements. Navigating a formal CMMC assessment requires careful coordination, which is why we break the journey down into a structured, phased approach to guide your organization toward successful certification.

The first step is reviewing your System Security Plan (SSP) and validating the scope of the assessment. Afterward, we begin the formal CMMC assessment, which includes a thorough examination of your environment, interviews with key stakeholders, and control testing to determine whether your organization aligns with CMMC requirements.

Because CMMC is so comprehensive, there are many controls that overlap with the requirements for HITRUST and ISO 27001. By leveraging BARR's coordinated audit approach, our team can efficiently map these controls to multiple frameworks to help you achieve your compliance goals more efficiently.



CSA STAR

The Cloud Security Alliance Security, Trust & Assurance (CSA STAR) program [assesses](#) the security of cloud service providers (CSPs) based on the CSA's Cloud Controls Matrix. CSA STAR was designed specifically to overlap with ISO 27001 and SOC 2 for organizations operating in cloud environments like Microsoft Azure, AWS, and Google Cloud Platform, making it a seamless addition for organizations already pursuing a SOC 2 report or ISO 27001 certification.

When CSA STAR is added to an ISO engagement, the result is a CSA STAR certification. When CSA STAR is added to a SOC 2 engagement, the result is a CSA STAR attestation. Together, compliance with these standards not only provides greater assurance to your customers and stakeholders, but also helps to differentiate your organization as one that takes cloud security seriously.

TODAY'S COMPLIANCE LANDSCAPE

In today's multi-regulatory landscape, the need for a coordinated auditing process has become more critical than ever. Across industries, security and compliance leaders must contend with increasing demands from customers and regulators who want assurance that the organizations they work with are prioritizing data security.

We designed our coordinated audit approach to grow and evolve with your business. As you expand to new markets and as new regulations emerge, we can seamlessly integrate additional frameworks into your existing compliance strategy.

By leveraging our coordinated audit approach, organizations such as [Kinsta](#), a leading WordPress hosting provider, have accelerated their growth both in the U.S. and internationally. Kinsta needed an auditing partner who could be flexible to meet the demands of its fully distributed team and had the expertise to tackle not only SOC 2 reports, but also multiple ISO certifications.

They found that partner in BARR, who helped Kinsta [align their existing practices](#) and security controls with complex ISO requirements, ensuring they were set up for success in the auditing process.



It was just easy. We didn't spend hours and hours on calls—it was very streamlined, **we got everything we needed done.**

[Erik Van Dijk](#), Head of IT at Kinsta



Through its partnership with BARR, Kinsta successfully achieved a SOC 2 report as well as ISO 27001, ISO 27017, and ISO 27018 certifications, strengthening its data security program and accelerating growth.



Achieving compliance has significantly **boosted customer trust and satisfaction** at Kinsta. Our SOC 2 report and ISO certifications have become key differentiators in the market, giving our customers confidence in our security and data management practices.

[Nathan Bliss](#), Chief Sales Officer



With expertise across all of the leading cybersecurity frameworks, our team can help you map out a compliance plan that will help accelerate your organization's growth.

ABOUT BARR ADVISORY

BARR Advisory is a security and compliance solutions provider specializing in cybersecurity and compliance for organizations with high-value data that serve regulated industries such as healthcare, financial services, and government. Serving some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements.

Our Services & Frameworks



SOC Examinations

[SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]



Advisory & Managed Services



ISO Certification

[27001, 27017, 27018, 27701, 42001, 9001, 22301]



GRC & Engineering



Healthcare Services

[HIPAA, HITRUST]



Assessments & Testing



Government

[FedRAMP, GovRAMP, CMMC, DFARS, NIST]



Attestation & Certification



Privacy & Data Protection

[GDPR, CCPA, GLBA, PCI DSS, CSA
STAR, Microsoft DPR]



Contact Us to Get Started