ISO 27001
A STEP-BY-STEP APPROACH TOWARD CERTIFICATION

Working toward ISO 27001 certification can be an overwhelming endeavor. Here at BARR Certifications, we are committed to guiding you through the engagement process as you work towards ISO 27001 certification. We've identified a proven, step-by-step approach so you know exactly what to expect when partnering with BARR. Let's get started.

PRE-CERTIFICATION ACTIVITES

To request BARR Certifications services, you'll want to **contact us** to let us know you're interested. You can expect to hear from a BARR associate within 24 hours. Next, we will conduct a client evaluation and engagement acceptance review. We'll need information over your Information Security Management System (ISMS) scope and boundaries of the system to determine fee arrangements and resourcing needs.

This includes information like the approximate number of people, infrastructure, software components, key activities and data, and locations (physical and virtual) of the ISMS. If your organization has a Statement of Applicability or other ISMS scoping documentation, let us know, as these items are also helpful.

Information BARR will need:

- **Approximate number of people**
- **Infrastructure and software components**
- **Key activities and data**
- **Locations (physical and virtual) of the ISMS**

PRE-ASSESSMENT (OPTIONAL)

A formal readiness assessment against the ISO/IEC 27001 standard is also helpful in preparing organizations for initial certification. While a pre-assessment is not a requirement, it identifies ISMS deficiencies to the ISO/IEC 27001 standard.

INITIAL CERTIFICATION AUDIT

This involves **two stages:**

STAGE 1

First, we will evaluate the management system and documentation with a primary focus on the design of the system. You can expect this stage to take approximately two to three days to complete with the following;

ISO Stage 1 Initial Meeting: We'll discuss the Stage 1 audit and select dates to walk through ISO clauses 4-10.

ISO Stage 1 Walkthroughs: We'll review documentation and conclude if ISO clauses were met.

ISO Stage 1 Closing Meeting: We'll communicate nonconformities and opportunities for improvement and discuss next steps.

ISO Stage 1 Remediation: You'll develop and execute corrective action plans for any identified nonconformities. We'll then review the corrective action plans and validate nonconformity remediation.

STAGE 2

Next, we will evaluate the implementation and effectiveness of the management system. This stage is performed either remotely or at the client location(s) and can often be completed within one to two weeks with the following:

ISO Stage 2 Initial Meeting: We'll discuss the Stage 2 audit and select walkthrough dates.

ISO Stage 2 Walkthroughs: We'll review documentation and conclude if Annex A controls were met.

ISO Stage 2 Closing Meeting: We'll communicate nonconformities and opportunities for improvement and discuss next steps. During this meeting, BARR Certifications will also communicate our recommendation for certification.

ISO Stage 2 Remediation: You'll develop and execute a corrective action plan for any identified nonconformities. We'll then review the corrective action plan and validate nonconformity remediation.

ISO Certification: If we issue an internal report and public-facing certification, it is valid for three years with surveillance audits.

SURVEILLANCE AUDIT

The initial certificate issued is valid for three years from the issuance date. At least annually, surveillance audits are conducted to ensure the certified organization is able to maintain its compliance to the standard. These audits include limited testing and an onsite review to determine the impact of any significant changes since the original certification.

RECERTIFICATION

Arrangements for recertification are planned ***before the certificate expires***. Recertification activities include a full audit of the ISMS.

NOTICE OF CHANGES

If during the 3-year certification period there are changes in scope of the certification (i.e., reduction or expansion) or changes to requirements, this will be discussed with the BARR Certifications team.

1 OF 9

BARR Advisory is one of only nine US firms eligible to perform ISO 27001, SOC 2, and HITRUST audits.

> *"BARR's professionalism, attention to detail, and thoroughness throughout the process was exceptional. I appreciate the dedication and commitment they showed to ensure that our organization's ISMS was secure and compliant. The insights and recommendations provided have been invaluable to improving our internal processes and procedures.*

Airtable

BARR ADVISORY

Contact Us

Interested in learning more about ISO 27001? 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 Compliance 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 ISO 27001 and how it can benefit your organization?

Contact us today, or visit our **content library** to learn more about the ISO 27001 engagement process.