EVERYTHING YOU NEED TO KNOW ABOUT THE ISO 27001:2022 RELEASE

BARR ADVISORY

In October, the International Accreditation Forum released ISO 27001:2022. All ISO standards are officially reviewed at least once every five years to remain current and reflect new and evolving security challenges. With the last ISO 27001 update in 2013, incorporating the new ISO 27001:2022 requirements into your information security management system (ISMS) now will demonstrate your commitment to security and ensure you're prepared for the transition.

1 OF 9

US firms eligible to perform both ISO 27001 certifications and SOC 2 examinations.

As **one of only nine firms** in the nation eligible to perform both ISO 27001 certifications and SOC 2 audit examinations, BARR experts are here to guide you through this transition period. Whether you're just getting started with ISO or already have a certification, here's what you need to know about ISO 27001:2022 and how your organization should approach the changes.

What are the changes to ISO 27001?

Most updates to ISO 27001:2022 are minor, which means you can rest assured your organization won't need to go through a major overhaul with your security program. The main ISO 27001:2022 changes can be broken down into two parts:

- Changes to the management system clauses
- Changes to the Annex A controls

Management System Clauses

For the 2022 version, there's been a small change to ISO 27001 management system clauses which address clauses 4.4 and 8.1.

- **Clause 4.4** adds to the context of the organization, including the requirement to identify necessary processes and their interactions within your ISMS.
- **Clause 8.1** adds a requirement to define process criteria.

Additionally, minor clarifications and specifications have been made to a handful of other management system clauses.

Annex A Controls

Annex A controls updates are moderate and have been derived from ISO 27002:2022, which was released earlier this year. Organizationally, the former 14 families of Annex A are now focused on four themes: organizational, people, physical, and technological.

Most controls have stayed the same or been renamed, and another group of controls were merged to reduce the total number of controls. However, the requirements within those controls are almost all the same.

The biggest change has been the addition of 11 new controls, added to reflect new and evolving security areas. Specifically, the control categories are as follows:

- Threat intelligence
- Information security for the use of cloud services
- Information and communications technology for business continuity
- Physical security monitoring
- Configuration management
- Information deletion
- Data masking
- Data leakage prevention
- Monitoring activities
- Web filtering
- Secure coding

For further details and descriptions of these controls, BARR experts recommend purchasing the ISO 27001 and 27002 standard and reviewing those documents with your team. The updated version of these standards will guide you in determining any changes that need to be made to your ISMS. When reviewing, keep in mind that the ISO 27001 standard will outline the requirements that need to be met while 27002 will provide implementation guidance. Review the requirements in ISO 27001 first, and then use 27002 to help with implementation. BARR associates are here to guide you through the process and answer any questions you may have about how the changes might impact your organization. Contact us today if you have any questions.

Already have an ISO 27001: 2013 certification? Here's what you need to know about the transition:

When conforming to the newly updated ISO 27001:2022 standard, there's a **three year transition** period for all organizations.

ISO 27001:2013 certificates will expire or be withdrawn no later than **October 31, 2025**.

For organizations working toward a certification, companies are eligible to certify against the 2013 version up until **October 31, 2023**.

If your organization obtains an active certification, don't worry—there's plenty of time to make the necessary changes.

A few tips for transitioning your certification to the updated ISO standard include:

- Start by reviewing the standards and updating your ISMS and statement of applicability to align with the revised requirements;
- Incorporate these changes into your risk assessment and management review so that key parties at your organization are on board with the changes; and,
- Reach out to BARR for guidance on the logistics of the transition. We're happy to help!

For organizations working toward certification, start incorporating the new standards into your preparations today. Certification bodies will require you to be ready to certify against the new standard by April 30 of 2023, though most will be ready to certify prior.

Standard updates and the associated transition process can sometimes feel a bit daunting, but BARR is here to walk your teams through the process and reduce some of the burden.

What does the audit process look like?

The audit process hasn't changed. From kickoff to final deliverable, BARR associates will use our proven process to help your organization through a smooth engagement.

The internal audit is the first step in the process and is often the biggest lift for organizations when preparing for ISO 27001 certification. If this is your first ISO 27001 audit, or your organization might need extra assistance, you can employ an independent third-party firm to help complete your internal audit. Consulting firms like BARR will help you create policies and complete your internal audit while maintaining independence. While it's not required, most organizations who use a third-party auditor for their internal audit experience a greater level of success within the certification process.

Once you've completed your internal audit and have developed and implemented the other ISO documentation and processes outlined in ISO 27001, you're now geared up for Stage 1 and Stage 2 of the ISO 27001 certification process:

Stage 1 lasts 2-3 weeks. BARR will assess your policies, procedures, results of the audit, and issue a report with findings.

Stage 2 lasts 2-2.5 months, and can be combined with SOC 2 testing. Following the completion of stage 2, we'll issue an internal report and public-facing certification, good for three years with surveillance audits.

When you partner with BARR, we go beyond the compliance checklist and assess all aspects of your organization's unique environment—identifying risks, areas for improvement, and ways to simplify the processes and controls needed to turn compliance into a strategic asset. We follow a unified, agile process to ensure minimal disruption to your business.

ISO Engagement Process

Connect

- About us
- About you
- Solutions
- Proposal

ISMS Implementation and Internal Audit

- Third-party assistance (optional)

STAGE 1

ISO Stage 1 Kickoff

- Discuss Stage 1 audit
- Select dates to walk through ISO clauses 4-10

ISO Stage 1 Walkthroughs

- Review documentation
- BARR to conclude if ISO clauses were met

ISO Stage 1 Closing Meeting

- Review nonconformities
- Discuss next steps

ISO Stage 1 Remediation

- Develop and execute corrective action plan
- BARR to validate nonconformity remediation

STAGE 2

ISO Stage 2 Kickoff

- Discuss Stage 2 audit
- Select dates to walk through Annex A controls

ISO Stage 2 Walkthroughs

- Review documentation
- BARR to conclude if Annex A controls were met

ISO Stage 2 Closing Meeting

- Review nonconformities
- Discuss next steps
- BARR to communicate certification decision

ISO Stage 2 Remediation

- Develop and execute corrective action plan
- BARR to validate nonconformity remediation

Certification

- Draft report
- Quality review
- Issue report

Celebrate & Optimize

- Debrief
- Rate engagement
- Improve security
- Next steps (includes annual surveillance)

Simplified ISO 27001 Certification

Test Once, Report Many

BARR takes a "test once, report many" approach, meaning you can have a SOC 2 audit and ISO 27001 certification upon project completion.

Ensure Customer Trust

According to a study by Centrify, 65% of data breach victims lost trust in an organization as a result of the breach. BARR's audit process will ensure the confidence you and your customers deserve when it comes to your cybersecurity posture.

Enhance Brand Value and Reputation

Share prices of compromised companies fell an average of 3.5% following an attack, and underperformed the Nasdaq by 3.5%. A proactive security mindset will drastically reduce the risk of tarnishing your brand.

Avoid Fines and Penalties

ISO 27001 is a globally accepted standard, meaning you can avoid the high fines associated with non-compliance for the most rigorous security and privacy regulations.

Meet Regulatory Requirements

ISO 27001 was created with global regulations and standards in mind, so you can achieve control coverage in line with the GDPR, NIST CSF, and SOX.

Not Just Auditors — What Sets BARR Apart

Human First Approach

Using real talk, not tech talk, we will educate and empower your people. This not only raises awareness, but it changes behavior, and embeds best security practices into your company culture.

Perspective

We are a trusted advisor to some of the fastest growing cloud service providers (IaaS, PaaS, SaaS) in the world. We understand your challenges because we faced the same challenges when we sat on your side of the table.

Connections

Through our global network and ecosystem of partners, we will connect you with best-fit experts. And it goes far beyond a simple referral. These partners are integrated into our own tools, processes, and services.

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 Suite of 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**
- **Virtual CISO Services**
- **Compliance Program Assistance**

Connect with BARR

Want to learn more about ISO 27001:2022 and what this new release means for your organization?

Contact us today.