BARR ADVISORY

2024 Whitepaper

Breaking Into the U.S. Market

A Comprehensive Guide to Cybersecurity Compliance for International Growth

Table of Contents

Introduction

For Europe-based cloud service providers (CSPs), entering the U.S. market brings significant growth potential, but it also requires navigating unique cybersecurity compliance expectations.

Understanding the Compliance Expectations for International Market Entry

The absence of a national data privacy law in the U.S. means that American companies rely on frameworks like SOC 2, ISO 27001, FedRAMP, and HIPAA to assess vendors' security practices. While ISO 27001 remains a foundational global standard, the SOC 2 framework is often viewed as a key differentiator in North America.

This whitepaper offers European organizations a comprehensive view of U.S. compliance, emphasizing the unique advantages of adding SOC 2 to their compliance strategy as they pursue U.S. market entry.

BARR Advisory's coordinated audit approach enables companies to adopt SOC 2 seamlessly alongside ISO 27001 and other frameworks, accelerating their path to market readiness.

The U.S. Compliance Landscape

Understanding the Compliance Expectations for U.S. Market Entry

While the European Union's GDPR provides a unified standard for data protection, the United States has no federal equivalent, resulting in a fragmented regulatory environment that requires additional diligence from businesses. This discrepancy can surprise European providers but underscores why SOC 2 is often critical in establishing U.S. market trust.

For European organizations, this divergence presents a crucial consideration: adhering only to ISO 27001 may not be sufficient for customers in the U.S., especially in sectors where data protection is paramount. U.S. businesses frequently require SOC 2 compliance to validate that their vendors understand and are meeting the distinct security and privacy standards that are expected in North America.

Key Differences Between GDPR and U.S. Data Protections

While GDPR has established a comprehensive data protection protocol in Europe, it primarily focuses on data privacy and individual rights. In contrast, U.S. compliance frameworks—particularly SOC 2—place a stronger emphasis on verifying that an organization has implemented robust internal controls for securing data from unauthorized access, ensuring system reliability, and maintaining data integrity. These distinct focuses mean that GDPR-compliant European companies may still fall short of U.S. client expectations if they lack a SOC 2 report.

Here are some of the most critical contrasts between European and U.S. compliance standards:

- **National vs. State-Level Regulations:** The U.S. does not have a national equivalent to GDPR. Instead, it has state-specific laws like the California Consumer Privacy Act (CCPA), which mandates certain data privacy practices for residents of California. While CCPA shares some similarities with GDPR, it lacks the same sweeping, federal applicability and primarily concerns consumer rights rather than security protocols.
- **Framework-Specific Requirements**: U.S. companies use frameworks such as SOC 2, FedRAMP, and HITRUST to validate that their vendors meet certain security standards. While these frameworks are not legally required, they are highly regarded and often serve as an unofficial baseline for vendor selection.
- **Third-Party Assurance Needs:** American companies frequently require vendors to demonstrate compliance through third-party audits, such as SOC 2. This is particularly the case in sectors like finance, healthcare, and technology, where client data security is paramount. A SOC 2 report serves as proof that a vendor meets key security standards beyond those covered by ISO 27001 or GDPR alone.

SOC 2 – The Key to Unlocking U.S. Business Opportunities

Why SOC 2 Is Essential for Establishing Trust in the U.S. Market

SOC 2 is increasingly seen as a vital component for building trust with American clients and a competitive differentiator in North America. A SOC 2 report is often regarded as a key indicator that an organization has taken necessary steps to safeguard sensitive information and can be trusted to manage risks according to U.S. expectations.

In sectors where vendor trust and rigorous security practices are critical—such as healthcare, financial services, and SaaS—U.S.-based companies frequently conduct thorough due diligence before engaging with third parties. A SOC 2 report often plays a pivotal role in vendor assessments, serving as a standard means for companies to evaluate whether an organization's systems are secure. Without SOC 2, organizations may find themselves at a disadvantage, potentially losing business to competitors who have taken the extra step to obtain this important attestation.

The Role of SOC 2 in Building Trust with U.S. Customers

SOC 2 reports, which assess controls against one or more of five trust services criteria—security, availability, processing integrity, confidentiality, and privacy—give U.S. clients confidence that their sensitive data is protected. In an increasingly security-focused market, SOC 2 compliance can:

- Serve as a key decision-making factor in vendor assessments.
- Instill confidence in U.S. clients by meeting their preferred security benchmarks.
- Open doors to more business opportunities, as it is often required to secure contracts with larger enterprises in the U.S.

How BARR's Coordinated Approach Facilitates SOC 2 for ISO-Certified Businesses

For businesses with ISO 27001 certification, adding SOC 2 can seem redundant, but BARR's coordinated audit approach integrates both standards efficiently. This approach enables organizations to leverage ISO 27001 controls within the SOC 2 audit, minimizing additional workload and making the adoption of SOC 2 seamless and cost-effective.

So, how does it work to audit against two frameworks through a coordinated engagement? While certifying toward ISO 27001 takes a certain amount of initial planning, its flexibility means most requirements will map over seamlessly with SOC 2 controls. Let's explore the details of our proven process to help clients achieve ISO 27001 certification and SOC 2 compliance.

How BARR's Approach Works

Certification to ISO 27001 consists of two stages, both including walkthroughs, a review of nonconformities, and a remediation plan. 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.

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

While ISO 27001 certification requires a certain amount of days with your auditor, BARR's team of experts will leverage our resources to 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, saving you countless hours to achieve two of the highest levels of security.

Benefits of ISO + SOC 2

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

Benefits of obtaining both ISO 27001 and SOC 2:

- Save time and resources to achieve information security and compliance
- Increase 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

ISO 27001

A Foundation for Global Compliance

ISO 27001: The International Pillar

ISO 27001 provides a recognized baseline for information security that applies well across global markets, including the U.S. However, while ISO 27001 demonstrates international security standards, it may not fully satisfy U.S.-based clients who prioritize SOC 2. Integrating both frameworks offers European organizations a balanced approach to global and regional security needs.

BARR's ISO 27001 Expertise

As an accredited certification body, BARR can help you obtain an ISO 27001 certification to demonstrate your compliance and your commitment to keeping information secure. BARR specialists have deep experience in conducting ISO 27001 audits over information security management systems (ISMS) and put you and your business first, providing unparalleled communication and accessibility at all times.

ISO 27001 Extensions for Enhanced Cloud Security

ISO 27001 can be extended to address specific concerns related to privacy and cloud security through standards like ISO 27701 and ISO 27018. BARR offers a coordinated approach to help organizations achieve these add-ons, enhancing their appeal to a range of U.S. clients.

> ***"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, ISO Practice Leader

FedRAMP: Access to U.S. Federal Contracts

The Federal Risk and Authorization Management Program (FedRAMP) is essential for organizations that want to work with U.S. federal agencies. This framework enforces strict controls for data security, vulnerability management, and incident reporting, making it a high-value addition for businesses targeting government contracts.

Do You Need FedRAMP?

Whether headquartered within the United States or internationally, cloud service providers must comply with FedRAMP requirements in order to do business with U.S. government agencies. If you have no plans to pursue government contracts, it may not make sense to undergo the lengthy and sometimes costly FedRAMP authorization process. However, CSPs that could potentially be part of the government ecosystem, either directly or indirectly through their customers, should thoughtfully consider pursuing FedRAMP authorization.

Simplifying FedRAMP Compliance

For organizations aiming to grow and mature their compliance programs, achieving FedRAMP authorization may not be as great of a lift as you think. Many FedRAMP requirements, especially those related to control implementation and security governance, can map back to leading industry standards like ISO 27001, PCI DSS, and HIPAA. By leveraging BARR's coordinated audit approach, cloud service organizations can build a unified compliance program that fulfills customer requirements and accelerates business growth.

Benefits of FedRAMP

Even if your organization does not currently work with U.S. government agencies, you may still want to consider FedRAMP as a guiding measurement of cybersecurity maturity for your cloud service offering. Benefits of FedRAMP include:

- Helps your team identify and remediate vulnerabilities in your risk management procedures
- Opens the door for your company to compete for government business
- Positions your organization as one that customers and stakeholders can trust.
- Gives you a competitive advantage over other cloud service providers when bidding as part of a government RFP process.

HIPAA: Essential for Health Data Compliance

The Health Insurance Portability and Accountability Act (HIPAA) sets standards for handling protected health information (PHI) in the U.S., relevant to any CSP managing health-related data.

HIPAA Compliance and the Protection of U.S. Healthcare Data

While there is no formal certification, HIPAA compliance is often required by healthcare clients and can differentiate CSPs in the market. If your organization handles or plans to handle any U.S. PHI, you will be required to comply with HIPAA or risk facing hefty fines.

BARR's Coordinated Audits Align HIPAA with SOC 2

With a dedicated team of healthcare compliance efforts, BARR can add certain controls for HIPAA compliance to your SOC 2 engagement. This helps CSPs demonstrate health data security without duplicative assessments, offering an efficient path to meet both sets of requirements.

Additional Frameworks for U.S. Market Expansion

Depending on the organization, additional frameworks may be necessary and can offer extra assurance:

HITRUST

As an international gold standard of security, HITRUST can demonstrate that your organization meets the highest standards in information security. As a HITRUST Authorized External Assessor, BARR has extensive experience in the HITRUST process and tools, and can serve as your trusted partner every step of the way.

CSA STAR

The Cloud Security Alliance's Security, Trust, Assurance, and Risk (CSA STAR) is a powerful certification program for CSPs. As an accredited certification body, BARR Advisory can perform rigorous yet efficient independent security assessments to help CSPs demonstrate their commitment to security and privacy best practices.

PCI DSS

If your business stores, processes, or transmits credit card data, then the Payment Card Industry Data Security Standard (PCI DSS) likely applies to you and is considered a must in the American market. As a PCI DSS qualified security assessor (QSA) firm, BARR Advisory helps organizations achieve PCI DSS compliance so your customers can rest assured that their data is secure as your business grows.

BARR's Expertise in Mapping Multiple Frameworks

Choosing and implementing the right combination of frameworks, with SOC 2 at the forefront, demonstrates a CSP's adaptability and alignment with U.S. security expectations.

Planning a Coordinated Compliance Strategy with BARR

Coordinated Compliance for Efficient U.S. Market Entry

With a dedicated certification body, BARR is among a small group of U.S. auditing firms that is qualified to audit against all of the highest-regarded security frameworks and industry standards, including SOC 2, ISO 27001, HITRUST, PCI DSS, 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.

Conclusion

Entering the U.S. market is a strategic move with immense growth potential. While ISO 27001 builds an essential security baseline, adding SOC 2 demonstrates a CSP's commitment to meeting U.S. security standards head-on, setting them apart in an increasingly competitive environment. BARR Advisory's expertise in coordinated audits helps CSPs efficiently add SOC 2 to their compliance toolkit, positioning them for sustainable success in the American market.

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. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements.

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 our coordinated approach to compliance? Contact us today.