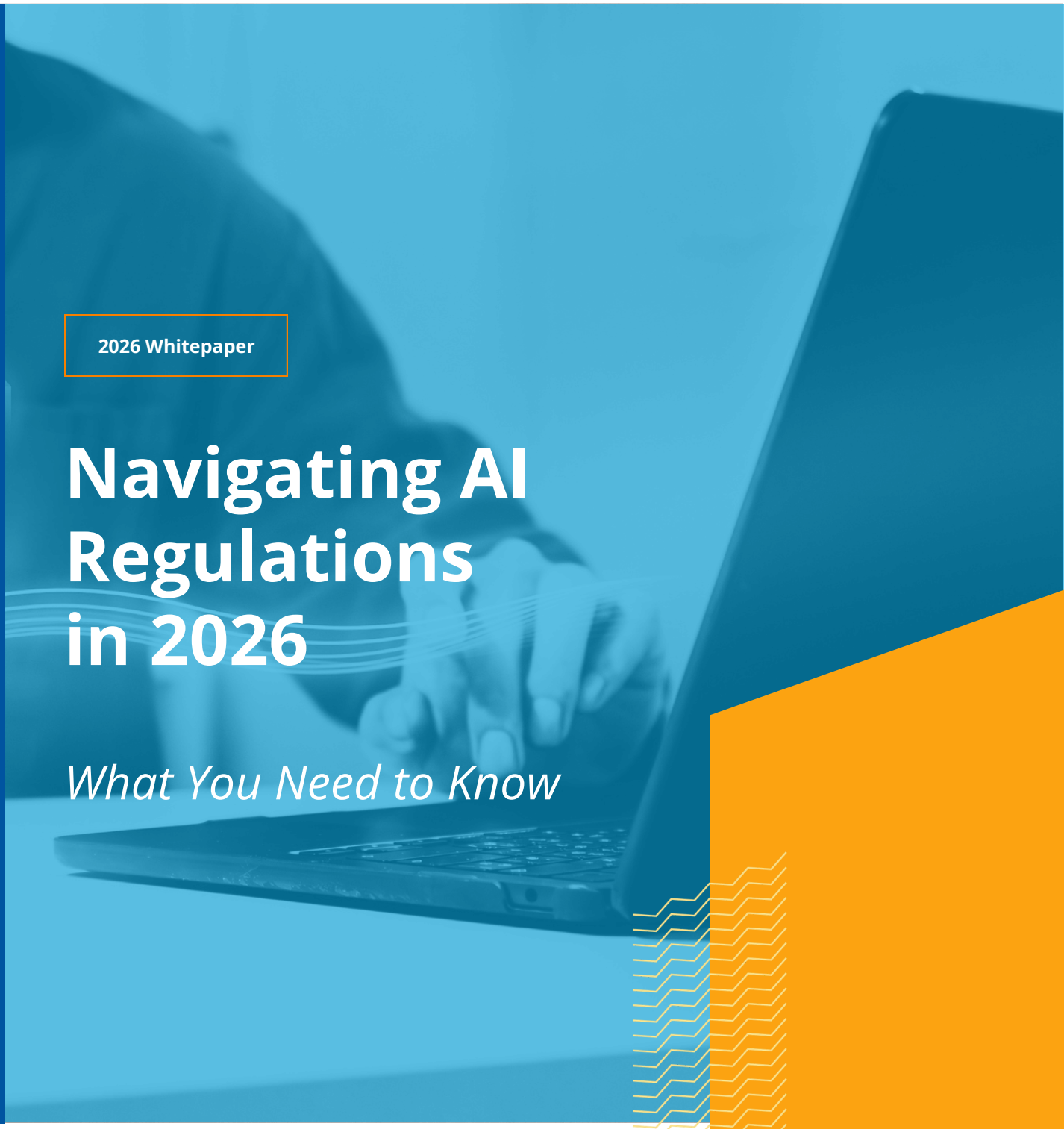
BARR ADVISORY



2026 Whitepaper

Navigating AI Regulations in 2026

What You Need to Know

TABLE OF CONTENTS

Introduction

As artificial intelligence becomes more embedded in business operations—from automating workflows to powering complex decision-making—regulatory expectations are evolving just as quickly.

For organizations that use or develop AI systems, navigating this shifting landscape in 2026 requires a proactive, structured approach to governance, risk management, and compliance.

Here's what you need to know:

- AI-specific compliance frameworks are gaining global traction.
- Regulators are increasing scrutiny around transparency, accountability, and risk management.
- Standards like ISO 42001 and the NIST Artificial Intelligence Risk Management Framework are becoming foundational tools for demonstrating responsible AI use.

In this whitepaper, we'll share exactly what this means for your organization.

Why AI Governance Matters More Than Ever

AI presents enormous opportunities for growth and efficiency—but it also introduces new risks. From security vulnerabilities and algorithmic bias to data privacy concerns and social engineering threats, AI systems can amplify existing risks and create entirely new ones.

As adoption accelerates, regulators and stakeholders alike are asking tougher questions:

- Do you know where your data is—and where it's going?
- Can you explain how your AI systems make decisions?
- Are you prepared to respond to AI-related incidents or failures?

In 2026, answering these questions isn't optional. It's essential to maintaining trust, competitiveness, and compliance.

The Rise of AI-Specific Frameworks

While traditional cybersecurity frameworks still play a critical role, AI has introduced governance challenges that require more targeted guidance. In 2026, organizations looking to demonstrate accountability and build trust around their use of AI should consider both AI-specific and foundational compliance frameworks.

SOC 2

For many organizations—particularly those operating in North America—SOC 2 remains a go-to framework for demonstrating strong cybersecurity and operational controls.

Designed as a scalable framework, SOC 2 enables organizations to show they are committed to sound risk management practices. By undergoing a SOC 2 examination, organizations receive an independent, third-party assessment of their operational controls based on one or more of the five trust services criteria (TSC) established by the American Institute of Certified Public Accountants (AICPA).

- **Security (required for all SOC 2 reports):** Protection against unauthorized physical and logical access
- **Availability:** Systems are available for operation and use as committed
- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized
- **Confidentiality:** Confidential information is protected as committed
- **Privacy:** Personal information is collected, used, retained, disclosed, and disposed of appropriately

A SOC 2 report provides a CPA's opinion on the design and effectiveness of your controls—either at a single point in time (Type 1) or over a defined period (Type 2). While SOC 2 does not result in a formal certification, it remains a widely accepted method for demonstrating commitment to data security best practices.

Because SOC 2 is flexible and customizable, organizations can tailor the scope of their examination to include AI systems and related processes. For example, your SOC 2 audit may include controls related to:

- Secure handling and access management of AI training data
- Change management processes for AI model updates
- Monitoring of automated decision systems
- Incident response procedures for AI-related failures or misuse

For organizations where AI is part of broader service delivery—but not necessarily the core product—SOC 2 can serve as a strong foundational assurance framework. However, organizations with complex AI systems, global operations, or AI-centric business models may need a more specialized and internationally recognized standard.

ISO 42001

ISO/IEC 42001:2023, often shortened to ISO 42001, is the first internationally recognized compliance framework designed specifically for managing AI systems. It provides a structured approach for establishing, implementing, maintaining, and continually improving an AI management system (AIMS).

The standard is organized into 10 clauses, covering areas such as:

- Defining the context and scope of your AI management system
- Establishing leadership accountability and AI policies
- Identifying and treating AI-related risks, including security vulnerabilities and algorithmic bias
- Ensuring AI systems are safely and transparently developed, deployed, and monitored
- Conducting performance evaluations and driving continuous improvement

After assessing these requirements, organizations must implement appropriate controls outlined in Annex A—carefully determining which controls apply based on their unique AI risk landscape.

For businesses that use or produce AI-powered products and services, ISO 42001 is quickly becoming a cornerstone of a modern compliance program.

HITRUST AI Frameworks

For organizations that require a more prescriptive or cybersecurity-focused approach to AI risk, the HITRUST AI standards provide additional options.

HITRUST AI Risk Management (RM) Assessment

The HITRUST AI RM Assessment includes 51 risk management controls and serves as a structured roadmap to identify and address gaps in your AI risk management strategy. It is available to any organization—regardless of existing HITRUST certifications—and offers a scalable approach to evaluating AI governance maturity.

While this assessment does not result in certification, it provides actionable insights into your organization's AI risk posture.

HITRUST AI Security Assessment and Certification

For organizations that build or provide AI-powered systems to end users, the HITRUST AI Security Assessment offers a more rigorous option. This certification includes 44 highly tailored, prescriptive controls focused specifically on AI security risks.

Unlike ISO 42001—which addresses a broad spectrum of AI governance issues—the HITRUST AI Security Assessment zeroes in on cybersecurity threats related to AI systems, including threat management, access controls, encryption of AI assets, and system resilience.

The framework was designed to be compatible with ISO 42001, making it a strong complementary certification for organizations that both develop AI technologies and operate in high-risk or highly regulated environments.

NIST AI Risk Management Framework

The NIST Artificial Intelligence Risk Management Framework (AI RMF) offers a voluntary, flexible framework to help organizations identify, assess, and manage AI risks.

Built around four core functions—Govern, Map, Measure, and Manage—the framework is designed to be adaptable across industries and organization sizes. It enables businesses to:

- Establish AI governance structures
- Identify and contextualize AI risks
- Measure and monitor AI system performance and impact
- Allocate resources to mitigate and manage risks over time

For organizations just beginning to formalize their AI governance efforts, the NIST AI RMF can serve as a practical starting point.

AI and Existing Compliance Obligations

AI governance doesn't exist in a vacuum. Organizations must also consider how AI intersects with existing regulatory and industry requirements. Depending on your industry and geographic footprint, this may include HIPAA, GDPR, and PCI DSS.

In addition, organizations operating in the European Union must contend with the EU AI Act, the world's first major comprehensive legal framework governing AI. The legislation introduces risk-based requirements, including transparency obligations and restrictions on high-risk or unacceptable-risk AI systems.

As global regulations continue to evolve, organizations that already have structured AI governance programs in place will be far better positioned to adapt.

Key Areas to Focus on in 2026

To successfully navigate AI regulations this year and beyond, organizations should prioritize three critical areas:

Strong Risk Management Foundations

AI can magnify existing risks—especially those related to data access and security. Implementing robust controls such as encryption, access management, and continuous monitoring is essential. Just as important is fostering a culture of cybersecurity awareness and training employees to identify and respond to AI-related risks, including sophisticated social engineering attacks.

Transparency and Accountability

Stakeholders increasingly expect visibility into how AI systems are trained, deployed, and governed. This includes:

- Establishing clear AI policies
- Assigning accountability for AI-related decision-making
- Conducting AI impact assessments
- Maintaining documentation and audit trails

Frameworks like ISO 42001 formalize these expectations, helping organizations demonstrate responsible oversight.

Continuous Monitoring and Improvement

AI systems evolve—and so do the risks associated with them. Effective governance requires ongoing performance evaluation, internal audits, and mechanisms for detecting emerging threats. Continuous improvement is not just a best practice; it's a core requirement of modern AI compliance standards.

Which Path Is Right for Your Organization?

Choosing the right approach depends on your organization's maturity, market presence, and the role AI plays in your operations.

If you're looking for a flexible, voluntary framework to begin formalizing AI risk management, the NIST AI RMF may be a strong starting point.

If AI is central to your products, services, or strategic decision-making—and you need globally recognized assurance—ISO 42001 certification may be the better fit.

In many cases, organizations benefit from leveraging multiple frameworks to build a comprehensive, future-ready compliance program.

Conclusion

AI is transforming the business landscape—and regulators are taking notice. In 2026, organizations that treat AI governance as a strategic priority rather than a reactive obligation will be best positioned to thrive.

By implementing strong risk management practices, aligning with recognized frameworks like ISO 42001 and HITRUST, and staying ahead of evolving regulations such as the EU AI Act, your organization can demonstrate that its AI systems are secure, ethical, and trustworthy.

Need help navigating AI compliance in 2026? Our expert team can guide you through framework selection, gap assessments, and certification readiness.

Contact us today for a free consultation.

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]

ISO Certification
(27001, 27017, 27018, 27701, 42001, 9001, 22301)

Healthcare Compliance
[HIPAA/HITRUST]

Government Compliance
[FedRAMP, GovRAMP, CMMC, DFARS, NIST]

Privacy & Data Protection
[GDPR, CCPA, GLBA, PCI DSS, CSA STAR, Microsoft DPR]

Advisory & Managed Services

GRC & Engineering

Assessments

Attestation & Certification

Contact Us to Get Started