BARR ADVISORY

2025 Whitepaper

The Intersection of AI and Compliance

What Businesses Need to Prepare For in 2025 and Beyond

Table of Contents

Introduction

Across all industries, artificial intelligence (AI) is reshaping the business landscape, opening doors to enhanced efficiency and innovation.

Introduction

For organizations that are currently leveraging AI or considering adopting the technology, adapting your security and governance strategies to keep pace with evolving risks and regulations is paramount.

With the right approach, organizations can harness the huge potential AI offers while ensuring security, transparency, and alignment with industry standards. In this whitepaper, we'll cover three areas to consider when mapping out your plan for AI security and compliance.

AI and Risk Management

While AI has the potential to offer huge benefits to businesses, it doesn't come without risk.

For organizations that use or produce AI-powered products and services, mitigating these risks is critical to maintain an effective and comprehensive risk management program.

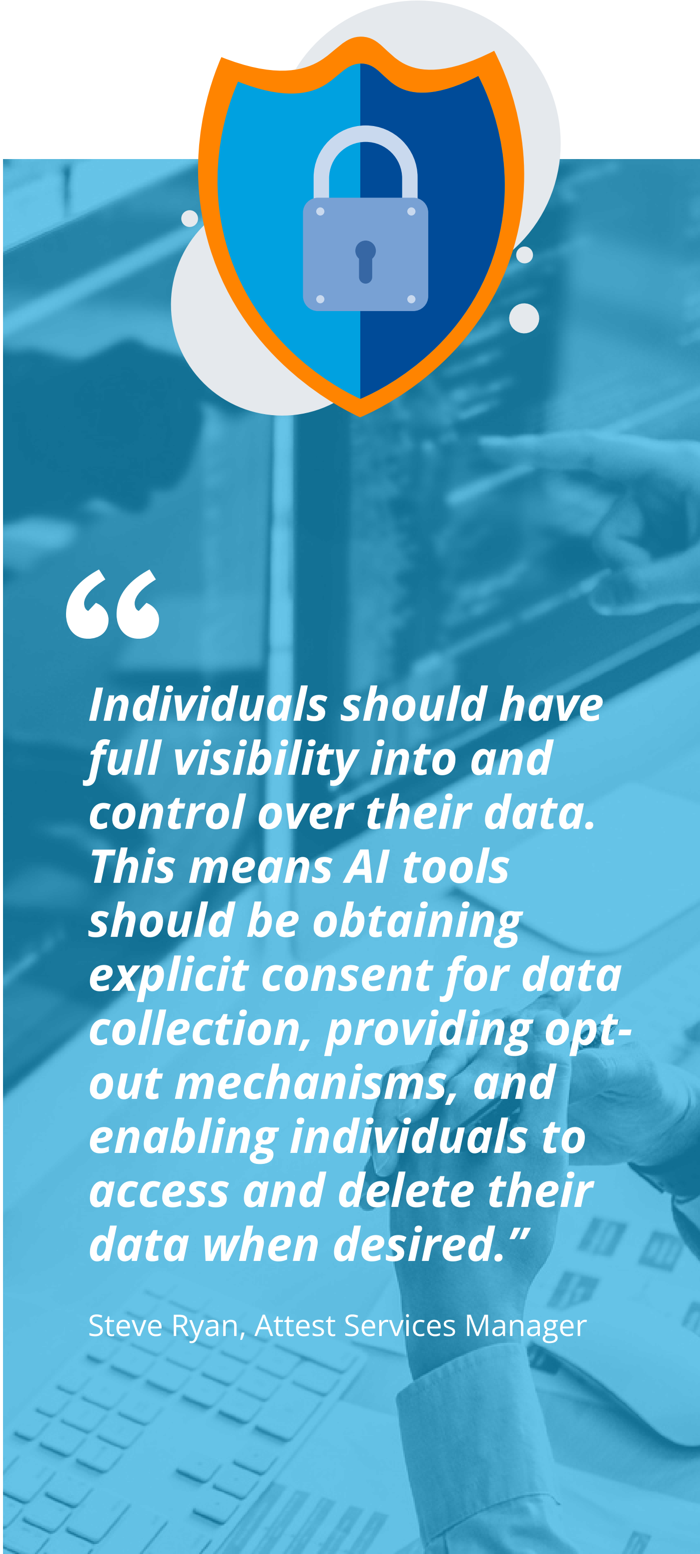
Building a Security Culture

It starts at the top. According to Steve Ryan, attest services manager at BARR Advisory, business leaders should prioritize privacy as a fundamental principle and strive to create a culture of cybersecurity across the organization. This means implementing privacy by design principles, conducting regular privacy impact assessments, and fostering transparency in data practices.

"Implementing robust security measures, such as encryption and access controls, is essential to safeguard data from unauthorized access," Ryan said. "Companies should also invest in employee training and education programs to ensure that individuals handling data understand the importance of privacy and are equipped to handle potential privacy risks effectively."

In addition, Ryan emphasized that transparency is crucial for AI-powered organizations to build trust with consumers and stakeholders.

"Individuals should have full visibility into and control over their data," Ryan explained. "This means AI tools should be obtaining explicit consent for data collection, providing opt-out mechanisms, and enabling individuals to access and delete their data when desired."



Individuals should have full visibility into and control over their data. This means AI tools should be obtaining explicit consent for data collection, providing opt-out mechanisms, and enabling individuals to access and delete their data when desired."

Steve Ryan, Attest Services Manager

AI and Risk Management, *continued*

Vendor Risk Management

Even if your organization does not produce or provide AI-powered products and services, it's likely that at least some of your vendors are leveraging AI to improve efficiency and power new technologies. For this reason, it's also crucial for compliance leaders to examine their organization's vendor risk management strategy and ensure it accounts for the use of AI.

As part of your vendor risk assessments, consider asking questions such as:

- Is the vendor following any specific security or privacy frameworks, such as NIST, SOC 2, ISO 27001, or ISO 27701?
- Do they have a roadmap for implementing new standards specific to the safety and ethical use of AI?
- Are they involved in any way in helping create such standards?

The answers to these questions can help you adequately assess your organization's risk when working with third-party vendors that use AI to provide their products or services.

Paths to AI Assurance

NIST AI RMF 1.0 and ISO 42001

For organizations aiming to use AI safely and demonstrate to stakeholders that you take AI security seriously, achieving compliance against an industry standard is a great first step. Leveraging frameworks like NIST's Artificial Intelligence Risk Management Framework (AI RMF 1.0) can help businesses of all sizes measure and manage their AI risks, including policies, practices, implementation plans, indicators, measurements, and expected outcomes.

Organizations that need greater levels of assurance should consider certification against standards like ISO 42001. Published in late 2023, ISO 42001 offers a structured approach to managing AI systems. The framework integrates seamlessly with ISO 27001 and ISO 27701 and mandates numerous controls for the establishment, operation, monitoring, maintenance, and continuous improvement of an organization's AI management system (AIMS). Compliance with this framework ensures that organizations have established effective processes for ensuring their use of AI is secure, ethical, and transparent.

HITRUST's New AI Frameworks

HITRUST has also announced two new frameworks for organizations that use or provide AI-powered products and services:

- The HITRUST AI Risk Management (RM) Assessment offers a starting point for evaluating an organization's AI risk management strategies. While not a formal certification, the HITRUST AI RM Assessment examines more than 50 risk management controls and provides a professional AI Risk Management Insights Report to help organizations better understand their AI risk management stance and identify potential gaps.
- The HITRUST AI Security Certification includes up to 44 carefully selected, highly prescriptive controls that address risks and threats related to AI systems. These controls are added to the core set of requirements for the e1, i1, or r2 assessment and cover areas such as AI security threat management, access to AI systems, encryption of AI assets, and the resilience of AI systems.

By leveraging one or a combination of these frameworks, businesses can show current and potential customers, partners, and stakeholders that they're taking active steps to implement AI safely and securely.

AI in Regulatory Compliance

In addition to ensuring your security program is up to par with stakeholders' standards, businesses that want to leverage new and innovative AI tools must also consider industry regulations and legal requirements. Depending on where the organization is headquartered and the kinds of products or services offered, you may be required to maintain compliance with rules like the U.S. Health Insurance Portability and Accountability Act (HIPAA), the General Data Protection Regulation (GDPR) in Europe, and the Payment Card Industry Data Security Standard (PCI DSS).

Organizations operating in the EU are also subject to specific rules governing the use of AI. The world's first major comprehensive legal framework on AI, the EU AI Act "aims to ensure that fundamental rights, democracy, the rule of law and environmental sustainability are protected from high risk AI, while boosting innovation and making Europe a leader in the field."

The legislation would prohibit AI systems that pose "unacceptable risk" from being used in the EU and require AI systems that pose "high risk" or "limited risk" to be subject to transparency requirements. This may include providing technical documentation, ensuring compliance with EU copyright law, and providing detailed summaries about how the system was trained. Slated to take effect in 2026, the EU AI Act will make waves globally and could inspire other nations to enact similar policies.

Did You Know?

Similar to the General Data Protection Regulation (GDPR), the EU AI act will apply to any providers or deployers of in-scope AI systems that are used in the EU, regardless of where the organization is headquartered.

The Bottom Line

AI presents both opportunities and challenges for businesses.

By implementing strong risk management practices, aligning with industry frameworks, and staying informed on evolving regulations, organizations can ensure their AI initiatives are secure, ethical, and compliant with industry and regulatory standards. The businesses that take proactive steps today will be best positioned to thrive in an AI-driven future.

> ***"Adopting technology before understanding the risks it poses can lead to catastrophic consequences, particularly when that technology has as broad a scope of impact as an AI tool."***
>
> Devin Olsen, Senior Consultant

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

Need help navigating compliance in the age of AI? Contact us today for a free consultation.