BARR ADVISORY

2024 Whitepaper

Managing AI Risk

A Strategic Approach to Compliance

Table of Contents

Introduction

The Rise of AI Innovation and Risk

Artificial intelligence (AI) has revolutionized industries, providing new opportunities for automation, efficiency, and innovation. From healthcare to finance, AI is driving significant advancements by augmenting decision-making, optimizing processes, and enhancing customer experiences. However, this rapid transformation has not come without challenges. As AI becomes more pervasive, it introduces new and evolving risks—ranging from bias and security vulnerabilities to compliance obligations.

Organizations that leverage AI must carefully navigate this landscape to harness its potential while safeguarding against the inherent risks. Effectively managing AI risk is no longer a choice, but a critical necessity for any organization looking to remain compliant, trustworthy, and competitive in the market.

> ***The widespread adoption of AI increases the likelihood of large-scale data breaches where massive amounts of personal information are compromised, leading to severe consequences for individuals and organizations.***
>
> Steve Ryan, HITRUST Manager at BARR Advisory

AI Risk Landscape

Emerging Challenges

While AI presents groundbreaking possibilities, it also poses complex challenges that must be addressed to avoid serious repercussions. Key risks associated with AI adoption include:

- **Bias and Discrimination:** AI systems are often trained on historical data sets that may contain hidden biases. These biases can lead to unfair, discriminatory outcomes in areas such as hiring, lending, and even healthcare. Organizations must ensure that their AI systems are designed and monitored to minimize this risk.

- **Privacy and Data Security Concerns:** AI requires vast amounts of data to function effectively, and that can include sensitive data. When users input sensitive data into AI systems, this can expose that data to potential breaches, unauthorized access, and misuse. Data security and privacy regulations—such as GDPR and CCPA—require organizations to implement strict safeguards around AI systems to prevent exploitation.

- **Transparency and Accountability:** Many AI systems, especially deep learning models, make it difficult for organizations to understand or explain how decisions are made. This lack of transparency can result in a loss of accountability, raising questions about responsibility when things go wrong.

- **Regulatory and Ethical Uncertainty:** Governments and regulatory bodies around the world are increasingly scrutinizing the use of AI, pushing for new regulations that demand transparency, fairness, and accountability in AI systems. As the regulatory environment evolves, organizations must be prepared to comply with these emerging rules while also adhering to ethical standards in AI development and deployment.

In response to these challenges, several risk management frameworks have emerged to help organizations address AI-related risks while maintaining compliance and fostering trust.

Addressing AI with Compliance

Where should my organization start?

To mitigate the complexities of AI risk, organizations need robust and adaptable compliance frameworks. These frameworks offer structured approaches to managing risks while ensuring alignment with industry standards and regulatory requirements. Three prominent frameworks that address AI risk include ISO 42001, HITRUST AI Risk Management Framework, and the NIST AI Risk Management Framework.

ISO/IEC 42001: AI Management System Standard

ISO/IEC 42001:2023—also known as ISO 42001—is a cybersecurity compliance standard designed to assess the security, safety, privacy, fairness, transparency, and data quality of artificial intelligence (AI) systems. Published in late 2023, the framework mandates numerous controls for the establishment, operation, monitoring, maintenance, and continuous improvement of an organization's AI management system (AIMS).

ISO 42001 was designed to serve organizations of all sizes and across all industries that participate in the use or development of AI-powered products and services. Additionally, organizations should consider ISO 42001 certification if they wish to demonstrate to internal and external stakeholders their ability to manage AI for decision-making, data analysis, or continuous learning.

Achieving compliance with ISO 42001 not only offers a competitive advantage to AI-powered businesses, but also positions your organization as one that prioritizes the ethical and responsible use of AI. Designed to integrate with standards such as ISO 27001 and ISO 27701, the framework serves as a seamless and smart addition to a modern, comprehensive compliance program.By implementing ISO 42001, organizations can better manage the full lifecycle of their AI systems, ensuring they are deployed safely, securely, and in compliance with international standards.

NIST AI Risk Management Framework

The National Institute of Standards and Technology (NIST) has developed an AI Risk Management Framework designed to help organizations understand, manage, and reduce the risks associated with AI systems. In collaboration with the private and public sectors, NIST developed the framework to better manage risks to individuals, organizations, and society associated with AI. The NIST AI Risk Management Framework is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. It is highly adaptable and can be applied across various industries to address AI's specific challenges.

Addressing AI with Compliance

HITRUST AI Risk Management Framework

HITRUST has launched the HITRUST AI Risk Management Assessment (AI RM Assessment), a comprehensive solution designed to help organizations evaluate and manage AI-related risks. This new assessment isn't just for those with existing HITRUST certifications—it's available to any organization that uses or produces AI technologies. Key features of the HITRUST AI Risk Management Framework include:

- **Comprehensive Coverage:** The HITRUST AI RM Assessment is built on 51 robust and practical risk management controls. These controls are harmonized with industry-leading standards such as ISO/IEC 23894:2023 and the NIST AI Risk Management Framework. This alignment ensures that organizations receive a thorough evaluation.

- **Proven Platform:** The assessment is supported by HITRUST's powerful MyCSF platform, known for its consistent, reliable results. This cloud-based solution simplifies the assessment process, enabling organizations to manage their AI risk management efforts efficiently and effectively.

- **Actionable Insights:** Beyond merely identifying risks, the HITRUST AI RM Assessment provides detailed scoring and a professional AI Risk Management Insights Report. This report offers a clear understanding of an organization's AI risk management stance and highlights potential gaps that need addressing.

> “
>
> ***AI can be a useful tool, but business leaders who want to harness the power of AI in 2024 must take active steps to adequately assess their risk.***
>
> Kyle Helles, Partner and Attest Practice Leader at BARR Advisory

Coordinating AI Risk and Compliance

With our coordinated audit approach, we help businesses streamline these efforts by integrating AI risk management frameworks, such as ISO 42001, into their broader compliance engagements—such as SOC 2, ISO 27001, and more.

This approach delivers a unified, simplified compliance process that reduces audit fatigue, optimizes resource allocation, and ensures that AI risk management is part of the overall compliance strategy. By combining multiple audits and assessments into a single, coordinated engagement, BARR Advisory enables organizations to reduce complexity, enhance efficiency, and ensure comprehensive risk coverage.

With our expertise in cybersecurity, compliance, and AI, we help organizations stay ahead of regulatory changes while fostering a culture of ethical and responsible AI development.

Secure Your Future with BARR

As AI continues to shape the future of business, organizations must address the risks and challenges that accompany this transformative technology. At BARR Advisory, we help businesses implement comprehensive AI risk management strategies by integrating leading frameworks into a streamlined compliance process.

Our coordinated audit approach ensures that organizations can focus on innovation and growth, knowing that their AI systems are secure, ethical, and compliant. Trust BARR Advisory to be your partner in navigating the complexities of AI risk and compliance, so you can unlock the full potential of AI with confidence.

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 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 AI risk management services?
Contact us today.