OPTIMA

Regulatory Alert

AI Is Already in Your Firm. Are You Managing It?

Artificial intelligence has quickly moved from a future technology to an everyday business tool. Employees are using AI to draft emails, summarize meetings, analyze documents, and accelerate routine tasks. In many organizations, adoption is happening faster than leadership teams can establish governance around it.

For financial firms, that creates a unique challenge.

The conversation is often centred on how AI can improve productivity. The more important question may be what happens when AI is used without appropriate oversight.

Unlike most new software, AI creates risks that are not always visible. Sensitive information can be entered into external platforms. Employees can rely on inaccurate outputs that appear credible. Cybercriminals can use AI to create convincing phishing emails, fake videos, and fraudulent communications that are increasingly difficult to identify.

The reality is that AI is not a future risk. It is a current operational risk that firms need to address today.

The firms that will benefit most from AI will not necessarily be those that adopt it fastest. They will be the organizations that establish clear guardrails, educate employees, and implement the right controls before widespread adoption takes place.

TRUST, BUT VERIFY

AI can be an incredibly valuable business tool, but it should be treated much like a highly capable intern. It can help accelerate research, draft communications, and organize information, but its work should never be accepted without review. Ultimately, the responsibility for the final product still rests with the employee using it.

One of the most well-known limitations of AI is its tendency to generate information that sounds authoritative but is incorrect. These errors, often referred to as hallucinations, can include fabricated statistics, inaccurate summaries, or citations that do not exist.

Even the companies building AI are not immune to these mistakes. During a public demonstration of Google's Bard chatbot, the system provided inaccurate information about the James Webb Space Telescope. The incident quickly became a reminder that confidence and accuracy are not always the same thing when it comes to AI-generated content.

BEFORE YOU PASTE INTO CHATGPT

One of the most overlooked risks associated with AI involves the information employees choose to share with it. Many users do not realize that certain AI platforms may retain prompts, outputs, or conversations depending on the product and licensing model being used.

When employees enter client information, internal communications, meeting notes, financial data, or proprietary business information into an AI tool, they may be exposing sensitive information to a third party.

A useful rule of thumb is to ask: Would you be comfortable sharing this information with an intern from outside your organization? If the answer is no, it likely should not be entered into an AI platform unless the firm has specifically approved the tool and verified its privacy protections.

For that reason, organizations should strongly consider enterprise-grade AI platforms that clearly state they do not use customer data to train their models and ban unapproved AI models (shadow AI). This remains one of the most important controls firms can implement as AI adoption expands.

THE RISE OF AI-POWERED FRAUD

Even organizations that restrict internal AI usage will still encounter AI-generated content. Criminals are increasingly using AI to create more convincing scams, impersonations, and social engineering attacks.

In one widely publicized case, an employee at professional services firm Arup was reportedly deceived into transferring approximately $25 million after participating in a video conference that appeared to include company executives. The individuals on the call were later determined to be AI-generated deepfakes.

As these technologies become more accessible, firms should expect fraudulent emails, voice messages, videos, and other forms of communication to become increasingly sophisticated. Traditional verification processes are becoming more important, not less.

GOVERNANCE BEFORE ADOPTION

The most effective AI strategy is not simply adopting new tools. It is establishing governance before adoption occurs at scale. This involves assigning responsibility internally and knowing how AI is being used within the business. The same AI models will have varying degrees of risk dependent on specific use cases. Compliance and IT can't create a positive control environment without knowing how its being utilized.

Every firm should have a clearly defined AI policy that addresses approved tools, acceptable use cases, data handling requirements, human review expectations, and employee responsibilities. Organizations should also ensure that AI platforms are integrated with identity management controls such as Single Sign-On to maintain visibility and access control.

Training is equally important. The cyber threats organizations already face, including business email compromise, social engineering, and ransomware, become even more effective when enhanced by AI-generated content. Employees must understand both the opportunities and the risks associated with these tools.

AI is not inherently a cybersecurity risk. Unmanaged AI is.

As adoption accelerates across the financial sector, firms should focus on implementing governance, educating employees, and deploying controls that support innovation without compromising security. Organizations that establish those guardrails today will be better positioned to capture the benefits of AI while avoiding unnecessary risk tomorrow.

SO, WHAT'S NEXT?

For many firms, the challenge is no longer deciding whether AI will become part of the business. It already has.

The next step is understanding how it's being used, ensuring employees know how to use it responsibly, and establishing governance that can evolve alongside the technology.

Over the past several months, these have become some of the most common conversations we're having with clients. As a result, we've expanded our AI offerings to help firms move from awareness to action.

AI STAFF TRAINING

A one hour, instructor-led session that gives employees practical guidance on using AI safely and responsibly in the workplace.

Topics include:

- Appropriate use of AI tools
- Confidentiality and data handling considerations
- Prompting best practices
- Recognizing AI enabled cyber threats and social engineering
- Firm expectations and acceptable use
- Live Q&A with real world scenarios

Each session is tailored to your firm's AI policies, approved technologies, and day to day operations.

AI READINESS ASSESSMENT

A practical review designed to help organizations evaluate their current AI governance framework and identify opportunities to strengthen oversight before adoption continues to expand.

The assessment includes a review of:

- AI governance and oversight
- Existing AI policies and acceptable use guidance
- Employee awareness and training
- Data handling and confidentiality practices
- AI tools and third-party vendor usage
- Cybersecurity and regulatory considerations
- Practical recommendations to strengthen your AI program

Whether your organization is just beginning to explore AI or already has employees incorporating it into their daily work, these services provide a practical roadmap for building the governance and controls needed to support responsible AI adoption.

If you'd like to learn more about either offering or simply discuss how other firms are approaching AI governance, we'd be happy to continue the conversation. Please take our Artificial Intelligence Usage Survey or reach out to the Optima Partners Cyber team at **cybersales@optima-partners.com**.