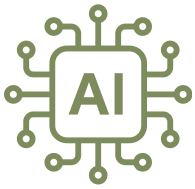
# Artificial Intelligence and Emerging Cyber Risk
# How Companies Can Start Assessing AI-Specific Risk

*August 2026*

Firms are rapidly adopting Artificial Intelligence ("AI") to improve efficiency, reduce manual work, expand research capabilities, and accelerate business processes. AI is also increasingly embedded into common business tools, including productivity platforms, meeting applications, document systems, customer relationship management platforms, and automated workflows. In other words, AI is already so deeply integrated into our working environment, we barely know when we are using it.



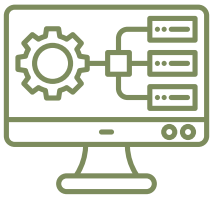

While AI can provide meaningful benefits, it also introduces risks that many companies have not fully identified or assessed. The question is not simply whether a company "uses AI." The more important questions are: i) where is AI already being used? ii) what information can AI tools access? iii) how are employees using AI (are they aware of their use), and iv) do we have appropriate oversight over such use?

Traditional cybersecurity reviews remain important. Companies still need to evaluate access controls, endpoint protection, vendor risk, incident response, employee training, and other core cybersecurity safeguards. However, traditional cybersecurity reviews may not fully address AI-specific risks. Such risks include unmanaged employee use of AI tools and "off channel use", excessive data access, inaccurate AI output, confidential information exposure, prompt injection (See below for more information), and automated actions taken without sufficient review. These are the obvious risks, but with all new technology, we don't know what we don't know and with time and use, new issues emerge.

A practical AI risk assessment can help establish a baseline so firms can better understand how AI is being used by their people, where material concerns may exist, and whether additional safeguards or oversight should be implemented.

## AI-Specific and AI-Amplified Cybersecurity Risks

AI concerns do not replace traditional cybersecurity concerns but can change how certain risks arise and how quickly they spread. Some risks are specific to AI systems, while others are traditional cybersecurity risks that AI can make more convincing or more difficult to detect.



For example, AI can help bad actors create more polished phishing emails, impersonation attempts, fraudulent communications and social engineering campaigns. AI-generatied messages can be targeted, well-written, and harder for employees to identify as suspicious. Voice cloning, deepfake video, and AI-generated images may also make impersonation attempts more credible.

While external risks are abundant, many AI risks arise from inside the organization. Employees may use personal, consumer, or unapproved AI tools for company work without understanding the potential consequences or knowing they are doing so. Employees may be uploading documents, pasting emails, summarizing meeting notes, drafting communications, or analyzing client or company information using tools that have not been vetted or approved.

***The risks are  not determined by whether an AI tool is free or paid for. The risks emerge based on whether the company understands:***

- Which AI tools are being used.
- Whether those tools are approved for business use.
- What information employees are uploading or sharing withAI tools.
- Whether such data may be retained, reviewed, or used by the vendor.
- Whether the company can monitor or audit AI usage.
- Whether appropriate access, retention, and privacy settings are in place within the tools being used.

A company cannot effectively manage AI risk if it does not know where and how AI is being used, Period.

## The Securities and Exchange Commission ("SEC")

The SEC has not updated rules for AI. Rather, the SEC appears to view AI as a tool similar to other financial service provider tools. The SEC has included questions about AI use during its adviser examinations and in March 2025 the SEC held an roundtable focused on the use of AI in the financial services industry. [1] Generally speaking, the round table identified issues and several practices to consider when financial services companies use AI including;

- **H**aving a reasonable basis for the belief that the AI output is appropriate given an adviser's fiduciary duty and is in the best interest of the client.
- The adviser must understand AI's limitations, and ensure its outputs are in the client's best interest.
- Identifying cybersecurity as a risk when using AI.
- AI use for advertising must be substantiated and not misleading.
- Advisers' policies and procedures must be reasonably designed to prevent violations of the Advisers Act. This means AI-related risks should be identified, and compliance programs should be updated to address and manage them.
- Do not treat AI as a simple software upgrade. Consider how AI is incorporated into the governance structure of the company, with appropriate stakeholders (legal, compliance, IT, and investment professionals) to oversee AI adoption, testing, and implementation.
- Conduct rigorous vendor due diligence. The diligence process should scrutinize the vendor's methodology, data sources, testing procedures, and its approach to managing bias and conflicts.
- Testing AI to ensure the quality, integrity, and security of the data used to train and/or operate AI models.
- Documenting the reasonable basis for distributing investment advice, and model risk management provided by AI.
- Training so that all personnel, from portfolio managers to client-facing staff, are educated about the capabilities and limitations of the AI tools being used, as well as the adviser's policies and procedures governing their use.
- Accountability: "the model told me so" is an insufficient answer to a regulator's inquiry. The SEC will hold advisers accountable for the outcomes produced by the technology they use.

## Data Privacy Issues

One of the most significant AI risk areas is data access. AI tools may receive information through prompts, uploaded files, meeting transcripts, emails, chat messages, document repositories, databases, plugins, connectors, APIs, or automated workflows.

[1] SEC.gov | SEC Roundtable on Artificial Intelligence in the Financial Industry

In some cases, an AI tool may only process information directly provided by the user. In other cases, AI tools may be connected to company systems and able to retrieve information based on user permissions, integrations, or configured data sources. This can create risk if the AI tool has access to more information than necessary.

Companies should determine and monitor:

- What systems and repositories AI tools can access.
- Whether AI tools inherit user permissions.
- Whether integrations or service accounts have excessive access.
- Whether sensitive folders, documents, or records are appropriately restricted.
- Whether AI activity is logged and auditable.
- Whether company, client, or personal information is being entered into unmanaged AI tools.
- Whether data submitted to AI tools may be retained, reviewed, or used for training.

AI tools should be configured based on business need at the start of use, not broad convenience. Excessive access can increase the risk of confidential data exposure or unintended disclosure. These choices should be made by the company and not the individual user.

## Inaccurate Output and Overreliance

AI tools can generate useful content, but AI output is not automatically accurate, complete, current, or appropriate for business use. AI systems may produce unsupported claims, inaccurate summaries, outdated information, fabricated citations, or content that appears authoritative but is incorrect.

This risk is especially significant when AI-generated content is used for client communications but certainly not limited to that. These risks extend to research summaries, business recommendations, policies and procedures, marketing materials, contract summaries, internal reports, or operational decisions. The ease of use and seeming efficiency are temptations we find hard to resist, so the cost should be front and center to users.

Companies should consider employee AI training to include the following topics:

- When AI may be used.
- What types of AI output require review.
- Who is responsible for validating AI-generated content.
- Whether AI-generated content may be used in external communications.
- Whether certain uses of AI require approval and by whom.
- Whether source materials or supporting documentation should be retained.

***AI should support human judgment, not replace it, so appropriate review and oversight is important.***

## Prompt Injection and Automated Actions

Prompt injection is an AI-specific risk in which malicious or unintended instructions influence how an AI system behaves.

This risk becomes more significant when an AI system has access to confidential information or is connected to tools that can send emails, retrieve files, create records, update systems, or trigger workflows.

This is why companies should consider whether appropriate safeguards exist around data access, external communications, system changes, logs for auditing, and human review before AI-enabled workflows are used in higher-risk business processes.

## Intellectual Property Infringement


AI tools also create intellectual property and content-related risks. Employees may use AI to generate marketing materials, client communications, research summaries, presentations, policies, software code, images, or other work product without knowing whether the output is accurate, original, properly sourced, or appropriate for business use. Such work product may use copyrighted, trademarked or patented material inadvertently exposing the company to a host of legal issues.

Employees may also input proprietary company information or third-party materials into AI tools without considering whether the tool is approved for that use. AI outputs may include unsupported claims, “hallucinated” citations, or content that resembles protected material.

An AI risk assessment does not resolve legal questions about ownership, copyright, trademark infringement, or permissible use. Those questions should be addressed by qualified legal counsel when appropriate. However, an assessment can help a company understand where AI-generated content is being used, whether employees have guidance on acceptable use, and whether outputs are reviewed before publication or distribution.

## Accountability

AI risk management requires clear ownership. Without defined accountability, AI adoption can become fragmented across departments, vendors, platforms, and individual employees.

Companies should understand who (Internally or externally) is responsible for:

- Approving AI tools.
- Reviewing vendor data-handling practices.
- Configuring access and permissions.
- Monitoring usage.
- Maintaining acceptable-use policies.
- Training employees.
- Reviewing high-risk AI outputs.
- Approving AI-enabled workflows.
- Managing exceptions.
- Responding to AI-related incidents.
- Communicating material AI risks to leadership.

Depending on the organization, appropriate stakeholders will include some combination of the business leadership, the IT team, cybersecurity vendors, compliance and/ or legal professionals, operations, data owners, and outside service providers. Identifying who is accountable is key to making the risk assessment valuable.

## What Makes an AI Assessment Different

Traditional cybersecurity reviews remain essential, but they may not fully integrate AI -specific vulnerabilities.  It is unlikely a traditional cybersecurity review will address how the AI tools a company uses is configured, what information the tool can access, what actions AI-enabled tools can take, or how employees are using unapproved AI services. An AI specific assessment addresses these questions.

The purpose of an AI risk assessment is not to discourage AI adoption. The goal is to help companies understand their current environment, identify meaningful risks, and prioritize practical improvements, with the overarching goal of protecting the company and its clients.

## What an AI Assessment Should Review

A practical AI assessment should be proportionate to the company’s size, technology environment, business needs, and actual AI usage. It should not create an unnecessary administrative burden or recommend broad technology changes where the risk does not justify the cost or effort. Like all useful risk assessments in the financial services industry, the assessment should be tailored to the company.

An effective AI assessment should generally review three primary areas:

- **AI tools and usage**, including approved tools, embedded AI features, unmanaged employee use, and AI-enabled business processes.
- **Data access and configuration**, including whether AI tools can access sensitive information and whether access is appropriate for the business purpose.
- **Oversight and operational controls**, including policies, training, approval processes, output review, accountability, and controls over AI-enabled actions.

An assessment should help identify both control gaps and effective practices already in place. And it should evolve with the fast-evolving world it is assessing.

## Conclusion

AI can create meaningful business value, but companies should not assume that the existing cybersecurity and technology reviews they already have in place, address AI-specific risks. AI tools are already present in common business applications, document systems, communication platforms, data repositories, and automated workflows. Employees may also be using personal or unapproved AI tools without leadership visibility. All of these uses should be enumerated, vetted, and monitored on a continuous basis in order to safeguard the firm, its proprietary information and its clients.

A practical AI risk assessment can help establish a baseline. It can help identify where AI is being used, what information AI tools may access, what controls are already in place, and whether targeted improvements may reduce risk. For firms that have not yet evaluated AI usage across the organization, this type of review can provide leadership with a clearer understanding of current practices and potential areas of concern.

As the SEC continues to evaluate the risks associated with AI, and as firms face incidents involving unmanaged or poorly controlled AI use, it is reasonable to expect AI governance, cybersecurity, supervision, vendor oversight, and documentation practices to become areas of increasing regulatory scrutiny. Because investment advisers owe a fiduciary duty to their clients and investors, firms that establish a periodic AI risk assessment process will be better positioned to demonstrate that they understand how AI is being used, have considered the related risks, and are taking reasonable steps to protect client, investor, and firm information.

**About 3iCO**

3iCO is a compliance solutions firm serving regulated financial services companies, including investment advisers, broker-dealers, private funds, private equity firms and registered investment companies. Founded by experienced Chief Compliance Officers andattorneys, 3iCO provides practical, proactive compliance solutions grounded in deep regulatory expertise and a people-first approach. Its multidisciplinary team works as an extension of each client's business, combining insider understanding with the independence required for effective oversight. 3iCO helps firms manage risk, strengthen their compliance programs and move their businesses forward with confidence. **People First Compliance. Business Forward Thinking.**

**About Centient1**

Centient1 is a technology consulting firm that helps small and mid-sized businesses apply AI, automation, integration, data, and custom technology solutions to real-world business needs. Centient1's AI Assessments provide a practical review of how AI is being used across an organization, what information AI tools can access, and whether appropriate technical, operational, and governance controls are in place. The goal is to help firms identify meaningful risks, prioritize practical improvements, and adopt AI with greater visibility and confidence.