

24 APRIL 2023 • 10 MINUTE READ



AI tools are already here: How they can help compliance officers, and four general principles

Written by: Brian Benjet, Bennett Borden, Katrina Hausfeld, Evan Liu, Gregory Ferroni

Artificial intelligence (AI) technologies such as self-driving cars and ChatGPT, are increasingly in the public eye – and are often being portrayed as dangerous, dystopian wild cards – even villains. But the quiet, inexorable rise of AI tools and systems over the past several years has brought myriad benefits to the corporate world. Companies across industries are leveraging AI to automate routine tasks, optimize decision-making, and drive efficiencies.

Similarly, AI is rapidly changing the landscape of corporate compliance. AI-powered solutions can help compliance officers to automate tasks, identify risks, and investigate potential misconduct. However, there are several issues that compliance officers need to be aware of before implementing and deploying AI solutions.

The regulators' expectations for AI and compliance

The growing capabilities and availability of AI tools in data analytics has certainly not escaped the attention of regulators who are increasingly expecting, if not actually demanding, that organizations use AI and data analytics to drive compliance within their organizations. While the use of AI has been accepted by regulators for some time to assist with the review and production of documents in response to government subpoenas and litigation discovery requests, there is now also recognition that well-designed AI tools and data analytics deployed against large and diverse datasets can be ideal instruments to assist in the identification and mitigation of risks, monitor compliance, and detection and investigation of potential violations that might otherwise be too unwieldy for "conventional" methods and human analysts.

For instance, the Department of Justice's (DOJ) guidelines on the [Evaluation of Corporate Compliance Programs \(ECCP\)](#), while not addressing AI specifically, have long emphasized the importance of leveraging the corporate data available within the company to ensure that its compliance program is well-designed, adequately resourced and empowered to function effectively, and working in practice. Key considerations for prosecutors who are assessing a compliance program include a) whether the compliance function has access to relevant data sources within the company and b) how the company is utilizing the data to understand the risks the company is facing and to monitor and test the effectiveness of its program.

The ECCP also makes it clear that compliance officers will be expected to address any impediments to access/use of the data – which can be reasonably interpreted to include addressing how to triage and assess the volumes of data potentially available. Indeed, at the American Bar Association's National Institute on White Collar Crime in Miami last month, Assistant Attorney General Kenneth Polite [noted](#) that prosecutors themselves are using "proactive and sophisticated methods of identifying criminal wrongdoing" including "ground-breaking data analytics."

How AI tools can help the compliance officer today

The growing capabilities and availability of AI tools in data analytics can assist modern compliance officers in assessing the effectiveness of their compliance program and monitoring for potential risks in a number of ways.

- **Identifying potential risks.** AI can be used to analyze large amounts of data, such as transaction data, employee records, and social media data, to identify potential risks that may not be apparent to human analysts. This can help

compliance officers by focusing their attention on the areas that are most likely to pose problems. For example, AI can be used to identify unusual transactions that may be indicative of fraud or money laundering.

- **Monitoring compliance programs.** AI can be used to monitor compliance programs to ensure that they are being implemented effectively. This can help to identify areas where a program may be lacking and allow for corrective action before problems surface. For example, AI can be used to review employee training records to ensure that employees are aware of the company's compliance policies and procedures.
- **Providing insights into compliance data.** AI can be used to analyze compliance data to provide insights that can help compliance officers to make better decisions. The strength and capabilities of AI can be leveraged to identify patterns and relationships that may escape the attention of human analysts. For example, AI can be used to identify trends in compliance data that may indicate a need for changes to the company's compliance program.
- **Automating compliance tasks.** AI can be used to automate some of the more mundane compliance tasks, such as reviewing documents and reports. This can free up compliance officers to focus on more strategic tasks. For example, AI can be used to review employee expense reports to identify potential fraud or errors.

AI data analysis tools are proving themselves capable of digesting diverse datasets in search of patterns and relationships that may not be obvious or even visible to human analysts. Further, these tools can process immense volumes of data quickly, accurately, consistently, and cost-effectively.

For example, AI powered risk scoring systems that review relationships between employees, vendors, and other third parties, analyzing travel, expenses, and other transactions can assist organizations in identifying behavior that may be at risk for violating the Foreign Corrupt Practices Act, allowing the organization to take steps to mitigate these risks. Similarly, healthcare organizations may use AI to sift through many types of clinical data such as medication dispensed, nursing observations, and treatments prescribed to identify patients at increased risks for falls or other specific complications.

However, it must be noted that AI systems cannot provide the context that only human analysts can. Overall, AI can be a valuable tool for compliance officers; it can help them to identify potential risks, monitor employee behavior, generate reports, provide recommendations, and educate employees about compliance. But compliance officers will need to carefully navigate the interplay between these

powerful tools, the data that they are applied to, and the results and recommendations that are generated to avoid significant pitfalls.

What compliance officers need to know before deploying AI solutions

There is no question that AI is rapidly changing the landscape of corporate compliance. AI-powered solutions and data analytics clearly can help compliance officers to automate tasks, identify risks, and investigate potential misconduct. However, as with any rapidly evolving technology, there are a number of issues and challenges that compliance officers need to be aware of before deploying AI solutions within their corporate compliance programs.

Perhaps one of the biggest challenges facing compliance professionals is **assessing bias in AI models**. AI models are trained on data, and if that data is biased, the model will be biased as well. This can lead to problems if the model is used to make decisions, particularly if those decisions are about people, such as whether to approve a loan or hire someone for a job.

There are a number of ways to assess bias in AI models. One is to assess the data that the model is trained on. If the data is biased, the model will be biased as well. For instance, if a model is trained on data that includes more men than women, the model may be more likely to favor men. Another is to closely evaluate the results of the model. If the model is consistently making decisions that are unfair or discriminatory, it may be biased. For example, if the data used to train an AI system used for job applicant screening comes from performance data of previous employees, it is possible that without proper attention, the tool could make recommendations that repeat or even amplify prior biases against certain groups of applicants such as women or those with certain disabilities.

Another significant challenge is **understanding the logic of AI models**. AI models are often complex and opaque, and it can be very difficult to understand how decisions or recommendations are made. This can make it difficult to trust the results of the model and to explain the model's decisions to others.

Clearly, it is important to understand the logic of AI models in order to trust the results of the model and to explain the model's decisions to others. There are a number of ways to understand the logic of AI models. While it may be possible to examine the underlying code that the model is written in, perhaps a more accessible method might be to evaluate the data that the model is trained on. Alternatively, it may be more helpful to engage in discussions with the people who developed the model to understand their thinking and methods behind the model.

Finally, compliance officers must ensure that any AI solution they deploy **complies with all applicable regulations, including data privacy laws**. This can be a challenge, particularly in cross-border situations, as there are sometimes no specific regulations, or regulations in evolution, governing the use of AI in compliance, or more specifically, addressing the privacy of the data that is being used or requested by the AI tools. For example, just within the United States, some state jurisdictions such as **California**, New York, Massachusetts are pushing forward legislation affecting and regulating the use of AI. In a much more comprehensive effort, the European Union is in the process of engaging in an ambitious proactive effort to regulate multiple aspects of the use of AI (including human autonomy, privacy, and dignity) that will likely have far-reaching effects.

Four general principles for deploying AI in compliance

To appropriately deploy AI technologies in compliance, it is useful to consider these general principles.

First, compliance officers must consider the impact of deploying AI data analytics within their compliance programs, particularly considering **potential liability**. In general, such tools should be thoughtfully deployed in a focused and step-wise manner, with an emphasis on prospective compliance rather than retrospective examination.

Second, AI must be deployed and used in a **transparent and accountable** way. Compliance officers should be able to explain how the AI model works and why it makes the decisions that it does. Further, officers should also be able to demonstrate that the AI model is accurate and reliable.

Third, AI must be used in a **fair and non-discriminatory** way. AI should obviously not be deployed in a way that generates unfair or discriminatory decisions or recommendations. Compliance officers must be aware of the potential for AI models to be biased and take steps to mitigate bias.

Finally, compliance officers should use AI in a way that respects and adheres to **privacy and data protection** laws, only using data that is necessary for the purpose of compliance and taking concrete steps to protect the privacy of individuals whose data is used within the AI models.

Given the complexity of AI and data analytic systems, the large volumes of data that are often produced, and the impactful decisions and recommendations that are generated, close partnership between compliance officers and legal counsel is

often invaluable. To learn more about the rapidly evolving landscape of artificial intelligence tools and corporate compliance, how it will affect your business, and how DLA Piper can assist you and your company in navigating a clear path, please contact any of the authors or your usual DLA Piper counsel. You may also be interested in our new resource center, [Focus on Artificial Intelligence](#).

If you'd like to discuss how to monitor AI systems for unintended bias, please reach out to [Bennett Borden](#) or [Danny Tobey](#).

Related insights



Publication

SPRS cybersecurity reporting: It's now more than just a number

12 APRIL 2023 • 3 MINUTE READ



Publication

Regulatory, litigation and disclosure considerations concerning artificial intelligence

27 FEBRUARY 2023 • 2 MINUTE READ



Past event

The future of AI law: webinar playback

12 APRIL 2023 • 2 MINUTE READ

Related capabilities

Regulatory and Government Affairs

White Collar and Corporate Crime

Compliance

Global Investigations

Corporate

Technology

Artificial Intelligence and Data Analytics

People

Capabilities

About us

Insights

Careers

Locations

News

Events



Find an office

Subscribe

Contact us

[Legal notices](#)

[Privacy policy](#)

[Cookie policy](#)

[Modern slavery](#)

[Sitemap](#) 

DLA Piper is a global law firm operating through various separate and distinct legal entities. For further information about these entities and DLA piper's structure, please refer the [Legal Notices](#) page of this website. All rights reserved. Attorney advertising.