Secretariat

Mitigating AI Risks: Insights from Regulatory Guidance and Enforcement

by Bilal Shah, Eric Poer, Edward Westerman, Richard Finkelman,
Chris Riper, John Rademacher, and Abby Williams

MARCH 2025

TABLE OF CONTENTS

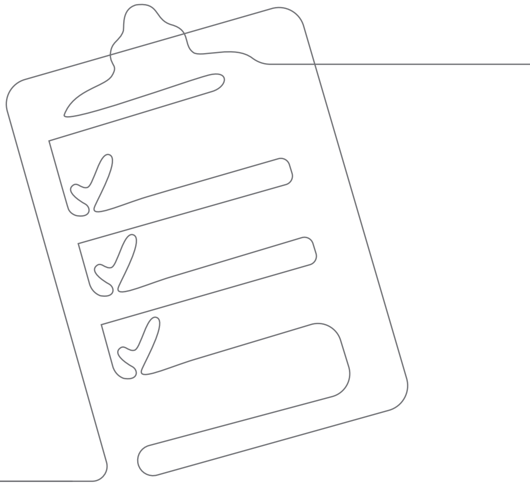
1

Introduction

The rapid rise of Artificial Intelligence (AI), particularly Generative AI, has transformed various industries. From finance, where AI algorithms help manage investment portfolios and detect fraud, to marketing, where it enables personalization for ad targeting, to operations, where predictive maintenance and logistics optimization have streamlined supply chains — AI is making its presence felt. The accelerated integration of AI has made organizations more efficient but has also introduced new risks, including ethical, privacy, and security challenges. Consequently, governments globally are implementing regulations to ensure responsible implementation and usage of AI (*e.g.* the EU AI Act).

Within the United States, AI regulation has been characterized by a patchwork of federal- and state-level initiatives, with states proposing more legislation (such as the Colorado AI Act of 2024) and the federal government providing fragmented policies and executive orders aimed at fostering innovation and managing risks. The Department of Justice (DOJ) and Securities and Exchange Commission (SEC) have been active in providing guidance and bringing enforcement actions related to AI. The DOJ recently updated its guidance for the evaluation of corporate compliance programs to include specific considerations for AI and emerging technologies,[1] while the SEC designated AI-related risks (for investors) as a primary focus for its 2025 Examination Priorities.[2]

This article provides an overview of AI policies in the United States at the federal level and discusses recent developments in AI oversight by the DOJ and SEC. Additionally, it offers recommendations for organizations implementing AI technologies to mitigate the risks identified by these regulators.



[1] https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl. [henceforth, DOJ Compliance Guidelines, 2024]

[2] https://www.sec.gov/files/2025-exam-priorities.pdf.

2

Overview Of AI Policies In The United States At The Federal Level

In the United States, various governmental agencies have been actively developing AI strategies and policies since at least 2016.[3] These initiatives share several overarching themes that organizations should adopt for their own AI journeys:

1. Promoting AI innovation and research;
2. Ensuring AI safety and security;
3. Protecting privacy and civil rights;
4. Developing an AI-ready workforce;
5. Establishing ethical guidelines for AI development and use; and
6. Enhancing international cooperation and U.S. leadership in AI.

Key initiatives of the US government have included:

- The Obama administration's National Artificial Intelligence Research and Development Strategic Plan in 2016, which identified priority areas for federally funded AI research.[4]
- The Trump administration's American AI Initiative in 2019 that prioritized increasing federal investment in AI R&D, reducing barriers to federal resources and ensuring technical standards for safe AI development and deployment.[5]
- The White House Office of Science and Technology Policy in October 2022, which released the Blueprint for an AI Bill of Rights, outlining five principles for the ethical development and use of AI systems.[6]
- President Biden's Executive Order 14110 in October 2023, which set forth a comprehensive framework for AI governance across eight policy areas, involving over 50 federal agencies in more than 100 specific tasks.[7] The order also established the White House Artificial Intelligence Council to coordinate implementation efforts.
- President Trump's executive orders in January 2025, which revoked previous AI policies perceived as restrictive to innovation, prioritized the development of AI systems free from ideological bias, mandated the creation of an "AI Action Plan" within 180 days, and directed the review of prior AI regulations to align with the new strategy.

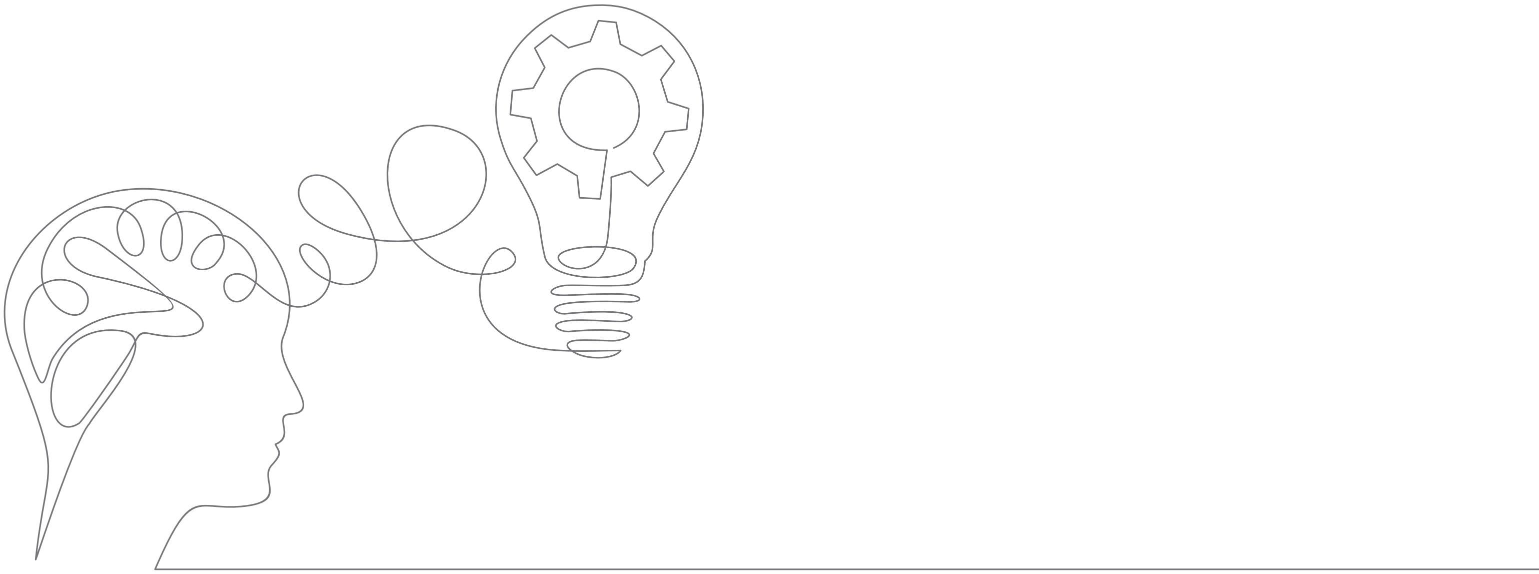
[3] https://iapp.org/resources/article/us-federal-ai-governance/.

[4] https://iapp.org/resources/article/us-federal-ai-governance/.

[5] https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Chapter-7.pdf.

[6] https://iapp.org/resources/article/us-federal-ai-governance/.

[7] https://iapp.org/resources/article/us-federal-ai-governance/.



Key initiatives by US governmental agencies, apart from the DOJ and SEC, include:

- The National Artificial Intelligence Initiative Act of 2020, which coordinates AI activities across federal agencies.[8]
- The AI Risk Management Framework developed by NIST in 2023.[9]
- The Department of Homeland Security's AI Public Sector Deployment Playbook.[10]
- The National Science Foundation's establishment of seven new National AI Research Institutes.[11]
- The Office of Management and Budget's guidance on use and procurement of AI for federal agencies.[12]

The DOJ released updated compliance guidance in September 2024, which included guidance on AI. This guidance was preceded by the DOJ's Justice AI initiative in February 2024,[13] and its comprehensive internal AI strategy[14] published in December 2020.

The SEC has also stepped up their AI oversight and enforcement efforts, including further scrutiny of cyber-security practices and financial disclosures involving AI technologies, as detailed in their 2025 Examination Priorities. This increased focus follows AI being identified as an emerging technology to keep an eye on in their 2024 Examination Priorities.[15]

Analyzing the DOJ's broad AI-related compliance guidance alongside the SEC's increased AI oversight and enforcement illustrates the overall compliance framework government agencies are promoting to hold organizations accountable for the responsible implementation and use of AI.

[8] https://www.softwareimprovementgroup.com/us-ai-legislation-overview/.

[9] https://iapp.org/resources/article/us-federal-ai-governance/.

[10] https://www.law360.com/technology/articles/2280757/dhs-releases-playbook-for-ai-public-sector-deployment.

[11] https://crsreports.congress.gov/product/pdf/R/R47843.

[12] https://epic.org/omb-finalizes-guidance-on-federal-government-ai-procurement/.

[13] https://www.justice.gov/archives/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-university-oxford-promise-and.

[14] https://www.justice.gov/d9/pages/attachments/2021/02/04/doj_artificial_intelligence_strategy_december_2020.pdf. [henceforth, DOJ AI Strategy 2020]

[15] https://www.sec.gov/files/2024-exam-priorities.pdf.

3

Key Takeaways On The DOJ's Updated Compliance Guide For Investigations Regarding AI

While the DOJ's updated compliance guide is directed toward investigators and prosecutors, it can also be interpreted as a compliance playbook for organizations. As such, we have broken down our key takeaways into two sections; DOJ's guidance to prosecutors and takeaways for organizations (management, boards, etc.).

At first glance, it might seem like the DOJ incorporated a small section for AI into its updated compliance evaluation guidelines. However, by incorporating AI as a component that needs to be accounted for, monitored, and controlled within a corporation's compliance program, and with AI becoming an increasingly integral part of operations and decision-making processes in many organizations, it is reasonable to assume that most, if not all, elements of a compliance program (and evaluation) can be applied to an organization's implementation and use of AI.

Key AI Guidelines for Prosecutors and Investigators

1. Assess the management of risks associated with the use of AI and their integration within the wider Enterprise Risk Management (ERM) strategy of the company, its AI governance, and the relevant internal controls put in place to be compliant "with applicable law and the company's code of conduct."[16]
2. Evaluate whether a company is regularly monitoring its AI-based decisions, especially to verify the tool's alignment with corporate ethics and legal standards.
3. Gauge access of company data to an organization's compliance department and personnel.
4. Appraise training programs for employees, and the level of technical training and qualifications of leadership of an organization.
5. Assess human oversight and Human-In-The-Loop (HITL) processes in core AI-driven decision-making.
6. Analyze risk assessments conducted by organizations on utilizing new technologies as well as relevant risk mitigation strategies.
7. Judge the frequency of testing technologies and their controls.
8. Evaluate how vendor management integrates with an organization's ERM framework, policies, review processes, and ongoing oversight.
9. Assess secure channels for reporting concerns at an organization, specifically concerning whistleblowing.
10. Gauge resource allocation for compliance and compare it to spending on revenue generation, daily operations, and profit-making.

[16] DOJ Compliance Guidelines, 2024, p. 4.

Key Takeaways for Organizations

1. INCORPORATE AI IN ERM

Organizations should explicitly account for AI within their ERM strategy and ensure mechanisms are in place to stay informed of the ever-evolving landscape of AI rules, regulations, and executive orders. Organizations should also maintain an inventory of their AI-related technology, uses, and risks, and assess whether appropriate controls have been put in place to mitigate risks to an acceptable level. In short, organizations should develop a structured framework for AI governance, aligning with DOJ guidance on compliance, ethics, and accountability. They should also define roles and responsibilities for AI oversight, including a cross-functional AI risk management committee.

2. MONITOR AI-BASED DECISION-MAKING

Organizations are increasingly using AI to make decisions within their commercial operations and compliance programs, which may add another layer of legal and ethical risks if appropriate guardrails are not implemented. Such risks can arise from bad and/or biased input data; failure to account for the evolving nature of data privacy and AI-specific regulations; lack of transparency and understanding of business processes pre-AI; lack of appropriate checks, balances, and human oversight to account for "hallucinations" (made-up answers by AI); and lack of data governance to avoid unauthorized access to data through AI solutions. Compliance programs should mandate regular monitoring of AI-based decisions to verify that AI decisions align with corporate ethics and legal standards. Due to the fast pace of AI evolution and its state of continuous learning, organizations must continuously evaluate the AI's efficacy, testing, alignment with the company's code of conduct, and speed of detection and correction of "wrong" AI decisions.

a. Corporate compliance programs should not only inventory all AI-based decision-making and their processes but should also ensure that there is ultimate transparency in the components of all AI-driven decisions (which are easily auditable and monitored).

b. Data quality controls should be implemented to prevent biased or inaccurate AI decisions.

c. Regular audits of AI-related datasets should be mandated to ensure fairness, accuracy, and compliance with anti-discrimination laws.

3. EVALUATE DATA ACCESS

AI models and algorithms often access sensitive data, either on a temporary or continuous basis, within commercial operations, business functions, or legal and compliance. Organizations should evaluate the risks associated with continuous access to sensitive data used by both in-house developed and third-party provided AI solutions and services vendors, especially in highly regulated industries such as finance and healthcare. Furthermore, the Chief Compliance Officer (CCO) of an organization should have continuous access to relevant data needed for mitigating legal and regulatory risk, including data being used in AI models, tools, and platforms.

a. Master data management and data governance solutions can help improve the accuracy of data analytics models and the efficacy of AI models by improving data quality. They also serve another function — improving transparency and data access for compliance officers and evaluators.

4. CONDUCT AI TRAININGS

Organizations should be up to date on their Data and AI governance, use, and security policies and conduct regular trainings for all employees related to the policies. Trainings should give equal importance to both the "Do's" and "Don'ts" of using company-mandated AI solutions and should be updated frequently to keep pace with the latest AI developments and risks. Trainings should also include the limitations of said AI solutions, links to appropriate policies and guidelines, and firm reminders of each employee's ethical and legal responsibilities when using firm-provided AI solutions. Basic trainings should be required at all levels, including for management and the board, to set a baseline for safe AI use. Advanced, risk-based (and in some cases, custom) trainings should be mandated based on specific roles within the organization.

5. EXERCISE HUMAN REVIEW

Human oversight is critical in mitigating AI risks arising from AI-driven decisions. The HITL is a core concept in building safe and reliable AI solutions, requiring that human review checkpoints be built in various places along the decision-making path of said AI solutions. Organizations implementing HITL systems should have clear testing, monitoring, and remedial policies drafted for each AI-driven (or assisted) decision path that human reviewers need to follow. Critically, organizations should have personnel with sufficient compliance expertise and qualifications to ensure appropriate human oversight of AI decisions. This also extends to senior management and board members as AI oversight becomes a critical component of board and management oversight. Senior leadership, management, and the board must stay up to date on the latest AI developments and associated risks.

6. FOCUS ON RISK MITIGATION

While AI offers many benefits, it also presents a plethora of internal and external risks, existing and new. AI thrives on data and improves rapidly the more data it is fed. However, as more internal and sensitive data is fed to AI solutions, the probability of risky events happening increases. Without appropriate risk mitigation strategies, risks such as bias in AI output, inadvertent access of sensitive data to internal non-authorized users, data breaches, consumer data theft, AI adversarial attacks, external and internal data poisoning, unethical decision-making, inaccurate outputs, and lack of auditability and traceability are increased exponentially. The key to good risk mitigation strategies is a thorough risk assessment. Organizations should evaluate how the use of new and emerging technologies, such as AI, impact the organization's risk profile, and then take meaningful steps to mitigate risk from its use. Organizations should establish clear protocols for investigating and remediating AI-related compliance violations. They should also conduct root cause analysis of AI failures and apply lessons learned to prevent recurrence.

7. TEST AI MODELS AND MITIGATING CONTROLS

Organizations should consider the extent and frequency of the testing and monitoring of AI models and their controls, pre- and post-production, to confirm reliability and detect potential system vulnerabilities, among other risks.

8. ASSESS THIRD-PARTY RISK FROM AI

Third-party management is a critical component of effective compliance programs. With most leading AI models hosted through enterprise cloud subscriptions, third-party management will keep gaining importance. As such, vendor management processes should be incorporated into an organization's ERM framework and policies. An organization should consider the effectiveness of the vendor review process, ongoing vendor risk monitoring and management, appropriate controls for use of third parties as well as the contracts signed with them, and their relationship with the third-party vendors. When sourcing AI solutions and technologies from third parties, organizations should be precise with their data use and privacy policies as well as the business purpose of the vendor agreement. Organizations should require third-party AI providers to comply with regulatory guidance on ethics, transparency, security and include AI compliance obligations in contracts with vendors and business partners. Additionally, organizations should assess the third-party provider's controls and risk management framework around its AI platforms, solutions, and technologies.

9. STRENGTHEN REPORTING MECHANISMS

Organizations should communicate their policies around AI misuse or ethical breaches, and ensure employees are aware of reporting channels for such cases. Whistleblower programs should be expanded to cover AI-related concerns and misconduct, and employees must have means to anonymously report AI misuse without fear of retaliation.

10. ALLOCATE RESOURCES

Organizations should allocate sufficient resources to compliance, proportionate to the level of assets, resources, and technology used to capture market opportunities and daily operations within revenue generation and profit making. Within the realm of AI, this would mean companies spending on researching, building, and implementing AI technologies into their operations should spend a proportionate amount on governance and compliance around the use of those AI technologies within their organizations.

4

Key Takeaways From The SEC's AI Oversight, Enforcement, and 2025 Priorities

The SEC has steadily been building their AI capabilities internally. They published their AI compliance plan in accordance with the Office of Management and Budget's M-24-10 memo, released their AI use case inventory, and actively use AI in risk analysis, cybersecurity threat detection, and data and document management, among other functions.[17] At the same time, they have stepped up their AI oversight and enforcement efforts:

1. In July 2023, the SEC proposed a rule under the Advisers Act requiring investment advisers to mitigate conflicts of interest arising from predictive data analytics.[18]
2. In August 2023, the SEC's Division of Examinations launched an AI-focused review ("AI sweep") to assess how private fund advisers use AI in client portfolio management, marketing, and supervisory controls.[19]
3. In March 2024, the SEC settled its first explicit AI-related actions against investment advisors over "AI-Washing" (misleading claims about AI capabilities).[20] It also began issuing comment letters to companies regarding their use of AI in disclosures, marking a sharp focus on enforcement issues tied to AI.[21]
4. In October 2024, the SEC identified AI as a key focus for its 2025 Examination Priorities. This includes further scrutiny of cybersecurity practices and financial disclosures involving AI technologies.[22] This focus follows AI being identified as an emerging technology to watch in the SEC's 2024 Examination Priorities.[23]

While the SEC is presently focused on "AI washing" due to the tactic readily falling within the ambit of existing laws, regulations, and compliance guidelines, it is acutely aware of other areas of AI concerns, such as AI and accounting fraud, algorithmic bias, AI and blockchain, AI and corporate governance, and robo-advising.[24]

[17] https://fedscoop.com/sec-artificial-intelligence-ai-financial-securities-markets/.

[18] https://www.mayerbrown.com/en/insights/publications/2024/04/securities-and-exchange-commission-brings-first-enforcement-actions-over-aiwashing.

[19] https://www.privateequitylitigation.com/2024/04/a-tale-of-two-regulators-the-sec-and-fca-address-ai-regulation-for-private-funds/.

[20] https://www.mayerbrown.com/en/insights/publications/2024/04/securities-and-exchange-commission-brings-first-enforcement-actions-over-aiwashing.

[21] https://business.cch.com/srd/SP_AI-enforcement-part-II_10-15-2024_final_locked.pdf.

[22] https://www.whitecase.com/insight-alert/sec-will-prioritize-ai-cybersecurity-and-crypto-its-2025-examination-priorities.

[23] https://www.sec.gov/files/2024-exam-priorities.pdf.

[24] https://www.sec.gov/files/sec-cfu-presentation.pdf.

The SEC has also warned individual actors of AI-related security risk disclosure failures, adopting a carrot-and-stick approach to ensure healthy cooperation. Disclosures in good faith will likely result in less scrutiny, whereas individual liability for disclosure failures will be treated as a security threat.[25]

Here is what organizations should take away from the SEC's activity regarding AI:

1. Both the DOJ and SEC have been purposefully broad about their views on compliance and enforcement over AI-related issues. This is because they need flexibility and experience as AI regulation evolves. The SEC is committed to preventing "AI washing," primarily because it is extremely similar to behavior that has been well-litigated over the past few decades. In light of this, organizations should be extremely conservative in their claims around expected use and ROI regarding AI.
2. Document AI use, inputs, outcomes, and relevant procedures. As the SEC broadens the net and purview of its "sweeps," organizations should be prepared for their investigators and demands. Similarly, organizations should clearly identify data being used in AI use and proactively have said data in a "discovery-ready" state.
3. Ensure appropriate disclaimers and AI use statements are put in all public disclosures (10Ks, 10Qs, press releases, etc.). Be extremely transparent in the use of AI and data within AI solutions. Thoroughly evaluate all disclosures and public statements on AI.
4. Be collaborative with the SEC in its investigations.

[25] https://www.whitecase.com/insight-alert/sec-warns-individual-actors-potential-liability-ai-related-security-risk-disclosure.

5

What Organizations Need To Be Asking Themselves

The DOJ's compliance guide draws inspiration from existing AI risk management frameworks (RMF), such as the NIST AI RMF Playbook, and shares similarities with the EU's AI governance policies and mandates. The clear message from its guidance is one of adopting transparency and strong controls with regard to AI implementation and use.

The SEC's remarks and actions about AI-related oversight and enforcement are very complementary to the DOJ's updated AI compliance guidance. By adhering to the DOJ's compliance guidelines (and/or risk management frameworks such as the NIST AI RMF) and evaluating their AI disclosures to investors, organizations will be well-equipped to respond to investigator inquiries should issues arise.

Key questions that organizations must be prepared to answer to help avoid DOJ and SEC investigations:

1. Do we have a robust AI governance framework?
2. Have we established clear compliance policies around the use of AI?
3. Do we have appropriate risk assessments and risk mitigation plans around our AI technologies and solutions?
4. Are our data and AI strategies aligned?
5. Is our data governance and master data management solid?
6. Do our vendor agreements comply with legal, ethical, and regulatory standards?
7. Are our cybersecurity, data privacy, data protection, and data quality measures sufficient?
8. Do we have proper controls over public messaging on AI?
9. Are our legal and compliance teams fully aligned with business development and operations?

DISCLAIMER

This publication was prepared by Secretariat for general information and distribution and is not intended to address the specific circumstances of any individual or entity. Although we endeavor to provide precise and timely information, there can be no guarantee that such information is accurate and complete as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. While the data used in this report stems from publicly available sources and are attributed throughout the publication, any analysis and views expressed are those of Secretariat alone.

ABOUT THE AUTHORS

Bilal Shah, *Director*
bilalshah@secretariat-intl.com

Bilal is a Chartered Financial Analyst and an economist by trade. He has more than 12 years of experience in litigation, economic, strategic, and Data & AI consulting.

Eric Poer, *Managing Director*
epoer@secretariat-intl.com

Eric has more than 20 years of experience leading complex investigations and providing attorneys and clients with dispute consulting and forensic accounting services.

Ed Westerman, *Managing Director*
ewesterman@secretariat-intl.com

Ed is a leading forensic accounting and internal investigations expert with more than 25 years of experience working on engagements in the US and around the world.

Richard Finkelman, *Managing Director*
rfinkelman@secretariat-intl.com

Richard advises clients on how to adopt machine learning and artificial intelligence solutions in the context of litigation and legal technology.

Chris Riper, *Managing Director*
criper@secretariat-intl.com

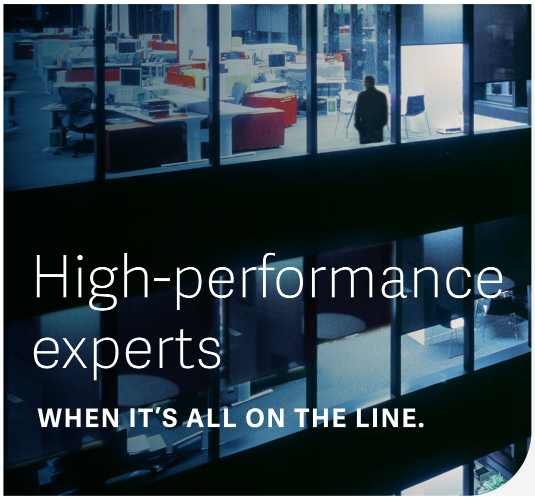
Chris helps clients resolve their high-stakes legal and regulatory issues. He also assists in complex litigation matters with data analytics, finance, accounting, and valuation support.

John Rademacher, *Managing Director*
jrademacher@secretariat-intl.com

John leads global investigations on behalf of Audit Committees, GC, CCOs, and their outside counsel, and advises clients on the design and operation of corporate compliance programs.

Abby Williams, *Director*
awilliams@secretariat-intl.com

Abby specializes in forensic investigations, litigation support, and ethics and compliance services, partnering with organizations and law firms in preventing, detecting, and remediating fraud and misconduct.



SECRETARIAT EXPERTS ARE TRUSTED in the highest-stakes legal, risk, and regulatory matters around the world. Renowned law firms, leading corporations, and respected governmental entities turn to our disputes, investigations, economic, and data advisory services when the stakes are high. Quality, integrity, and independence are woven into every aspect of our work.

We would like to hear from you

info@secretariat-intl.com | secretariat-intl.com