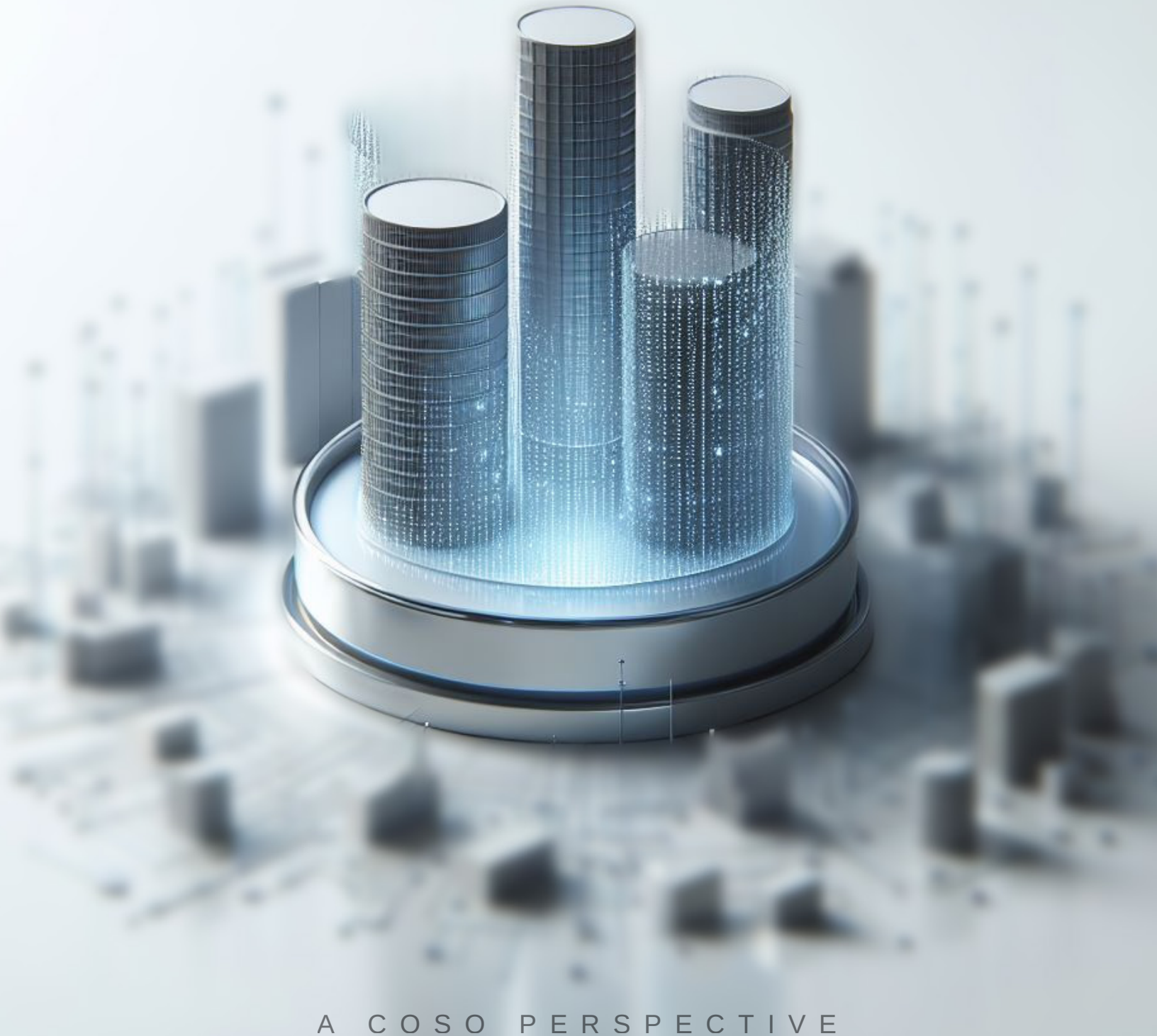
COSO

ALTDATA



A COSO PERSPECTIVE

Authors

Ryan Blair, Nicolas Dumont, Michael Egan, and David Navetta.

Acknowledgements

We would like to recognize and thank Nicolas Dumont of Cooley LLP for his leadership on this project. Additional thank you goes to the COSO Board, and COSO Board Chair and Executive Director Lucia Wind for providing input, assistance, and valuable feedback in developing this paper. We also thank Ryan Blair Partner, Michael Egan, Partner, and David Navetta, Partner, Cooley LLP for their technical input and advice.

COSO Board Members

This project was commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence.

COSO is a private-sector initiative jointly sponsored and funded by the following organizations:

American Accounting Association (AAA)

American Institute of CPAs (AICPA)

Financial Executives International (FEI)

The Institute of Management Accountants (IMA)

The Institute of Internal Auditors (IIA)

Design and layout: Sergio Analco

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org

Contents

Introduction

Risk management is an integral part of strategic planning and financial and operational success of any organization. The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) Enterprise Risk Management Framework (ERM) is used by risk professionals on their journey to proactively identify and manage emerging risks. This publication provides organizations with an introduction to the topic of alternative data, or altdata, as a possible significant risk factor for consideration. Every organization needs to be aware that altdata about them is widely collected, whether internally within an organization or by third parties. Emerging technologies, techniques, and concepts such as artificial intelligence, data management, harvesting, and security are all relevant risk topics that should be considered not only as they relate to financial and operational information, but to their potential implications for an organization's altdata as well.

Our publication provides a definition of alternative data, its potential uses, and how COSO's ERM Framework can be applied to the challenge and opportunity of altdata. The ERM framework is particularly helpful to identify, assess, and address certain risks relating to altdata, including inadvertent disclosure of sensitive or confidential information, reporting and compliance issues, and failure to maximize potentially significant value of altdata. As the significance of alternative data grows and evolves, both in terms of its value to organizations and its associated risks, boards of directors, senior management, data compliance, and disclosure personnel should each become familiar with the risks and opportunities it presents.

What is alternative data?

Altdata generally is understood to include information about an organization that is available outside of traditional financial and regulatory reporting channels, press releases, or other authorized materials. It includes data about an organization and its operations that the organization makes public or otherwise discloses to third parties knowingly or unknowingly. Altdata has no standard definition provided by industry groups or regulators, and as such the definition remains inherently fluid. Common sources of altdata include e-mail, information from mobile devices and apps, payment card transactions, geolocation data, social media information, sensors, web-scraped data, internet traffic, Internet of Things-based devices, satellite data, point-of-sale information, and rewards programs. This list is not exhaustive: as the volume of data produced by organizations rises, so too does the volume of altdata, absent operational or definitional reframing.

Every organization needs to be aware that altdata about them is widely collected. Altdata is commonly collected and used to identify patterns and obtain insights relevant to or about a target industry, company, or user-base. It is leveraged to gain market intelligence and advantage by using multiple available data points to extrapolate timely and valuable information.

The altdata market has grown significantly in recent years and is expected to continue to do so. This increase is in part linked to the exponential growth of the amount of data resulting from the digitalization of the world and its economy. As data proliferates, companies' data ecosystems expand in turn. This trend likely is to be compounded by the availability of generative artificial intelligence (AI), which promises to better synthesize the massive volume of altdata and extract valuable insights from it. According to Globe Newswire, the estimated value of the altdata market could reach approximately $156.23 billion by the year 2030.

The altdata collection industry ecosystem consists of organizations that are data sources (public facing and internal); data aggregators/brokers; service providers (including those specialized in data integration, enrichment and quality; data analytics/AI; and compliance); data marketplaces; and regulators. Different participants within that ecosystem interact with altdata in various ways. Almost all organizations generate altdata (whether unknowingly or deliberately), often as a byproduct of their operations. Entities might also consume altdata to develop business strategies and conduct research. Altdata is also commonly utilized for competitive intelligence and to gain competitive advantage. Other ecosystem participants, such as altdata service providers or brokers, specialize in the collection of altdata primarily for resale to organizations and consumers. Finally, other ecosystem participants are largely consumers of altdata, such as trading firms who seek to obtain insights, drive trading strategies and evaluate opportunities.

Our publication focuses on the first category of altdata ecosystem participants, primarily consisting of corporations that generate altdata. For them, altdata brings risks that should be identified and addressed, as discussed further below, consistent with ERM practices within their organizations. But careful assessment of altdata can also lead to important performance, competitive, financial, compliance and reporting improvements. As discussed below under Risk 3, altdata also represents potential new revenue streams: with proper guardrails, organizations should be able to monetize or otherwise leverage altdata by selling or licensing it.

Identifying and managing altdata risk using the COSO ERM Framework

The COSO Enterprise Risk Management (ERM) Framework is used by risk and other professionals to identify and mitigate a variety of organizational risks. COSO defines ERM as "The culture, capabilities, and practices, integrated with strategy-setting and its performance, that organizations rely on to manage risk in creating, preserving, and realizing value." Risk is defined as "the possibility that events will occur and affect the achievement of strategy and business objectives." Risks considered in this definition include those relating to business objectives.

Risks associated with altdata, including those identified below, linked to identification, compliance, valuation, or governance issues may constitute business risks. ERM is an ongoing, iterative process, and should be updated whenever there are significant changes to the environment and organization. Organizations should consider whether the proliferation of altdata constitutes a change meriting analysis of each of the ERM components as applied to an organization's data environment.

The COSO ERM framework comprises five interrelated components, each of which may be applied to altdata analysis as follows:

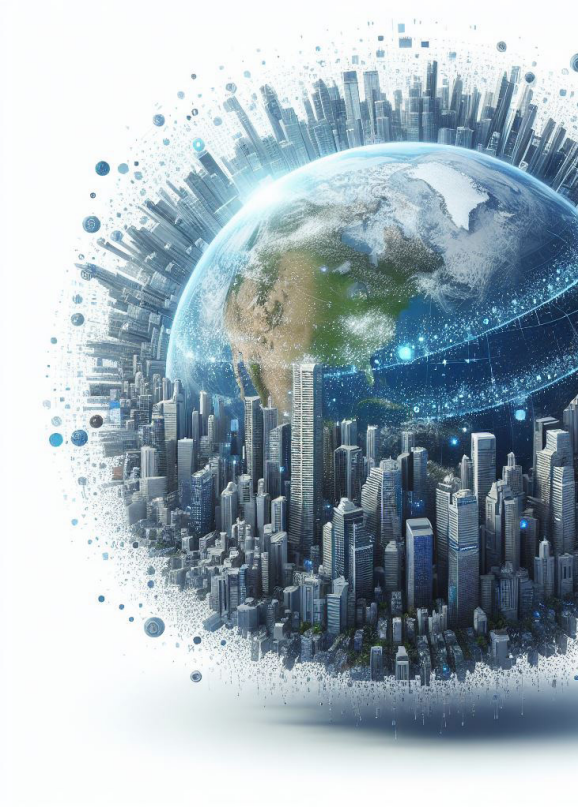
- **Governance and Culture**, which in part sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management, as well as understanding of risk in the entity. As discussed further below, organizations should assess how to align their governance structures to better assess altdata risks and opportunities.

- **Strategy and Objective-Setting**, which includes enterprise risk management, strategy, and objective-setting working together in the strategic-planning process. Organizations should determine how best to integrate altdata into the definition of their strategic objectives and operational or financial performance. Altdata may be used to enhance enterprise value as part of a monetization or licensing strategy, or identified as an asset to protect in order to conserve enterprise value. Effective risk management practices related to altdata can also safeguard future strategic decisions or transactions, such as mergers and acquisitions or dispositions.

- **Performance**, which includes identification and assessment of risks that may impact the achievement of strategy and business objectives, prioritization of those risks by severity in the context of risk appetite, selection of risk responses and portfolio view of the amount of risk it has assumed. As altdata is a fluid topic, organizations should determine what altdata risks they are exposed to in light of their strategic objectives, and how best to respond to those risks.

- **Review and Revision** by which an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed. As altdata sources and uses change and can be expected to do so over time, organizations must continually review their altdata profile and revise their approach.

- **Information, Communication, and Reporting**, or a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization. As discussed further below, organizations should pursue information reporting and gathering exercises to enhance their reactivity to altdata and develop proper reporting channels.



What risks does altdata pose to the organizations?

Risk 1 Inadvertent disclosures.

Organizations incur risk when they are not aware of the existence of altdata they produce and the story it can reveal about them. That failure could lead to the inadvertent disclosure of sensitive competitive information or strategy objectives, information that would otherwise constitute material non-public information (MNPI), intellectual property (IP), or even financial results or operational performance. Any time a company acts outside its organization or interacts with a third party, organizations should consider how this behavior could be used or perceived for alternative data analysis purposes, or how it could inadvertently reveal sensitive information.

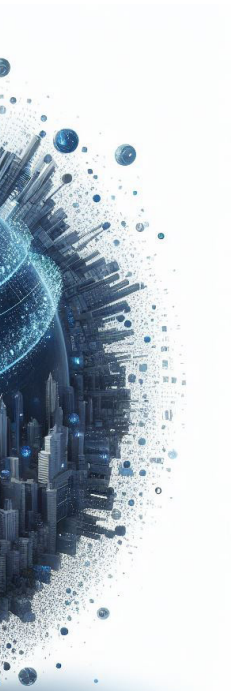
This inadvertent revelatory activity typically occurs when organizations fail to properly identify and assess information that may have been identified for public consumption, but not necessarily analysis. For example, company websites may well be destined for consumption by the public, but their analysis by sophisticated parties could reveal activity, resource deficiency or strategic focus. Sales and marketing may publish statistics or stories for thought leadership or branding purposes that can be used by alternative data providers to develop underlying performance insights. Posts of job opportunities could likewise grant insights into where and how a company is growing, anticipates growth or an area (geographical or technical skill level) where the institution is struggling with resource retention. Failure to assess this information as altdata at an enterprise risk level could be problematic as it could reveal performance data or business strategies that the organization does not ultimately intend for analysis (or as to which the company may not itself be aware). Every company is potentially an altdata generator if material amounts of data about the company are available to third parties; these organizations in turn incur the risk of inadvertent disclosure about a range of information about the organization. The use of AI solutions by employees that deliver base data to larger models may exacerbate this problem.

Because how alternative data is ultimately analyzed and processed by third parties is ultimately unknowable, the risk of inadvertent disclosure through failure to identify altdata is great. As the alternative data industry is evolves rapidly, organizations might deploy a “known-unknowns” framework in assessing alternative data.

Risk 2 Inaccurate reporting, and compliance failures.

Through a combination of board independence and committee rules and responsibilities, auditors who are regulated by the Public Company Accounting Oversight Board, and lawyers who are responsible in part to the SEC, the law endeavors to ensure that financial transactions and data of U.S. public companies are reported accurately. Similar, though less stringent, controls exist for private enterprises that may create audited financial statements for use by the organization and other stakeholders, including investors. To date, these initiatives appear to have been largely successful in avoiding widespread accounting fraud in the U.S. capital markets, both private and public. With these guardrails in place, the next great source of informational risk to organizations is likely to come from elsewhere.

Alternative data, if not assessed and managed properly through ERM practices, could very well be that source. Altdata represents a technological paradigm shift in the nature, volume, accessibility, connectability, and interpretability of information, and in particular forward-looking, predictive real-time information. Because of these characteristics, altdata has the potential to reveal differences between the knowledge that is imputed as a matter of law and custom to organizations, and the actual knowledge of that organization, which is effectively that of corporate managers, employees, and boards of directors and those they supervise. The proliferation of altdata suggests that the volume of data about an organization may now be larger than what current internal control and data analysis programs are designed to currently assess or have considered assessing. That characteristic represents an epistemological challenge to organizations, one that could be addressed by applying the principles embedded in the ERM Framework: governance structures and information, communication, and reporting processes may need to evolve to address altdata from a risk perspective.



Could this paradigm shift result in operational, compliance, or reporting issues corporate managers and boards of directors themselves have not identified? An example illustrates this potential concern, which lies beyond mere "skeletons in the closet" from vast stores of data. Imagine, for example, a company that sells products both in physical stores and over the Internet. The company routinely produces reports either for regulators or its stockholders regarding its results of operations, financial conditions, and prospects. These periodic reports are the results of internal financial controls and processes that are designed to capture past financial performance and translate those results into financial statements and disclosures that are guided by reporting rules. But investors operate based on future performance and prospects, not performance that may be indicative of past trends but not the future. If the company does not consider and analyze its altdata, it may not properly report the current trajectory of its web-based business. The company may not describe to its investors or regulators future risks or opportunities that may not be evident from past results, but which may be evident from available real-time altdata data points (or, as discussed above, may inadvertently disclose information).

As a result, altdata generated deliberately or inadvertently by an organization potentially presents compliance risks to that organization that go beyond the regulatory concerns currently associated with data as a class, such as privacy and intellectual property laws. Corporate sources should be mindful of failing to identify material trends or disclosure issues through lack of analysis of available altdata. In case of discrepancies or compliance deficiencies, failure to so assess could lead to regulatory action or private litigation.

Risk 3 Failure to realize value and opportunities.

Organizations also can fail to identify value from potentially significant altdata, which impedes the organization's goal of maximizing shareholder value. This failure can occur in two ways. First, an organization that generates altdata may also acquire third party altdata generated by external sources for competitive analysis or performance benchmarking. If the organization misanalyzes that external altdata or does not conduct proper diligence on the source of that data, it could at a minimum fail to realize the intended value of such data, or worse expose itself to regulatory action or litigation. Second, organizations that generate data can fail to properly value, or valuate, the altdata they themselves have generated. This failure of valuation can stem from two principal causes: first, a failure to identify valuable altdata as an exploitable asset; and second, a failure to safely create value from the sale or other exploitation of those assets.

Even if an organization properly identifies altdata for sale or license and prices that transaction correctly, it should not do so without appropriate reporting and compliance analysis, and governance safeguards in place. When analyzing how to deploy altdata strategically, either for purposes of internal analysis or in the context of an external transaction, organizations should consider how to apply the ERM at least at the Strategy and Objective Setting and Performance levels.

Failure to implement the principles embedded in the ERM Framework could have consequences. Should an organization fail to conduct proper monetization procedures on its altdata assets, it is exposed to threat from third parties, who can potentially assess the organization's prospects and value better than the organization itself and use those information asymmetries to their advantage. Similarly, the failure to conduct proper governance and legal analysis could expose the organization to regulatory or litigation challenges.

What specific risk assessment and management steps should organizations consider?

1 Assess and enhance data controls and procedures to help identify and analyze altdata.

Companies should consider designing and implementing policies to facilitate the identification and analysis of alternative data, as well as assess and reinforce protective measures with respect to altdata. Leveraging the principles embedded in the ERM Framework can be useful to this task: organizations should evaluate their governance structures and information, communication, and reporting edifices to the task of altdata analysis. By assessing the impact and likelihood to their organizations specifically, organizations can better develop effective mitigating action plans to combat the short term or long-term effect of altdata risk.

Effective internal control systems have a proven record in minimizing organizational risk. Similarly, data controls and procedures should enable a company to understand what information regarding it is publicly available, and how that information could be leveraged by others. Protective measures for such information may include policies, procedures, software, and legal protections for unintended use cases, such as AI-focused policies and procedures, firewalls, and terms-and-conditions.

As part of their overall effort to exercise good data hygiene, organizations should be careful when selling or giving their own information to data aggregators who routinely pay and solicit companies for data. Organizations should conduct diligence on such parties to assess the policies and procedures apply to data and their record of legal compliance.

2 Leverage analytic tools to achieve consistency between alternative data and regulatory reports.

By analyzing altdata, or employing AI native processes such as natural language processing, organizations should strive to identify differences between publicly reported data, including financial or regulatory reports, and other data that is disclosed intentionally or unintentionally. Divergences between the two may yield useful trading advantages when they reveal past performance or future trends that are otherwise undisclosed.

Reporting organizations should strive to diminish variability between the result or potential result of analyzing alternative data and external reports. For example, organizations could expose themselves to liability should financial statements suggest that internet sales have risen from quarter to quarter, yet detailed analysis of web traffic suggests otherwise.

The insights altdata offers should prompt companies to assess what their own generated altdata can tell them about their operational posture, reporting strength, and compliance status. Since altdata is growing significantly, its insights and impact on corporate compliance and risk will be likely difficult to ignore for most data-centric companies.

3 Adapt governance structures.

Failure to adapt governance and risk management processes to the proliferation of altdata represents a fundamental risk to altdata generative organizations. As altdata practices evolve, it will become important that activities spanning risk, compliance, control, and governance be coordinated to aid in the assessment of altdata. If an organization's governance infrastructure fails to identify and assess the legal, ethical, competitive, and financial impacts of collecting and using altdata emanating from other entities, it could face governance and leadership reprimand. Adapting governance structures serves as a key method of adapting an organization's ERM to the risks posed by altdata.

What is the proper role of an organization's board with respect to alternative data in light of these trends? Generally, boards should understand the range of alternative data available regarding the organization it oversees and its public use. As financial statements are reviewed and approved by boards of directors (or audit committees in the US public company context), boards (or data and risk committees) could work with disclosure committees or other compliance and reporting structures to review public information and consider how that output relates to other available altdata. Similarly, boards could also defensively monitor controls and protection guidelines for altdata and monitor and address disinformation initiatives or other malicious behavior. Boards should avail themselves of the resources needed to complete their duty, including outside advisers, and should exercise their discretion to advise management to devote additional resources to alternative data issues.

Governance enhancement could also include better internal education on the topic of altdata. Creation of and monitoring an organization-wide strategy to identify, manage, document, and address altdata risks is recommended, as well as recruiting key technical experts and advisors that can advise the board on risks and opportunities. Regularly conducted altdata risk and value assessments may be useful, including upstream reporting, as well as identification of areas of possible future risks, including metrics to evaluate how well the organization is addressing those issues. Boards could also be charged with evaluating the ethical and legal considerations relating to the organization's own consumption of altdata.

Companies have considerable discretion in crafting policies and procedures that suit their structure and risk profile. They should consider adopting a principles-based approach to altdata rather than formal rules, since altdata, definitionally, changes in scope and nature, and can be expected to continue to do so in the future. In the near future, the practice of data governance will likely migrate from static policies, compliance reviews, security and retention to more active and evolutive data asset management: data hygiene management, audits, data use analysis, AI reviews, valuation, policies, compliance, security, and retention.

While certain boards may, after review, conclude that altdata does not represent a significant risk or opportunity to their particular organization, it should still exercise strategic oversight of altdata matters, including, as applicable:

- Identifying whether the full board, a committee and/or specific directors are responsible for oversight.
- How the board is informed of altdata issues related to disclosure or financial reporting.
- How frequently the board discusses altdata issues.
- Whether and how the board considers altdata as part of the company's business strategy, risk management, operations and financial oversight.
- Staying current on regulatory developments, best practices and industry trends.
- Understanding the company's measures to assess, develop and defend altdata.
- Documenting the committee's/board's review of policies and its role in oversight.
- Appraisal of, and subsequent assessments of, risks.
- Challenging management and seeking advice from external advisers, including auditors, lawyers and altdata consultants.

Management's role in managing and monetizing altdata and implementing appropriate policies and procedures might include identifying and documenting the following:

- Which management positions or committees are responsible for managing altdata risk, and what is the relevant expertise of those individuals?
- Who at the company is best suited to address risk and opportunity, what is the relevant expertise of the individual and to whom do they report at the company?
- What is the process by which management is informed of and monitors the company's altdata?
- Does management report to the board of directors on these issues? If so, how frequently?
- Who are the stakeholders at the company responsible for managing risk and data policies and procedures?
- How does management report to the board, in terms of content and characterization?

Coordination will also be required between key internal stakeholders such as IT departments, engineers/data input leads, customer experience, marketing, analytics and data use teams, and legal and regulatory compliance with external stakeholders such as third-party data sources, data aggregators, data consultants and vendors, and data purchasers and users.

Conclusion

As altdata grows in volume, velocity, and complexity, as well as accessibility, organizations should assess the impact of this ecosystem on their operations, reporting, compliance, and risk systems. Since the growth of altdata presents both opportunities and risks, the data infrastructure and related governance of many institutions may be required to adapt to a complex and evolving environment. The COSO ERM Framework is well-suited for application to the issues presented by altdata for organizations, and provides much-needed structure for identification and analysis of altdata within organizations.

Footnotes

1. A-Guide-to-Alternative-Data_jan2021..pdf (fisd.net)

2. The arrival of altdata should not be viewed in isolation. Certain technologies, terms, and concepts that are directly correlated with increased availability and utility of altdata include the following:

   - Big Data/Open Data: Big data refers to the wide variety of data coming from sources such as IoT, social media, and other data sources too large or complex to be processed by traditional applications. In a sense, altdata is a manifestation of big data. Open data is in turn a subset of big data: large, usually structured, data sets, usually made available by governments. Big data, IoT, and AI may all be used together in the future and, working in conjunction with internal control processes, could become a powerful toolset to enhance an organization's operations, reporting, and compliance profile.

   - Artificial intelligence (AI): AI is an area of computer science where intelligent machines work and react like people (albeit people with infinite memories, who never tire, and are constantly improving) for tasks like decision-making, problem-solving, emulating senses, learning, planning, and activities like visual perception and speech recognition. AI has experienced a renaissance recently due to the advent of widely available generative AI technologies, such as ChatGPT. At core, AI is particularly useful at identifying patterns, outliers and non-obvious correlations. AI can be used to augment human involvement or serve as its replacement. For instance, AI can be used to analyze real-time trade transactional data and other information to simulate human judgment in classification, recording, analytics, and decision-making. Generative AI can also be used to create new data, techniques or code, some of which could potentially be used by entities as part of their altdata profile.

   - Internet of Things (IoT): Internet of Things is a broad term for the growing list of things that can link to the Internet. With home automation devices, just about anything that can turn on and off can be Internet-enabled and be part of a network of things that can monitor, report about, and act upon the environment around it. The promise of data monetization and the drive to obtain data-based insights is readily apparent in the auto industry now that practically every new car rolling off the lot is connected to the Internet. IoT devices can potentially write to or act upon information to enhance an altdata profile.
     See "Blockchain and Internal Control: The COSO Perspective."

3. globenewswire.com/news-release/2023/08/30/2734059/0/en/Alternative-Data-Market-worth-156-23-Billion-by-2030.

4. cmr.berkeley.edu/2022/11/harnessing-alternative-data-for-competitive-advantage.

5. public.axsmarine.com/blog/the-rise-of-alternative-data-unveiling-hedge-funds-secret-weapon.

6. The components, principles, and points of focus of COSO's Internal Control-Integrated Framework (ICIF) may provide a method of addressing altdata activities and information in response to the risks identified and addressed by the ERM. As defined by COSO, *"Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."*
   The COSO Internal Control Integrated Framework (ICIF) outlines the principles and points of focus for effective internal control programs.

About the authors

Ryan Blair focuses his practice on securities, corporate governance and shareholder litigation, including the defense of securities class actions, derivative suits and M&A litigation. He also represents companies, boards and special committees in connection with Securities and Exchange Commission investigations and civil enforcement actions, as well as internal corporate investigations. Ryan has worked with clients in the hardware, software, semiconductor, biotechnology, pharmaceutical, internet and digital media industries. His practice also includes complex commercial litigation. Ryan received his BA from Stanford University and his JD from University of California at Los Angeles School of Law.

Nicolas Dumont is a member of Cooley LLP's public companies, capital markets and artificial intelligence groups, as well as a leader of the firm's alternative data group. He has represented clients in North America, Asia and Europe. His transactional practice centers on advising corporate and investment banking clients in public and private corporate finance transactions, with experience in initial public offerings (IPOs), special purpose acquisition companies (SPACs), common and preferred stock issuances, private investment in public equity (PIPE) offerings, and other types of offerings. He has advised in a wide array of industries, including tech, life sciences, crypto, banking, shipping, natural resources and insurance. Nicolas' alt data work lies at the intersection of capital markets regulation and evolving machine learning and artificial intelligence technologies and techniques. In close collaboration with Cooley's cyber/data/privacy and litigation practices, his current focus is on data monetization and controls, public company reporting, and related governance and corporate systemic risk topics. Nicolas received an AB from Princeton University (*summa cum laude*), a JD from Stanford Law School and a *diplôme* from Sciences-Po (Paris).

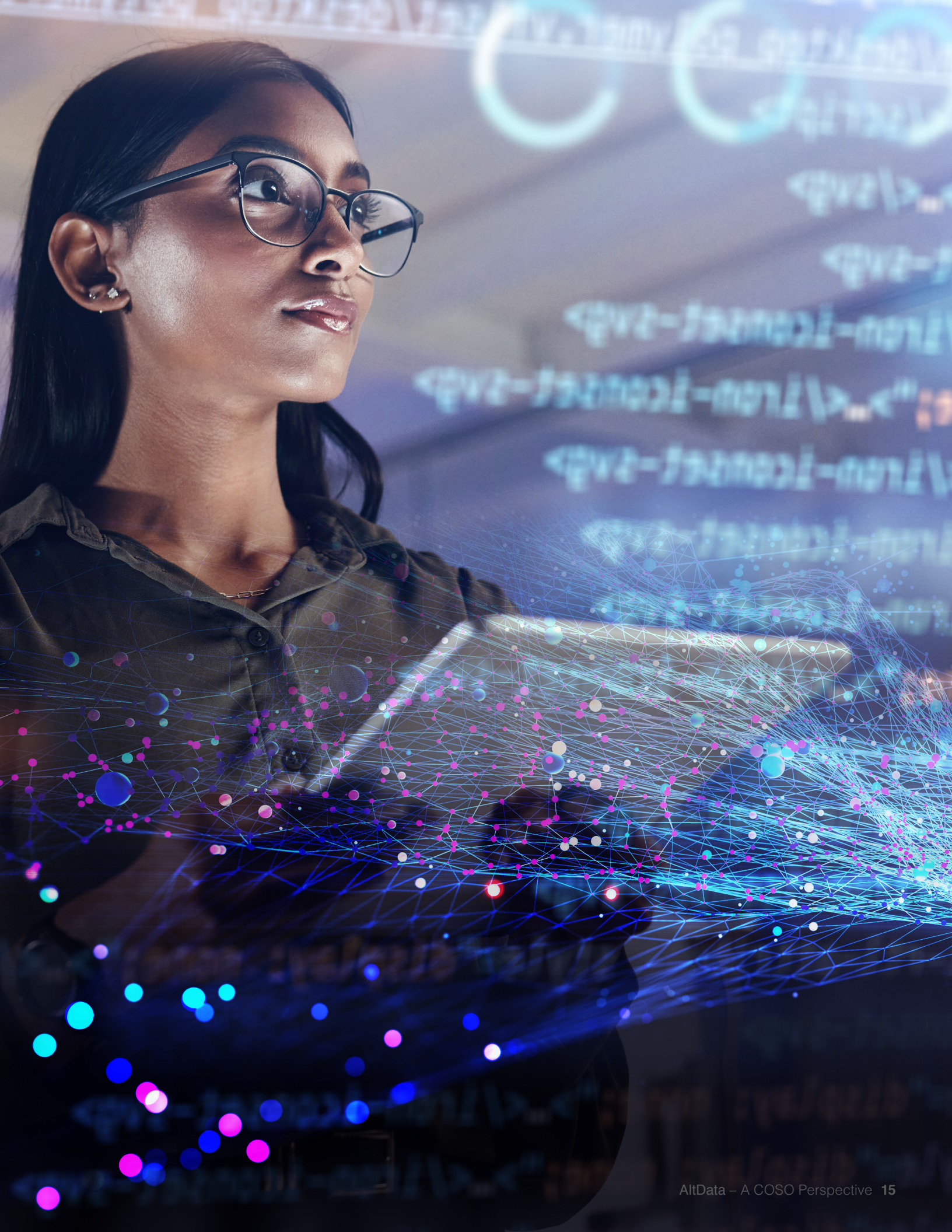
Michael Egan has focused on cyber/data/privacy issues in the areas of technology, innovation, retail and consumer solutions, life sciences, manufacturing, financial services, and healthcare since 2007. He advises clients on all legal aspects of global data protection, data privacy, data security, data breaches, information technology, and related restrictions on data collection, use, and transfer. He has represented companies before numerous government agencies and bodies, including the US Federal Trade Commission, the US Department of Justice, and the US Securities and Exchange Commission, as well as data protection authorities around the world. Michael received his BA from Georgetown (*cum laude*) and his JD from Boston College.

David Navetta is a prominent leader in privacy, information security and technology law. He has extensive experience counseling clients on novel and cutting-edge data protection issues, including data breach response, cybersecurity risk management, consumer and employee privacy, incident response planning and preparedness, technology transactions, vendor management, board of director advice and consultation, regulatory investigations, litigation and due diligence in corporate transactions. David serves as a "breach coach" on an approved panel for numerous cyber insurance carriers and companies, and he has helped some of the world's leading corporations to effectively respond to complex data security breaches and protect their enterprise. David's clients range from startups to large *Fortune 500* multinationals across a range of industries, including ecommerce, consumer products, name-brand traditional brick-and-mortar, hotels and hospitality, social media, technology, professional services, healthcare, financial institutions and energy. David received his BA from Michigan State University and his JD from DePaul University College of Law.

Each of Ryan, Nicolas, Michael and David are founders of Cooley's Alternative Data, Monetization and Governance practice group.

About COSO

Originally formed in 1985, COSO is a joint initiative of five private sector organizations and is dedicated to helping organizations improve performance by developing thought leadership that enhances internal control, risk management, governance, and fraud deterrence. COSO's supporting organizations are the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), the Institute of Management Accountants (IMA), and The Institute of Internal Auditors (IIA).



ALTDATA

THE COSO PERSPECTIVE

COSO

Committee of Sponsoring Organizations
of the Treadway Commission

coso.org