2020 investment management regulatory outlook
Contents

Global foreword 4
Introduction 7
Regulation Best Interest (Reg BI) 8
SEC hot topics and looking ahead to 2020 10
Cybersecurity 12
Proactive risk identification and mitigation through improved analytics and compliance monitoring 14
Enterprise risk management: Integrating risk management drives strategic growth 16
Staying ahead 18
Leadership 19
This publication is part of the Deloitte Center for Regulatory Strategy, Americas’ cross-industry series on the year’s top regulatory trends. This annual series provides a forward look at some of the regulatory issues we anticipate will have a significant impact on the market and our clients’ businesses in 2020. The issues outlined in each of the reports provide a starting point for an important dialogue about future regulatory challenges and opportunities to help executives stay ahead of evolving requirements and trends. For 2020, we provide our regulatory perspectives on the following industries and sectors: banking; capital markets; insurance; investment management; energy, resources, & industrials; life sciences; and health care. For a view of the other trends that affect investment management in 2020, we encourage you to read the Deloitte Center for Financial Services companion paper.

We hope you find this document to be helpful as you plan for 2020 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at CenterRegulatoryStrategyAmericas@deloitte.com.
Global foreword

After a decade of global regulatory reforms defined by the financial crisis and misconduct issues, the regulatory environment is now changing profoundly. The international consensus on regulatory reform is fraying. Political appetite for globalisation is retreating, and trade tensions are mounting. Technological change and social concerns, including environmental sustainability, are rising on regulators’ agendas. Financial services firms need to be prepared to respond to these trends.

Economic outlook

We may see weak growth in a number of regions in 2020, with significant downside risks. Regulators’ and supervisors’ work programmes are likely to be heavily influenced by their assessment of the economic conditions under which firms will be operating. Increased trade tensions, especially between the United States and China, are likely to fragment markets further, dampen growth and create a harsher business environment for financial services firms.

In the United States, the yield curve on Treasury bonds was inverted until recently, which has in the past been a harbinger of recession. Equity valuations are high, in large part, due to monetary easing: The US equity market is more overvalued on some measures than at any point since the dotcom bubble.

Meanwhile in China, growth has continued to slow and gross debt surged from 171 percent of Gross Domestic Product in 2008 to 299 percent in 2018. High debt levels could become unsustainable if growth slows further.

In our view, the risk of a recession is highest in Europe. Growth in Germany is expected to be as low as 0.5 percent in 2019, partly due to its manufacturing sector’s vulnerability to poor export markets, although some recovery is expected in 2020. Italy is facing political uncertainty, economic stagnation and resurging financial turbulence, while servicing high public debt. And the UK faces an uncertain outlook, in part due to Brexit. Therefore, while growth for the Eurozone in 2020 is projected at 1.4 percent, which is similar to its postcrisis trend rate, significant downside risks remain.

Central bankers are likely to respond with further monetary easing, with the US Federal Reserve Board and the European Central Bank having already cut rates further and renewed their asset purchase programmes. However, with interest rates at an unprecedented low, and with a record amount of sovereign and even corporate bonds trading at negative nominal rates, the effectiveness of such measures in isolation is debatable. Authorities may consider using macroprudential measures, such as allowing banks to run down countercyclical buffers. Governments are also likely to face pressure to increase spending to stimulate growth, especially given the backlog of infrastructure spending in some countries.

These macroeconomic trends and conditions will put even more pressure on financial services firms’ business models, at a time when competition from new entrants and major digital players is also increasing. We expect supervisors to have a heightened focus on business model resilience, through stress testing, and on the quality of risk governance and oversight.

Banks may struggle to regain profitability, and even to maintain margins, through their traditional business model in a low, or negative, interest rate environment. For example, Japan has had a zero or negative interest rate policy for nearly two decades. Japanese banks have struggled with low interest margins and face increasing supervisory scrutiny on business model sustainability. A reduction in cross-border financial flows as risk appetites reduce may also narrow banks’ growth opportunities. Banks will need to redouble their efforts to control costs and refocus on more profitable business lines. However, they will need to be mindful of conduct risk. Supervisory focus on credit risk is also likely to intensify. For example, the Bank of England estimates that global banks retain exposures to over half of the leveraged loan market, and that the global stock of leveraged loans has reached an all-time high.

Insurers, particularly those providing long-term guarantees, are also likely to find it harder to be profitable in a persistently low interest rate environment. In Asia, however, the potential for the insurance market to grow in China may help insurers to generate more offsetting revenue.

Investment managers too will likely struggle to perform well in an environment characterised by high asset prices and low growth potential. The increasing scrutiny by investors and regulators of the value generated by active management is likely to drive a continued
“search for yield” and encourage investment in more exotic and less liquid markets. We expect supervisors to focus increasingly on how investment managers and distributors satisfy themselves that funds holding higher risk assets meet the needs and risk appetite of their target market.

The fraying international consensus
With the postcrisis reforms near completion and the political environment becoming less supportive of international cooperation, global standard-setting bodies—particularly the Basel Committee on Banking Supervision and the Financial Stability Board—have less ambitious plans to introduce new standards than in previous years. Work to implement the remaining aspects of the G20 financial regulatory reforms has slowed, with many jurisdictions behind in implementing Basel III (“Basel IV” to industry).10

Given the current economic conditions, political concerns will grow if regulation is seen to impede competition, new lending or investment. We are already seeing a deregulatory stance from the US authorities, including a limited relaxation of the Volcker Rule.11 Other countries may follow, and we might even see competitive deregulation. While deregulation might reduce some compliance costs, global firms will face more complexities and expenditure as regulatory standards across jurisdictions diverge in timing and substance. The G20 highlighted market fragmentation was an area of concern in 2019, and the Financial Stability Board has an ongoing work programme in this area.12 It is unlikely that global standard-setters will be able to reverse fragmentation that has already happened, but their efforts could reduce future divergence.

More accountability for senior individuals
In contrast, regulators are increasingly holding senior individuals to account for the compliance, professional standards and culture of their firms. Following the introduction of the UK’s Senior Managers and Certification Regime, similar regimes have emerged, or are emerging, in several other jurisdictions, including Ireland, Australia, Hong Kong Special Administrative Region, Singapore and South Africa. Other jurisdictions are driving increased accountability through different mechanisms. The US Federal Reserve Board has proposed guidance which seeks to delineate the roles, responsibilities and accountabilities of senior management and the board better.13 The Belgian Parliament recently announced the introduction of a “Banker’s Oath” similar to that which the Netherlands introduced in 2015.14 In response to these initiatives, firms will need to foster a culture of accountability through measures such as balanced incentive plans; strong governance and controls; and appropriate monitoring, reporting, escalation and disciplinary action.

Regulating technological innovation
Policymakers and regulators will continue to be challenged by the need to respond to the pace and scale of technological change. The financial services regulatory debate will be characterised by issues such as whether to expand the regulatory perimeter, risks associated with increasing use of artificial intelligence, the impact of innovation on operational resilience and cybersecurity, and digital ethics. These are global issues, but a lack of political will and adequate international bodies in some policy domains will likely hinder efforts to align regulatory approaches.

Cross-sector policies will increasingly affect financial services firms, although these will differ across regions. For example, in relation to data protection, the EU is taking a stricter stance on individuals’ right to access and control personal data than the US and China.15 Globally, the emergence of tighter data localisation requirements will introduce additional obstacles to cross-border data flows.

The growing evidence that ineffective implementation of technological change can increase cyber and operational risk is also attracting regulatory scrutiny. International standard-setters will likely try to establish baseline common approaches for operational resilience, but we expect progress on cyber-resilience to be made mostly at the G7 and European levels.

These trends will affect firms’ ability to use and share data to innovate, enhance their cross-border resilience, and deliver value and security to their clients.

Regulators and supervisors will also need to accelerate their own digital transformation. Well-resourced regulatory data science and analytics capabilities will be essential to understand and supervise a financial sector characterised by an increasingly blurred regulatory perimeter and greater technological complexity. Part of the solution may be for financial, security and data protection authorities to share resources, capabilities and insights more effectively. We see efforts in this direction, but more work is needed before regulators and firms can reap the benefits. Progress will more likely be achieved at national than at international level, mainly because of the absence of cross-sectoral global standard-setting bodies.
Responding to social concerns

Environmental sustainability is a rising social concern, and in Europe and Asia, a major focus for financial services regulators. In the US, it is not—at least not at federal level. However, even where regulators do not introduce specific requirements, firms will need to consider how climate change and unsustainable business models will affect their asset and liability exposures, as well as the new opportunities that may arise from the increasing customer demand for “green” products, including green investment funds.

Financial inclusion is another area of focus globally. The World Bank Group estimates that in 2017 there were still 1.7 billion adults without a basic transaction account, primarily in Asia and Africa. It has a goal for all adults to have access to an account to store money and make payments by 2020. In developed countries, regulators are focused on barriers to financial inclusion such as overly complex processes and lack of accessibility for “nonstandard” customers, including the elderly or people with disabilities. Firms should expect to be challenged by regulators if their services are unduly hard for certain groups to access.

Conclusion

Although the postcrisis wave of regulatory change is subsiding, there is much to attract regulatory and supervisory attention in 2020, and firms should not expect scrutiny to abate. Against a darkening economic background, there will be increased focus on firms’ financial and operational resilience, how they adapt to technological change and innovation, and how they respond to political and social pressures in areas such as sustainability and financial inclusion. In an environment where boards and individual senior managers are increasingly being held to account for their actions, financial services firms will need to ensure they have the foresight, governance, skills and operational capabilities to adapt and respond effectively.
Introduction

With the increasing prevalence and effectiveness of technology around the globe, the status quo is no longer an option. To keep up with the pace of change, investment management companies should continue evolving their approach to keep up with the myriad of challenges that they are facing, and more importantly, the opportunities that they can take advantage of in this fourth industrial revolution. Regulatory, legal, and compliance functions are being asked to do more with less while grappling with new and emerging challenges that stem from the near-ubiquitous use of advanced technologies to meet the increasing cost pressures and need to deliver value beyond “check-the-box” exercises.

In this digital world, new threats are emerging along with new laws and regulations to help protect consumers and the markets. Regulators, both domestic and foreign, are focused on data privacy protections to mitigate the risks that result from improper collection, handling, storage, and use of data. Cyber threats continue to become more sophisticated and more damaging, putting even more urgency around developing protections from bad actors, both external and internal.

Against this backdrop, investment management companies should continue to modernize and rationalize their regulatory, legal, and compliance functions and their practices. Investment management companies that take a holistic view of regulatory risk management may find efficiencies that lead to streamlined and rationalized programs. A modernized compliance function can help investment management companies achieve compliance as efficiently and effectively as possible by “thinking forward” and then harnessing the best available compliance practices and technologies to comply with current and future regulatory requirements. Some companies are even looking at their regulatory and compliance risk management programs as a competitive differentiator that allows them to be more nimble in the market place.

Regardless of how the changes promulgated by lawmakers and regulators affect investment management companies, it is imperative that they continue to modernize and rationalize their regulatory, legal, and compliance risk management programs so that they can meet applicable laws, regulations, and oversight and monitoring expectations in a sustainable, efficient, and cost-effective way.
Regulation Best Interest (Reg BI)

On June 5, 2019, the US Securities and Exchange Commission (SEC) adopted new regulations governing the conduct of broker-dealers and their associated persons, particularly regarding the manner in which they provide securities or other recommendations to retail customers. Reg BI imposes principles-based standards on broker-dealers and requires a broker-dealer to act in its retail customer’s best interest when making such recommendations. To meet this “best interest” standard, broker-dealers must, among other things, satisfy a number of requirements and specific obligations related to disclosure, standard of care, conflicts of interest, and compliance.

Reg BI aims to provide retail customers with full and fair disclosure about the products and services offered by broker-dealers so those customers can make informed investment decisions pertinent to their needs and investment goals while understanding the associated risks. As part of the SEC’s rule-making package, firms are required to file with the SEC and deliver to customers a Customer Relationship Summary Form (Form CRS). In no more than two pages, a broker-dealer or investment adviser is required to disclose information to its customers about the firm’s business practices, including its registration status; its relationship and services to the customer; the fees, costs, conflicts of interests, and standards of conduct related to those services; and the firm’s disciplinary history. The compliance date for both Reg BI and Form CRS is June 30, 2020.

In addition to the general obligation, Reg BI has four component obligations:

- **Disclosure obligation**: The disclosure obligation requires a broker-dealer to provide to retail customers, prior to or at the time of the recommendation, in writing, full and fair disclosure of all material facts related to the scope and terms of the relationship and all material facts relating to conflicts of interest that are associated with the recommendation.

- **Care obligation**: The care obligation requires a broker-dealer to, among other things, exercise reasonable diligence, care, and skill to understand the potential risks, rewards, and costs associated with the recommendation and have a reasonable basis to believe that the recommendation or series of recommendations is in the best interest of the customer.

- **Conflict of interest obligation**: The conflict of interest obligation requires a broker-dealer to identify and manage conflicts of interest, whether through mitigation or elimination and, at a minimum, disclosure. This obligation also requires written policies and procedures reasonably designed and enforced to identify and manage such conflicts.

- **Compliance obligation**: The compliance obligation requires a broker-dealer to establish, maintain, and enforce written policies and procedures reasonably designed to achieve compliance with Reg BI. This obligation is designed to ensure that broker-dealers have controls, testing, training, and periodic review in place to prevent Reg BI violations.
Key preparation activities

**Evaluate current-state gaps.** Firms should prepare for changes driven both by Reg BI and by various state fiduciary rules (e.g., NY DFS 187). When evaluating gaps in the current state, it is important to take a broad view that considers the potential impacts to people, processes, technology, and strategy.

**Assess “solely incidental” practices.** Firms should evaluate their business practices, particularly with regard to discretionary trading and account monitoring, to ensure the practices align with the SEC’s expectations for what constitutes an advisory activity. In its interpretative guidance release, the SEC clarifies that a broker-dealer exercising unlimited investment discretion over a retail customer’s account would be deemed advisory in nature and thus bound by a fiduciary duty of care.

**Identify and manage conflicts of interest.** Reg BI requires firms to identify and manage conflicts of interest related to their business practices. To that end, firms should consider developing formalized procedures for identifying, documenting, disclosing, and managing conflicts of interest.

**Evaluate sales practices and compensation programs.** Under Reg BI, certain types of sales contests and sales quotas are explicitly prohibited, as they create conflicts for broker-dealers and their associated persons to act in the best interest of their retail customers. As such, firms should evaluate their sales practice and compensation programs to ensure they meet standard-of-care obligations.

**Evaluate potential customer and financial adviser life cycle impacts.** As required by various obligations, including Form CRS delivery requirements, firms should holistically evaluate the life cycle needs of their customers and their representatives to determine the potential impacts and associated costs that may result from complying with the new requirements.

**Consider multiple federal, state, and individual requirements.** With various states and some professional organizations (e.g., the Certified Financial Planner Board) adopting (or considering) their own rules to govern the standard of conduct for broker-dealers and their associated persons, firms should evaluate their overall readiness efforts and the collective impact of potentially overlapping, duplicative, or divergent requirements. These evaluations can help to ensure a firm is efficiently and effectively meeting all of its regulatory requirements.

**Prepare for workforce readiness.** As with any major change initiative, successful implementation and workforce adoption will require an effective strategy for communication, training, and change management. Firms should carefully consider the impacts on employee retention and overall company engagement.

2. For dual registrants that include their brokerage services and investment advisory services in one relationship summary, it must not exceed four pages.
3. SEC, Regulation Best Interest: The Broker-Dealer Standard of Conduct

Let’s talk

**Maria Gattuso**
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
mgattuso@deloitte.com

**Bruce Treff**
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
btreff@deloitte.com

**Craig Friedman**
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
crfriedman@deloitte.com

**Josh Uhl**
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
juhl@deloitte.com
SEC hot topics and looking ahead to 2020

Regulatory hot buttons kept investment management firms busy throughout 2019 and will likely continue to do so in 2020. The SEC, through the Office of Compliance Inspections and Examinations (OCIE), issued its annual Examination Priorities for 2019, along with five Risk Alerts for consideration and action over the course of the year. The annual Examination Priorities publication highlights many “perennial risk areas” and serves as a useful guide for newer investment management firms, as well as those that have never been examined by the commission.

As expected, OCIE continued to focus on investor protections. This included privacy and Reg S-P, in which OCIE cited numerous firms for failing to provide initial, annual, and/or opt-out privacy notices to their customers. Data security and integrity surrounding customer records and information was another focus area. Findings related to data security included misconfigured network storage solutions, which often resulted from lack of effective oversight on initial solution implementation. Inadequate oversight of vendor-provided network storage solutions was also on the radar. Later in the year, OCIE focused on compliance programs and supervisory oversight of previously disciplined persons. Then in the fall, OCIE reminded firms engaged in principal and agency cross trading to be mindful of their policies and procedures, with a particular emphasis on providing sufficient disclosures to clients involved in such transactions.

In addition to the focus areas prioritized by OCIE through its formal Risk Alerts, many firms found themselves dealing with the SEC in targeted sweep examinations focused on mutual fund share class selection and the associated revenue sharing for certain mutual fund share classes. Meanwhile, the commission continued to focus on core compliance initiatives and requirements. Although the SEC has publicly subscribed to a more data-driven approach to reviewing firms over the past few years, we have seen recurring themes of enforcement related to lax policies and procedures and compliance testing that merely scratches the surface of a firm’s compliance program. The commission also renewed its focus on firms that employ previously disciplined persons (and the supervision and oversight of those persons). In addition, the industry continued to see enforcement actions against private equity firms for failing to properly allocate certain expenses across funds and co-investors and for failing to properly offset management fees in connection with undisclosed fee-sharing agreements with certain co-investors.

Although SEC staffing levels have decreased under the current administration, the commission still managed to increase the total number of cases it brought against firms. OCIE continued its focus on Main Street investors in 2019, and we expect it will follow suit in 2020 with continued pressure on firms that have a direct retail presence, as well as those that manufacture products used by retail buyers. Meanwhile, institutional firms—including those operating in the private equity and hedge fund spaces—will likely see continued pressure around their overall compliance programs. We also expect a continued focus on the topic of third-party risk management (e.g., “know your vendor”) and the integration/safeguarding of client data at those third parties.

We’ve all heard the phrase “a rising tide lifts all boats”; but when the tide recedes, in many cases, only boats that are appropriately prepared will continue to float. The same holds true for investment management firms. Firms that focus on core compliance issues, such as investor protections and a robust compliance program,
will likely find themselves better prepared to deal with inevitable market gyrations and regulatory uncertainties. This is especially true in an industry like investment management, where outsourcing and the use of third-party service providers is at the top of the C-suite agenda. With margin compression forcing firms to reevaluate their business models, they are increasingly turning to technology as a way to contain costs and maintain productivity. And as their reliance on third-party technology solutions grows, they will need to either train existing staff to understand and oversee those solutions or bring in additional resources with the subject-matter expertise to handle this oversight function.

Investment management firms that have not been visited by OCIE recently—or that fall into the category of “never examined”—should consider refining and refocusing their compliance program oversight. This includes conducting a policy and procedure review, followed by relevant testing focused on mitigating any deviations from firm policy, and then strengthening the control environment as needed. OCIE has made it clear that firms need to document their policies and procedures as thoroughly as possible, and then act in accordance with those policies. Firms should also revisit their policies and procedures related to third-party risk management and associated due diligence. A leading practice in the industry is to focus more holistically and thematically on risk at an enterprise level, and then distill and map the risks across the organization and operating areas, eventually tying the risks to the firm’s policies and procedures. A more holistic view of risk management may help investment management firms better respond and adapt to changes in market conditions and the regulatory environment.

Let’s talk

Maria Gattuso  
Principal  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
mgattuso@deloitte.com

Bruce Treff  
Managing Director  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
btreff@deloitte.com

Craig Friedman  
Senior Manager  
Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
cfriedman@deloitte.com

Cybersecurity

Investment management companies are focusing more resources and attention than ever on cybersecurity. However, cybersecurity issues continue to grow, fueled by determined, well-funded, sophisticated adversaries—and by a world that is increasingly interconnected and digital.

According to a recent industry survey conducted by Deloitte (in collaboration with FS-ISAC), financial services institutions on average spend 10.1 percent of their IT budget on cybersecurity. Yet the number of data breaches in the first six months of 2019 increased by 54 percent over the same period in 2018.

From a regulatory perspective, cybersecurity continues to be a key focus area, both in the United States and around the world. Issues coming under increased scrutiny and supervision from regulators include cybersecurity governance (board/leadership involvement), privacy/data security, cyber resilience, and outsourcing risks.

In response to these rising risks and regulatory expectations, investment management companies across the globe are continuing to strengthen their technology, risk, and compliance programs.

**Regulatory activity related to cybersecurity**

**OCC.** The Office of the Comptroller of the Currency (OCC) identified cybersecurity and operational resiliency as a priority in its 2020 bank supervision programs, with particular emphasis on threat vulnerability and detection, access controls and data management, and managing third-party connections. Examiner focus areas will include IT risk management and IT systems maintenance.

**Federal Reserve.** Cyber-related risks are a supervisory priority for the Federal Reserve for Large Institution Supervision Coordinating Committee (LISCC) firms, large and foreign banking organizations (LBFOs), and community banking organizations (CBOs).

**FDIC.** Enhancing oversight of banks’ cybersecurity risks is a top challenge for the FDIC. As part of its Community Banking Initiative, the FDIC is adding to its cybersecurity awareness resources for financial institutions. This includes adding two new Cyber Challenge vignettes focused on cybersecurity and operational resilience.

**US state regulations.** More than 30 states enacted cybersecurity-related legislation in 2019. California’s Consumer Privacy Act (CCPA) has prompted new calls for comprehensive data privacy and security laws across the nation. Other states, such as New York and Nevada, are introducing similar privacy bills.

**European Union.** The European Council adopted the EU Cybersecurity Act in April 2019. The Act permanently designates the European Union Agency for Network and Information Security (ENISA) as Europe’s cybersecurity agency and establishes an EU cybersecurity certification framework. Separately, European Supervisory Authorities (ESAs) published a Joint Advice on the costs and benefits of establishing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector. In addition, the European Union’s General Data Protection Regulation (GDPR) and the revised Payment Services Directive 2 (PSD2) requirements are driving closer regulatory scrutiny regarding the use of consumer data.

**Key focus areas**

**Cybersecurity governance.** The responsibilities and expectations for boards have evolved from just having a high-level understanding of cybersecurity to having an in-depth understanding of the cyber risks to which their organization is exposed; understanding the organization’s strategy for tackling those risks; and ensuring the strategy is being executed with sufficient rigor and accountability.

**Cyber resilience.** Cyber resilience is a focus for financial institutions globally, with an emphasis on building holistic, enterprise-wide cyber resilience programs. Lack of such programs could lead to extended disruption of critical functions, reduced confidence in firms and markets, and an inability to recover operations.

**Privacy and data security.** Businesses globally should increase their focus and efforts in this critical area as various jurisdictions ratchet up their privacy and data protection laws (e.g., GDPR, CCPA). Many countries are also focusing on cloud-related data residency requirements, limiting data movement beyond borders.

**Outsourcing risks.** Regulators are concerned about financial institutions’ increasing reliance on third-party service providers to support much of their critical infrastructure. Regulators are also concerned about too many financial institutions using the same providers and the widespread use of cloud.
Although regulatory scrutiny and pressure might be a key driver for cybersecurity programs, continued investment to strengthen cybersecurity programs is now a fundamental business need that can help companies grow and prosper in this evolving and challenging digital environment.

Let’s talk

Mark Nicholson
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
manicholson@deloitte.com

Proactive risk identification and mitigation through improved analytics and compliance monitoring

There is a fine line between fraud and error, and the distinction often lies in the intent of the individual. As such, it is crucial that investment managers and financial organizations proactively assess and identify their risk areas, using analytics to enhance their risk and compliance monitoring efforts. Harnessing analytics can help a firm preemptively identify abnormalities within its operations and assess whether they are the result of an error, a potential fraud, or a regulatory violation.

Applying analytics to the ever-increasing volume of data now being collected as a standard, regulators have been taking a strong enforcement stance to identify a wide range of issues that compliance and risk managers actively seek to avoid, such as potential violations related to market activity, firm operations, and fees charged.¹

Enterprise monitoring solutions can help detect abnormalities through 1) specific checks, such as identifying unusual patterns among trades; or 2) a proactive, integrated enterprise fraud and misuse management approach, uncovering hidden patterns, trends, and schemes that traditional fraud detection and compliance-oriented methods might miss. Advances in analytical tools have opened the door to better identification of such activity. For example, analytics can help risk and compliance managers identify unexpected trading patterns that could be signs of inappropriate behavior, market timing, or customer life cycle events that don’t align with regulatory guidelines or the customer’s best interest.

SEC enforcement and analytics are on the rise

Proactive identification and mitigation of large-scale compliance fraud can help firms avoid substantial financial and reputational damage. In FY 2019, the SEC brought 862 enforcement actions and obtained judgments for $4.35 billion in penalties and disgorgement.²

As part of its efforts to protect retail investors from fraud, the SEC has invested over $140 million in analytical monitoring capabilities³ and collected data on billions of trades to assess whether compliance violations are occurring. Also, it established the Division of Economic and Risk Analysis (DERA) and the Retail Strategy Task Force.

On September 25, 2019, SEC Chairman Jay Clayton delivered a speech to the US House of Representatives Committee on Financial Services. In the speech, he stated that the commission’s three goals for FY2019 through FY2022 are:

- Focusing on the interests of long-term Main Street investors
- Innovating and responding to the changing nature of markets
- Elevating the agency’s performance through technology and data analytics⁴

From FY2018 to FY2019, the number of SEC cases against investment advisers and investment companies increased by 60 percent, with fines in the millions per case.⁵ To avoid such problems, investment firms should match the SEC’s efforts and focus by making greater use of technology and data analytics to enable more proactive monitoring of investment adviser compliance as it pertains to Main Street investors.

Increased focus on cross trading

As noted in the previous discussion on SEC hot topics, on September 4, 2019, the SEC’s OCIE issued a new risk alert focused on principal and agency cross trading compliance issues over the past three years. Investment advisers are required to disclose to the client when they are purchasing or selling securities on their own behalf (“principal trades”).⁶ They are also required to disclose when they are acting as a broker for a third party attempting to sell or purchase a security from the client (“agency cross transactions”). The OCIE will increasingly be monitoring the actions of individual investment advisers regarding these issues.⁷

Although principal and cross trades are much less common than market trades, they tend to be more challenging to reconstruct retrospectively, because the trader is typically the only person who knows the rationale for the trade. Using analytics to identify these scenarios early can help compliance managers determine if there is a training deficiency, persistent human error, or a systemic issue that requires attention. Note that this is just one OCIE focus area where a comprehensive monitoring program that covers areas such as market activity, trades, program and portfolio fees, and commissions can help mitigate the unintended compliance oversight
that could potentially lead to inquiries, deficiency letters, and, in extreme cases, costly fines and penalties.

The sheer volume of trading data that compliance offices must continuously monitor to effectively unpack issues around principal and cross agency trading transactions, amongst other challenges, is ever-increasing. The use of analytical tools to help monitor operations proactively to mitigate such concerns is moving from a “leading practice” to a necessity. With the improvement of computer processing power, artificial intelligence algorithms, and tech-savvy regulators, not leveraging analytics to better control for trading risk and compliance is a strategic and reputational risk.

**Taking action**

In order to understand and better preempt SEC actions around compliance, risk, and potential fraud, internal compliance teams should invest in analytics that can help them understand the actions of their firm’s investment advisers. With the increasing volume of daily trades, enterprise monitoring programs that use analytics are essential for helping firms maintain compliance and oversight of their daily operations.

Investment firms have a strong incentive to stay aware and informed about updates and alerts from regulators and to apply leading-edge analytical techniques to address the SEC’s priority areas. As firms continuously strive to reach the goal of zero compliance issues, their efforts can be accelerated by preempting regulatory scrutiny through proactive risk identification and mitigation that includes analytics monitoring tailored to their specific risks.

5. SEC, *2018 Annual Report*
6. Ibid.
Enterprise risk management: Integrating risk management drives strategic growth

The journey of integrating risk management into the enterprise continues to evolve. Historically, risk management in the investment management industry was primarily focused on financial risk. However, after the financial crisis, many firms—to varying degrees—have increased their focus on nonfinancial risks, such as strategic, operations, compliance, and reputational risks, and the degree to which these risks are mitigated. The shift is being driven by powerful forces that are reshaping the investment management landscape, including market changes, investor demographics, margin and fee pressure, high compliance costs, and increased use of data assets and technology.

In response to these market dynamics, firms are making a conscious effort to modernize their risk management practices. Enterprise risk management can achieve greater value by:

• Linking risks to the overall business strategy
• Enabling risk-based decision-making
• Allocating resources more effectively to support the strategy
• Institutionalizing risk governance from the board level down through senior leadership and into the business units

Boards and senior executives are increasingly focusing on a broad set of risks that span the enterprise: financial, operational, reputational, regulatory, extended enterprise, strategy, and technology. The risk management function should be part of those top-level discussions. According to a recent Deloitte survey, when risk management is present at board or C-suite meetings “always or most of the time,” 38 percent of executives say it increases their confidence in decisions and strategies, and 88 percent say it increases their confidence in risk data.

In 2020, we expect OCIE to continue prioritizing the examination of certain practices, products, and services that potentially pose heightened risks to investors or the integrity of the United States capital markets. Regulators and investment management clients are both starting to ask more probing questions about risks across the business, and they want to understand the strategies, systems, and processes firms have in place for areas such as governance, clear ownership and accountabilities, and risk mitigation. In particular, cybersecurity and use of third-party providers are likely to remain high priority areas, both for risk management and regulatory compliance.

Outside the US, risk management capabilities are largely being shaped by the regulatory requirements of local (non-US) jurisdictions. Risk areas related to financial crimes—especially anti–money laundering (AML), antibribery and corruption, and conduct risk—have been a heightened focus for years and will likely remain paramount as regulators potentially seek personal liability against executives and senior leaders. In addition, new focus areas are emerging, including outsourcing (extended enterprise) risks, investment management–centric operational risks (e.g., complex business models and investment performance), and technology (cyber) and data management risks.

Regardless of the jurisdictions in which firms operate, embedding risk management into the business provides greater shared perspectives on the risks facing the organization and enables a holistic risk profile that spans all risk types. It also enables greater ownership and accountability for risk mitigation and prioritization. Last but not least, it promotes smart risk-taking through risk-based decision-making and resource allocation that better aligns with the firm’s business strategy.

Growing regulatory complexity

As investment management firms continue to expand their global footprints, they face a set of regulatory expectations that are complex, rapidly evolving and growing, and often conflicting. In the United States, the SEC’s OCIE noted in its 2019 Examination Priorities publication that “investment adviser examinations identified emerging risks at advisers selling or recommending digital assets, such as concerns related to custody and safekeeping of investor assets, valuation, omitted or misleading disclosures regarding the complexities of the products and technology, and the risks of dramatic price volatility.”

In 2020, we expect OCIE to continue prioritizing the examination of certain practices, products, and services that potentially pose heightened risks to investors or the integrity of the United States capital markets.

Regulators and investment management clients are both starting to ask more probing questions about risks across the business, and they want to understand the strategies, systems, and processes firms have in place for areas such as governance, clear ownership and accountabilities, and risk mitigation. In particular, cybersecurity and use of third-party providers are likely to remain high priority areas, both for risk management and regulatory compliance.

Outside the US, risk management capabilities are largely being shaped by the regulatory requirements of local (non-US) jurisdictions. Risk areas related to financial crimes—especially anti–money laundering (AML), antibribery and corruption, and conduct risk—have been a heightened focus for years and will likely remain paramount as regulators potentially seek personal liability against executives and senior leaders. In addition, new focus areas are emerging, including outsourcing (extended enterprise) risks, investment management–centric operational risks (e.g., complex business models and investment performance), and technology (cyber) and data management risks.

Regardless of the jurisdictions in which firms operate, embedding risk management into the business provides greater shared perspectives on the risks facing the organization and enables a holistic risk profile that spans all risk types. It also enables greater ownership and accountability for risk mitigation and prioritization. Last but not least, it promotes smart risk-taking through risk-based decision-making and resource allocation that better aligns with the firm’s business strategy.
Each of those benefits can be further enhanced through the effective use of risk management technology. However, recent surveys show that while advanced risk management programs can significantly improve performance, nearly 80 percent of firms surveyed today have not yet aligned technology with the needs of risk management.

Analytical technologies are essential for risk modeling and sensing. Similarly, data visualization is essential for risk tracking and monitoring—and for achieving leadership buy-in. However, according to a recent Deloitte study, less than half of the organizations surveyed are using technology to assist in risk sensing and internal approval processes. In many cases, firms have rushed to risk insight by applying artificial intelligence tools to disparate data stores without building the context around the data. Other firms adopted governance, risk, and compliance (GRC) technology to automate workflows without fully realizing the value contextualizing the risk data can bring. Now, many firms are shifting toward a common platform for GRC (either a single vendor application or a streamlined set of “best of breed” applications) in order to optimize the integration of risk data and enable a more predictive risk intelligence framework.

“GRC platforms continue to play an important role [in risk management] when insightful metrics, aligned with specific risk exposures, are collected and tagged with contextual reference data provided by a common taxonomy residing in a GRC platform.” The range of practice related to aligning risk and compliance stakeholders, establishing policies, and deploying technology and data structures to achieve integrated risk management has evolved. Today, many firms can achieve a moderate level of maturity in risk assessment and issue management in less than a year.

Taking action
Moving forward, there are some key areas to focus on when integrating enterprise risk management:

• Risk management capabilities enable a firm’s strategy, risk-based decision-making, and more effective allocation of resources.

• A robust governance structure helps risk management keep pace with the firm’s business strategy and growth opportunities, whether launching new products, expanding into new markets, responding to risk events, or adapting to changes in regulatory priorities.

• A comprehensive understanding of the risk landscape helps the leadership team identify, assess, monitor, and manage risks across the enterprise (and adapt to emerging risks).

• Technology helps integrate risk management data and information to support forward-looking, predictive analytics.

These four pillars can provide a strong foundation to help maximize the value of risk management across the enterprise.

2. Ibid.
3. Ibid.
4. Ibid.
Staying ahead

The regulatory landscape is constantly shifting. Some changes are big enough to grab headlines. Others are nearly invisible but can have a big impact. For the latest regulatory updates and insights, please visit www.deloitte.com/us/InvestmentManagementRegulatory/Outlook.
Leadership

Alok Sinha  
Regulatory & Operations Risk Leader  
Principal | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
asinha@deloitte.com

Monica O’Reilly  
Advisory Financial Services Industry Leader  
Principal | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
monoreilly@deloitte.com

Krissy Davis  
Advisory Investment Management Leader  
Partner | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
kbdavis@deloitte.com

Irena Gecas-McCarthy  
FSI Director, Deloitte Center for Regulatory Strategy, Americas  
Principal | Deloitte Risk & Financial Advisory  
Deloitte & Touche LLP  
igecasmccarthy@deloitte.com
About the Center
The Deloitte Center for Regulatory Strategy provides valuable insight to help organizations in the financial services, health care, life sciences, and energy industries keep abreast of emerging regulatory and compliance requirements, regulatory implementation leading practices, and other regulatory trends. Home to a team of experienced executives, former regulators, and Deloitte professionals with extensive experience solving complex regulatory issues, the Center exists to bring relevant information and specialized perspectives to our clients through a range of media, including thought leadership, research, forums, webcasts, and events.

This article contains general information only and Deloitte is not, by means of this article, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This article is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this article.

About Deloitte
As used in this document, “Deloitte” means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2020 Deloitte Development LLC. All rights reserved.