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 2019. 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 2019, 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 impacting investment management in 2019, 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 2019 and the regulatory changes it may bring. Please feel free to contact us with questions and feedback at CenterRegulatoryStrategyAmericas@deloitte.com.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global foreword</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>6</td>
</tr>
<tr>
<td>Regulatory enforcement: Data and analytics</td>
<td>8</td>
</tr>
<tr>
<td>Cybersecurity and privacy</td>
<td>10</td>
</tr>
<tr>
<td>Investment company liquidity risk management programs</td>
<td>14</td>
</tr>
<tr>
<td>Integrated risk management and compliance</td>
<td>16</td>
</tr>
<tr>
<td>Conduct risk</td>
<td>18</td>
</tr>
<tr>
<td>Model risk management</td>
<td>19</td>
</tr>
<tr>
<td>Operational risk</td>
<td>22</td>
</tr>
<tr>
<td>Best interest rules</td>
<td>23</td>
</tr>
<tr>
<td>Cryptocurrency</td>
<td>24</td>
</tr>
<tr>
<td>Taking the lead in times of change</td>
<td>26</td>
</tr>
<tr>
<td>Endnotes</td>
<td>28</td>
</tr>
<tr>
<td>Contacts</td>
<td>29</td>
</tr>
</tbody>
</table>
Global foreword

Nearly 10 years after the financial crisis, the long shadow it has cast has started to fade. With the exception of one final component of Basel III, most post-crisis prudential policies have now been decided, and banks in particular are now much better capitalized and more liquid than before the crisis. Amid varied approaches and timetables to national implementation of agreed prudential reforms, attention is now more acutely focused on culture and governance; the challenges of new technology; and emerging economic, market, and operational risks. Firms need to be prepared to respond to this shifting focus and the new demands that it will place on them.

Lifting of accommodative monetary policy

Globally, monetary easing and low interest rates are slowly giving way to interest rate “normalization,” although rates are expected to settle at levels significantly below historical norms. The United States has led the way with a series of rate rises and the Federal Reserve has begun to shrink its balance sheet. The Bank of England has tentatively begun to raise rates, and the European Central Bank is bringing an end to the expansion of its balance sheet. In Australia, interest rates remain on hold but are expected to begin rising. Japan is the major exception to this trend, with rates expected to remain low in the near future. Given the number of headwinds to the global economy (e.g., high levels of debt, elevated levels of geopolitical risk, and trade protectionism), the pace of any interest rate rises is likely to be slow.

Higher interest rates may be beneficial in net terms to certain firms: banks may enjoy higher net interest margins and insurers could benefit from rising asset yields. However, interest rate normalization may also lead to falls in some asset values and rising credit defaults as well as revealing structural weaknesses in both the global economy and individual firms. It is unclear what the overall effect of these opposing factors will be, especially at the level of individual firms and sectors.

An uncertain economic environment

Meanwhile, a period of accommodative monetary policy has contributed to a buildup of debt, with global debt levels now at $247 trillion, significantly higher than their pre-crisis peak. In many commentators’ eyes, this represents a key systemic vulnerability. Low rates also contributed to a sustained search for yield that may have led many lenders and investors to move down the credit quality curve. Further, comparatively higher capital requirements for banks have paved the way for a rise in nonbank lending, which means that exposure to credit markets now extends to a much wider variety of firms. Both the leveraged loan and real estate markets are likely to be vulnerable to higher interest rates, while consumer credit expansion and the resulting high levels of personal debt may have left many consumers vulnerable to interest rate rises, especially after such a prolonged period of low rates.

Looking at the wider global economic picture, we see a mixed outlook. Economic growth continues to be strongest in parts of Asia, although Chinese growth has slowed, while the outlook for emerging and developing economies is uneven. Recoveries in both the United Kingdom and United States are now close to a decade long, while eurozone expansion—although weaker—is also well embedded. Historically, downturns or recessions have occurred at least once each decade, suggesting that such an event may be overdue.³

Some commentators⁴ consider that the global economy has reached its “late cycle” phase, most evident in asset valuations that appear stretched on historic bases. In the European Union, close to €731 billion⁵ of nonperforming loans continue to act as a major risk to some banks’ resilience and profitability, while globally, increasing trade protectionism and political uncertainty also weigh heavily on the minds of many in the industry. Brexit continues to be a major geopolitical and regulatory uncertainty, and both regulators and politicians will attempt to mitigate its risks and effects throughout 2019. Nevertheless, if there is a disorderly Brexit, leading potentially to new political strategies and approaches, the implications for how a number of these regulatory predictions unfold in the United Kingdom could be profound.

Against this background, we expect regulators across sectors to remain highly vigilant to the risks of economic downturn and market shocks. They will likely want to use stress testing extensively to assess firm vulnerability and resilience, recognizing that during a period of unprecedentedly low interest rates some business models have grown up in relatively benign conditions and have yet to be tested in a sustained downturn.

A retreat from global coordination
The global regulatory approach is changing. The aftermath of the financial crisis saw a globally coordinated response to draw up a series of new regulations that would underpin a more robust and stable financial system. However, there is starting to be a move away from global policy making and a reduced appetite for cross-border regulatory cooperation. As a result there are increasing signs of regulatory divergence, including geographical and activity-based ring-fencing, as different regions and countries look to tailor regulations to their own needs. Global firms are, therefore, having not only to comply with these divergent rules in the different jurisdictions in which they operate, but also to optimize their local governance structures, operating models, legal entity structure, and booking models.

A shift to supervision
We do not expect regulators to embark on a path to wholesale unraveling or reversing the post-crisis reforms implemented since 2008. But it seems that, absent a significant unexpected event, there is little prospect of major new regulation, especially in relation to bank and insurance capital.

³ EBA, Risk Dashboard Data, Q2 2018.
Regulators’ key priorities are to consolidate and safeguard and—in some jurisdictions—refine the reforms of the past decade. What we do expect is a sharp tilt away from a period of regulatory re-design and innovation, to one of operating and embedding the reformed supervisory system.

As a result, firms in many countries are seeing rising supervisory expectations, reflecting the growth of principles-based supervisory approaches that emphasize the importance of firms’ governance, culture, and management approach and the outcomes, both prudential and conduct, these are delivering. Firms’ conduct and the treatment of their customers are also receiving increased focus in numerous countries, driven by political and regulatory concern over the perceived poor conduct of firms across all financial sectors.  

Supervisors are also adopting more intrusive practices, including greater use of on-site supervisory visits. This reflects global leading practice and the increasing need for supervisors to engage directly with firms in order to understand their strategies and business models, risk profiles and appetites, and risk management frameworks and approaches, and to hold boards and senior management accountable for the outcomes these deliver.

**New technologies**

Firms, regulators, and their customers are considering the opportunities and risks associated with new technologies. For example, due to the rapid development of artificial intelligence, machine learning, and fintech solutions, once-new technologies are quickly becoming mainstream. The powerful impact these technologies will have should not be underestimated, not only on consumers, but also on regulation and supervision. The pace of technological change, therefore, demands deep thinking about the appropriate regulation of processes, products, and institutions to avoid regulatory gaps and to ensure financial stability and consumer protection.

These technology developments and disruption have triggered a debate around the perimeter of financial services regulation. Many incumbent firms worry that new technology-driven entrants offer services that lie outside the boundaries of existing financial services regulation and which incumbent firms find more costly to deliver because of a “compliance leakage” from the regulated activities that they are undertaking. We do not expect regulators to “come to the rescue” of incumbents, who will have to look to their own resources to rise to the challenge of competition. However, we expect that these level playing field concerns, along with worries about the role of technology in society more generally, will drive increasing interest in how fintech firms and crypto assets are regulated—or rather, at present, how they are not. We expect clarification of the regulatory treatment of crypto assets, especially in the areas of investment by retail consumers, money laundering, and prudential capital for banks.

---

Acting in the face of uncertainty

While the current regulatory environment appears more settled compared to the recent past, regulators across the world continue to set high expectations intended to maintain a strong, resilient financial sector through firms having robust financial and operational resilience, supported by strong risk management and compliance capabilities. In our view, this may provide an opportunity for leading financial firms to pivot from having to build frameworks to reflect a barrage of new regulations to optimizing through taking advantage of new technologies and operating models.

The world changes and regulation changes with it

The debates around the regulatory perimeter and potential fragmentation of the financial system mean that firms’ operational resilience, as well as their susceptibility to cyber and financial crime, are becoming much greater issues for regulators. As part of this, we also expect a sharpening supervisory focus on how boards and senior management teams control the risks posed to them by their exposure to outsourced providers and other third parties.

The past decade has seen profound and lasting changes in the structure of the economy, employment, and society. The providers, consumers, and regulators of financial services are all changing. Aging populations and new Millennial consumers are demanding different types of financial services and products, distributed in different ways. This changing and challenging background makes it essential to consider the future of regulation holistically, rather than in a piecemeal manner. All sectors and stakeholders have an important role here, and we hope that this year’s outlook from our Regulatory Centers will both inform and stimulate this discussion.
Introduction

Compliance modernization helps companies pursue their core mission and 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. This is an ongoing need driven by never-ending technological advances and market expectations that are constantly rising. No matter how “modern” a company’s existing compliance systems and processes might be, there is always room to improve.

This is especially true when changes in political leadership can lead to different areas of regulatory focus. Following the 2018 midterm election, the Democratic Party leadership has indicated that the House Financial Services Committee will broadly focus its legislative agenda toward protecting consumers and investors, preserving financial sector stability, and encouraging responsible innovation in financial technology. Meanwhile, the Republican-controlled Senate has indicated that it will continue to focus its legislative agenda on the remaining refinements not already addressed in the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA)1 passed in 2018. Beyond the divided Congress, we note that the regulatory agencies are now all led by President Trump appointees who have discretion, subject to congressional oversight, to calibrate their supervisory policies and programs.

Regardless of what definitive changes lawmakers and regulators might make investment management organizations should continue to drive effectiveness and efficiencies across their risk and compliance programs so they can meet applicable laws, regulations, and supervisory expectations.
While much has been written in the press about the shift in governmental enforcement away from the “broken windows” concepts of the US Securities Exchange Commission (SEC) chaired by Mary Jo White, current SEC Chairman Jay Clayton recently emphasized that his tenure will focus on retail investors and seemingly smaller matters. However, this attention on protecting retail investors will likely lead many large investment management firms to focus on data quality at a much more granular level, because government inquiries may prompt firms to analyze large volumes of transaction data to better understand retail investor impacts.

Many data initiatives from the past are still in full force both for the SEC and Financial Industry Regulatory Authority (FINRA). In fact, in a draft of its strategic plan for 2018–2022 that was issued in June 2018, the SEC explained that one of its three strategic goals is to “elevate the SEC’s performance by enhancing our analytical capabilities.”

As the SEC increases its use of analytics to protect investors, organizations that manage investors’ funds not only need to improve the quality of data they currently produce, but also they need to improve the quality of data produced in the past. The days of regulators requesting data sets prior to beginning an inquiry, or in response to self-disclosure, are long gone. Today, regulators are requesting data to supplement the large volumes of data already in their possession—putting investment managers in a more defensive position than ever before.

**Key focus areas related to analytics**
In its strategic plan, the SEC stated “we should expand our focus... in vital areas such as market monitoring analysis, market operations, including clearing and settlement and electronic trading across our equity, fixed-income and other markets.” To keep pace with the SEC’s efforts, investment managers should be analyzing data sources related to those focus areas, checking for completeness and accuracy.

Two of the five initiatives in the SEC’s analytics enhancement objectives specifically relate to risk and data analytics:

- “Expand the use of risk and data analytics to inform how we set regulatory priorities... enabling rigorous analysis at a reduced cost.”
- “Enhance our analytics of market and industry data to prevent, detect, and prosecute improper behavior.”

Given these broad objectives, we believe the analytics office of the SEC’s Division of Investment Management will continue...
to take on greater importance as the data aggregator and monitor for the investment management industry.

What does the SEC’s focus on enhanced risk and data analytics mean for investment managers? As investment managers evaluate their current and legacy information systems, their service providers’ information systems, and the data obtained from customers, there are several specific areas to consider. They include:

Data quality and control
When evaluating current system capabilities and migrating from legacy systems to newer, cloud-based systems, maintaining quality and control of legacy data is crucial. During these transitions, data can easily be lost, corrupted, or mismanaged. Maintaining effective control over data completeness is particularly important in the event of a regulatory inquiry.

Transactional life cycle completeness
With the SEC’s emphasis on protecting retail investors, it has become increasingly important to maintain a complete record of investment management transactions. Having a complete record—from initial purchase, through the various middle- and back-office systems, and onto the ultimate sale—can enable a firm to understand each element in the life cycle of a security it owned. This information may include complex details such as foreign withholding taxes and associated rates (given the complexity of international tax laws and treaties), as well as foreign securities (such as American Depository Receipts [ADRs]). What makes transactional life cycle completeness especially challenging is the use of various order entry, order processing, fund accounting, and custody systems—many of which involve third-party service providers.

Service provider transitions and data quality
A change in service providers—or in a service provider’s systems—can have a critical impact on data quality/control and transactional life cycle completeness. We have seen many cases where a transition from service provider A to service provider B—or a change in a service provider’s accounting or data management systems—created significant data challenges. As part of any service provider transition, an investment management firm should be aware of the key data fields and elements in its current database and should take active measures to validate that those key data fields will be maintained by future service providers and their future systems. Failing to monitor data quality during a service provider transition or system transition can lead to incomplete data sets, driving up the potential cost and impact of regulatory inquiries and remediation.

Data interchanges
We have conducted forensic investigations for many firms where the simple movement of data from one system to another resulted in the loss of key data elements, making it difficult or impossible for a firm to fully understand a transaction. Knowing which data elements travel from one system to another during the course of a transaction can help investment managers avoid potential problems.

Impact of mergers/divestitures on data
Mergers and acquisitions—and the subsequent rationalization of investment managers, fund offerings, systems, and operations—present a myriad of data issues. When fund managers merge among themselves, simply combining their data is not enough. Instead, it is important to understand the various data elements each entity uses and stores in its databases, since providing complete data sets for the merged entity will likely be a necessary challenge in the event of a regulatory inquiry. When funds merge within an investment manager, it is important to maintain separate records for the merged fund prior to it being acquired by the acquiring fund. To provide accurate historical data, the closing statements (and associated historical transactional data) need to be maintained.

Keeping pace with the SEC
In light of the SEC’s growing use of analytics—and its increased access to data from a variety of sources—investment managers need to ratchet up their capabilities in data quality and analytics. This can help firms proactively identify and mitigate issues on their own, without a regulatory inquiry. This is something the SEC now expects, and getting it right can improve a firm’s credibility and help avoid costly penalties, fines, and reputation damage.
In an age when hacking and data breaches have become so commonplace that they are almost expected, cybersecurity continues to dominate both the headlines and the regulatory agenda. According to a 2018 study, the global cost of cybercrime in 2017 was a staggering $600 Billion. A study by Deloitte revealed that the business impact of a cyberattack spans beyond the traditional costs attributed to a cyber incident and range from regulatory and legal action to long-term loss of trust, customer relationships, and brand value. Financial institutions are at the forefront of bearing the brunt of cybercrimes. The US Treasury Department has named cyberattacks as one of the top risks facing the US financial sector.

As the SEC stated in its February 2018 guidance to companies on cybersecurity disclosure, “Cybersecurity risks pose grave threats to investors, our capital markets, and our country... Today, the importance of data management and technology to business is analogous to the importance of electricity and other forms of power in the past century.”

The US Administration has placed renewed emphasis in improving the coordination between federal agencies and state member organizations to improve the reliability and security of the financial sector infrastructure through the Financial and Banking Information Infrastructure Committee.

Specific trends in capital markets—such as increased use of outsourcing by financial institutions to reduce costs and large-scale adoption of innovations such as cloud computing—have increased the exposure to cyber risks. Further, exponential increase in data-processing capabilities because of mainstream adoption of RPA and use of machine learning has increased the ability to correlate large volumes of data sets and introduce decision making that can infringe upon the privacy and rights of individuals.

Legislators are working to keep pace by introducing new privacy and cybersecurity laws. A selection of key legislative and regulatory developments is presented below to provide insights into the nature of issues that legislators are requiring organizations to address.

**EU General Data Protection Regulation (GDPR)**

Among all issues related to data, privacy rights and ownership have come to the fore. Widely reported data breaches may have been one of the initial causes for increased consumer and supervisor concerns about data privacy. However, those concerns were quickly supplanted by concerns about what companies do with data after a consumer clicks “accept” on a user agreement. For capital markets institutions reliant on data analysis in various forms, this raises fundamental questions. In particular, how do you use data that in some sense belong to your customer, without violating customer privacy or raising regulator concerns?

This year saw the European Union (EU) General Data Protection Regulation (GDPR) take effect in May 2018, providing two years of adoption. GDPR replaced the EU Data Protection Directive of 1995 and is the first and most globally publicized move to safeguard consumer privacy rights. As such, it may be indicative of what is to come elsewhere. The GDPR regulates the processing by an individual, a company, or an organization of personal data relating to individuals in the EU.

Among numerous protections offered by GDPR, consumers need to be informed if their data are moved outside the EU; have the right to be “forgotten”; and must be given a chance to contest the use of automated algorithms. Other rights include the right to object to the use of one’s data for marketing purposes, as well as the right to data portability (i.e., the ability to receive one’s data in a machine-readable format and send it elsewhere).

Violations can be costly. Individuals suffering material damage from a violation have the right to compensation. Also, in response to infringements, European data protection authorities can impose sanctions that can be as drastic as a ban on data processing, as well as fines of up to 4 percent of annual global turnover.

**California Consumer Privacy Act (CCPA)**

In the United States, California enacted the California Consumer Privacy Act of 2018 (CCPA), a significant legislation that greatly expands data subject rights and introduces provisions for civil class action lawsuits based on statutory or actual damages. The law takes effect in July 2020.

Although there may still be amendments before the law takes effect, for now it provides California citizens with some similar protections to the GDPR. These include the right to access personal information (and to know how a company uses that information), as well as the right to have information removed in some circumstances.

Among other rights, the CCPA “authorizes a consumer to opt out of the sale of personal information by a business and prohibits the business from discriminating against the consumer for exercising this right, including by charging the consumer who opts out a different price or providing the consumer a different quality of goods or services, except if the difference is reasonably related to value provided by the consumer’s data.”

Consumers have a right to private action in response to uncorrected CCPA violations, and the state attorney general is also empowered to pursue civil penalties. There are certain exemptions
that are granted within the law for data that are subject to the Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA).

**New York Department of Financial Services cybersecurity regulation**

The New York State Department of Financial Services (NYDFS) regulation took effect on March 1, 2017, with a phase-in period concluding on March 1, 2019. The regulation requires financial services companies to establish and maintain a risk-based cybersecurity program and supporting capabilities.

The two-year phase-in provides a glide path toward compliance. Companies subject to the regulation should by now have satisfied most of its requirements, which include: creation of a written cybersecurity policy; designation of a Chief Information Security Officer (CISO); periodic penetration testing and vulnerability assessment; data preservation that enables accurate reconstruction of all financial transactions; and necessary accounting to respond to a cybersecurity event for at least three years.

To achieve compliance, the board of directors need to be involved in the creation of standards and should receive regular reports on cybersecurity. In addition, companies are required to file a risk and safeguards assessment in their annual report to regulators.

The next and final phase of the NYDFS regulation—to be completed by March 1, 2019—is the requirement that financial services organizations establish cybersecurity controls and protocols for third-party risk management (TPRM). This includes requirements related to developing and implementing a TPRM program, maintaining a third-party inventory for service providers that access non-public information (NPI) or information systems, and performing due diligence and ongoing monitoring.

It is important to note that the NYDFS regulation expands the scope of covered third parties beyond typical vendors to include all third parties with access to NPI. Given this broad purview, programmatic essentials such as governance, reporting, and broader end-to-end life cycle management are key for the sustainable management of an effective TPRM program.

**Third-party risk management**

TPRM is being viewed as a basic regulatory expectation. Examples of leading industry practices for an effective TPRM program related to cybersecurity and data risk include:

- Adequate reporting and governance, along with training to facilitate accountability and oversight
- Streamlined processes for third-party management, including stakeholders from sourcing, legal, etc.
- Appropriate third-party termination practices that address retention and destruction of records

In addition, a comprehensive TPRM program should address broader risk and control management practices, including service level agreement (SLA) performance; exit strategy; financial viability; resiliency; reputational review; and regulatory compliance.

Organizations today should consider investments in revisiting and validating their TPRM programs to formalize the program scope, enhance inventory processes, and optimize due diligence and assessment procedures—and to integrate contract management of their third-party landscape.

All of these components should be managed as part of a broader risk management and information governance effort that stretches beyond the CISO and IT. All data users—whether internal or external—are responsible for data security. However, it is the responsibility of the board and executive leadership to provide the required resources, authority, and accountability to ensure adequate data security across the enterprise. Also, it is critical for the board to lead by example, providing the necessary tone-at-the-top to convey the importance of properly managing this prime operational risk.
**SEC disclosure guidance**

The SEC issued disclosure guidance to public companies in early 2018. The guidance stipulates that public companies are required to disclose material information in a timely manner, and, among other guidance, the SEC clarified the desired extent of disclosure related to cyber risks and cybersecurity. In some cases, this may include retroactive disclosure.

The SEC also clarified the need for board involvement in cybersecurity and cyber risk management. CEO and CFO certifications “should take into account the adequacy of controls and procedures for identifying cybersecurity risks and incidents and for assessing and analyzing their impact. In addition, to the extent cybersecurity risks or incidents pose a risk to a company’s ability to record, process, summarize, and report information that is required to be disclosed in filings, management should consider whether there are deficiencies in disclosure controls and procedures that would render them ineffective.”

To address the need for uniformity and transparency in cyber risk reporting, the American Institute of Certified Public Accountants (AICPA) released its cybersecurity attestation reporting framework—“System and Organization Controls (SOC) for Cybersecurity”—in 2017. Organizations can use this framework to convey information about the effectiveness of their cybersecurity risk management programs in a common language, helping all stakeholders better understand the organization’s cybersecurity risk management program.

The SOC for Cybersecurity consists of three sections:

1. A management-prepared narrative description of the entity’s cybersecurity risk management program, designed to provide information about how the entity identifies its most sensitive information, the ways in which the entity manages its cybersecurity threats, and the key security policies and processes implemented and operated to protect the entity’s information assets against those threats.

2. Management assertion whether the description in the first section is presented in accordance with the description criteria, and whether the controls within the program were effective to achieve the entity’s cybersecurity objectives based on the control criteria.

3. Practitioner’s opinion, in which a certified public accountant (CPA) provides an opinion on the description, and on the effectiveness of controls within the program.

The SOC framework provides a number of potential benefits, including helping to satisfy information and oversight requirements for the board and senior management (as well as regulators) and helping to reassure investors and customers.

For organizations planning to embark on an attestation, a leading practice to consider might be a readiness assessment (figure 1).

---

**Figure 1. Cyber readiness assessment**

<table>
<thead>
<tr>
<th>Key stakeholders</th>
<th>AICPA Cybersecurity Attestation Reporting Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board of directors</td>
<td>Management’s description of the cybersecurity risk management program</td>
</tr>
<tr>
<td>Regulators</td>
<td>Management’s assertion on:</td>
</tr>
<tr>
<td></td>
<td>• The presentation of the description</td>
</tr>
<tr>
<td></td>
<td>• The operating effectiveness of the controls to achieve the cybersecurity objectives</td>
</tr>
<tr>
<td>Cyber insurance carriers</td>
<td>Practitioner’s opinion on:</td>
</tr>
<tr>
<td></td>
<td>• The presentation of the description</td>
</tr>
<tr>
<td></td>
<td>• The operating effectiveness of the controls to achieve the cybersecurity objectives</td>
</tr>
</tbody>
</table>

**Benefits**

1. Greater transparency;
2. Independent and objective reporting;
3. Operational efficiencies;
4. Useful in making informed and strategic decisions;
5. Strategic competitive advantage and enhancement to brand and reputation; and
6. A comprehensive set of criteria/control framework(s).

Source: Description Criteria for Management’s Description of an Entity’s Cybersecurity Risk Management Program, https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/AICPACybersecurityInitiative.aspx
Ongoing and future developments
Several other countries have continued to enhance their privacy and cybersecurity laws. Notable examples include:

- **Brazil** enacted its General Data Protection Law in July 2018 that significantly provides for significant rights and protections to personal information. The law is widely touted as being very similar to GDPR. Organizations have 18 months to comply.

- **United Kingdom** issued its Data Protection Act 2018 that implements the GDPR provisions and imposes as well as implements additional requirements, such as on matters related to national security and immigration.

- **Singapore** passed the Cybersecurity Act in March 2018, subjecting organizations to information sharing, reporting incidents, conducting cybersecurity audits, and participating in national cybersecurity exercises.

- **Australia** included mandatory data breach notification requirements within its Privacy Act that obligate financial credit institutions to notify individuals whose personal information is involved in a data breach that may cause harm.

Future outlook related to cybersecurity and data privacy continues to indicate strong regulatory developments, with several countries either implementing or enhancing existing regulatory requirements. Within the United States, organizations can also expect to see continued attempts toward simplification of regulatory compliance requirements, such as those noted within the Core Principles report from the Treasury, as well as continued efforts toward harmonization of data privacy and cybersecurity laws and regulations.
Investment company liquidity risk management programs

In last year’s regulatory outlook, we discussed the SEC adopting a new rule and form designed to promote better liquidity risk management (LRM) by registered investment companies. The rule (Rule 22e-4 under the Investment Company Act of 1940) requires funds, including exchange-traded funds (ETFs), to establish liquidity risk management programs. ETFs that qualify as “in-kind ETFs” are exempt from some of the rule’s requirements, and money market funds and closed-end funds are exempt from all requirements. The new required form (Form N-Liquid) is used by registrants to report certain breaches of the rule’s requirements.

The rule lays out numerous elements the SEC staff believes a liquidity risk management program should include, specifically:

- Assessment, management, and periodic review of a fund’s liquidity risk
- Classification of the liquidity of fund portfolio investments
- Determination of a highly liquid investment minimum
- Limitations on illiquid investments
- Board oversight
- Disclosure to shareholders on the operations and effectiveness of the LRM program

In the nearly two years since the rule was adopted, the SEC has issued regulatory guidance in the form of frequently asked questions (FAQs) and has amended the rule twice. Amendments include:

- Eliminating a pending requirement for funds to publicly disclose the aggregate liquidity classification profile of their portfolios on a quarterly basis (using Form N-PORT)
- Amending Form N-1A to require a fund to discuss in its annual or semiannual report the operation and effectiveness of its LRM program
- Allowing a fund to report a single portfolio holding across multiple liquidity classification categories on Form N-PORT
- Requiring a fund to report holdings of cash and cash equivalents—information that is made public on a quarterly basis

Many firms have invested significant time and effort to prepare for the rule’s staggered compliance dates. Fund complexes with greater than $1 billion in assets under management (AUM) must comply with certain elements of the rule by December 1, 2018, with full compliance no later than June 1, 2019.

In our discussions with firms, as they have embarked on implementing the rule, a number of issues and concerns have emerged. Somewhat surprisingly, the first and foremost issue appears to be “ownership” of the rule and the required LRM program. Specifically, who within the firm is going to administer the program? While many see this rule as a compliance issue, the compliance function isn’t necessarily its natural home. Some parts of the rule clearly have a compliance element, such as monitoring the limit on illiquid securities. Also, ensuring overall compliance with the program might very well reside within the compliance function. However, administration of the program is another matter. Many firms seem to be going with a “cross-functional committee” approach, whether formal or informal, relying on the fact that the rule allows multiple people to administer the program.
A second common issue is how a fund’s securities will be bucketed. Some firms have their own methodologies for assessing liquidity that do not coincide with the rule’s four-bucket schema. Other firms are relying on outside vendors to provide liquidity enrichment data, yet remain skeptical about the accuracy of the data. Firms with multiple business lines (e.g., registered funds, offshore funds, and institutional accounts) that all use the same strategy may have a liquidity profile for a security that is different from the vendor data they are receiving.

Finally, many funds employ a sub-adviser to manage the investment portfolio, and some funds even have multiple sub-advisers within a single portfolio. Thus, determining who is best positioned to determine liquidity is a significant issue for the industry. The fund itself is responsible for creating the LRM program and filing information related to liquidity and is in the best position to know about inflows, outflows, and the characteristics of the fund’s shareholders. On the other hand, the firm managing the money is arguably in the best position to evaluate a security’s overall liquidity profile (considering investment fundamentals about the security, as well as the firm’s overall stake in that security).

Recent SEC guidance has provided the industry with some clarification by allowing funds to delegate responsibility for asset classification to sub-advisers. However, there is not a “one size fits all” approach, and ultimately funds retain the responsibility at all times for complying with the rule. The decision of who should facilitate the classification should be based on a discussion between the prime adviser/sponsor and the sub-adviser, in consideration of data availability, asset class specialization, and oversight processes.
Integrated risk management and compliance

Investment management firms operate in a complex, highly regulated business environment where margins are increasingly tight. As such, integrated risk management and compliance is paramount. Risk management functions should no longer be operating in isolation as a siloed second line of defense.

Integrating knowledge and increasing collaboration across the three lines of defense is enabled by improved access to shared intelligence between the lines-of-defense stakeholders, which in turn is enabled by technology. These forces are combining to drive greater efficiency and actionable intelligence at many firms. Enhanced coordination between risk management, compliance, and internal audit—along with insights from first-line functions (portfolio management, product development, trading, operations, etc.)—is making it possible for firms to ensure that all risks, including emerging risks, are contemplated, understood, and managed appropriately.

An enhanced risk and compliance operating model can help produce better business strategy, improved performance, and more cost-effective insights. It can also increase alignment with regulations and supervision of financial institutions, both of which promote integrated risk management and compliance as a way to protect capital.

It’s impossible to know with absolute certainty what risks and opportunities are around the corner, especially as firms continue to grow and expand. However, an integrated approach to risk management and compliance has the potential to create significant business value and more effectively support a firm’s overall business strategy.

Disruptive forces shaping the industry

Today, a number of trends are disrupting the investment management industry: changes in consumer preference; changes in the workforce (talent pool); and technology innovation. Changing consumer preference is driving down fees and margins, prompting firms to rethink their overall strategies and how they launch new products, evaluate distribution channels, manage and extend enterprise partnerships, and use technology to achieve their business goals. At the same time, firms are looking for new ways to attract and retain top talent in a changing workforce landscape. Last but not least, technology innovation is now a primary source of disruption. New and evolving technologies—such as robo-advisers, artificial intelligence, and advanced analytics—can create value and competitive advantage by generating alpha. They can also boost operating efficiency, enabling firms to do more with less. On the flip side, a recent study found that cybersecurity risks and operational risks related to technology-enabled business transformation are two of the top three greatest challenges for investment management firms.19

Integrated risk management and compliance supported by governance, risk, and compliance (GRC) technology

The recent global regulatory landscape continues to hold firms increasingly accountable for managing risks, particularly risks related to sales practices; changes in regulatory policy; data governance and privacy; and oversight of third-party providers. Designing an integrated risk and compliance operating model provides businesses with a practical approach both for managing risks and for taking smart risks that support the overall business strategy. Such an operating model starts with a governance structure that brings a cross-section of business leaders together to collaborate and vet the company’s risk profile and risk landscape. The operating model then harnesses the necessary resources (including people, processes, data, and technology) to support identification, management, and reporting of risks—and to support a more effective control environment.

For example, a growing number of firms are now moving beyond traditional risk committee meetings in which stakeholders from various lines of defense discuss risks using a conversational “issue by issue” approach. Instead, these firms are starting to use those same meeting times to view culminated risk and issues trends, examining the impact through a variety of lenses. Comparisons are made between different points of view, which are based on common definitions and themes (e.g., regulatory view, organization/function view, product view). Within each theme, discussions drill down into individual issues, before rolling back up to the level of business strategy, execution and overall risk appetite. This “next generation” risk committee meeting is enabled by GRC platform technology, which provides the foundation for multiple GRC applications used throughout the lines of defense to automate workflows.

Another example, which involves chief compliance officers and their duty to ensure regulatory compliance, illustrates the rapidly evolving capabilities of GRC platform technology. Today, a single GRC app can be used to capture external regulatory alerts; assess the alerts’ risk; and link to an obligations library, which is further linked to related policies that trigger tasks for policy authors to update policies and standards. The refreshed policies and standards are then pushed out to the organization. Also, to cross-pollinate useful data, the policies and standards are
linked to controls that are used by control assurance activities and internal audit. At a minimum, applying this discipline satisfies effective practices to monitor and manage the regulatory environment.

Regulatory exam management is a recent extension on several GRC platforms.

**Next steps**

Many firms are deploying—or have already deployed—an integrated risk and compliance operating model on one or two integrated risk management technology platforms. Now, they are focusing on accelerating new insights and efficiencies to gain the expected benefits from their transformation investments. These firms can further benefit by exploring additional integration with surveillance-level tools and content feeds and by leveraging some of the newest digital tools to generate richer insights from data. A key early step in preparing to expand existing capabilities is to create a blueprint of data and architectures to add to the current program. For instance, three core infrastructure elements to consider adding are: (1) managed cloud and/or internal data platforms containing data lakes to support both structured and unstructured data; (2) cognitive tools; and (3) business intelligence-layer tools.

Other firms that are still operating with primarily manual methods have an opportunity to evaluate and select the latest integrated risk and compliance platforms. Firms should look for vendors that specialize in providing platform-level common referential language and taxonomies that are solid and scalable, as well as interrelated and used for rich contextual outputs once their applications are used to automate functions/workflows in the lines of defense.

Firms that are just getting started can begin by identifying executive management sponsors and defining a program mission and objectives. They can then start to organize their data and identify simple use cases for automating manual functions with platform applications. Common focal points include: (1) centralized issue/action management, and (2) risk assessments in a few key areas—or entire functions such as internal audit, operational risk, or compliance—to demonstrate value.

Whichever stage a firm is currently in, frequent review of the target operating model and rate of progress toward it—including identification of quantifiable benefits gained along the way—is crucial for building and maintaining positive momentum within the organization’s risk management culture. This review should include a specific look at (1) the program management office structure, activities, and governance; (2) evolution of the data model; (3) and technology adoption across the lines of defense. All of these elements are very important to help achieve success of the program.
We continue to see global interest across jurisdictions in advancing a conduct and culture agenda. This suggests that conduct risk is an issue that is likely here to stay. Outside the United States, there has been a general shift from approaches that are pragmatic and principles-based to approaches that are more rules-based (such as Market Abuse Regulation and Markets in Financial Instruments Directive [MiFID II]).

As a concept, conduct risk has taken on greater meaning since the financial crisis. Ten years ago, “business practices” and “conduct” started becoming more prominent topics. Five years ago, firms began establishing frameworks to identify, manage, and monitor conduct as a new dimension of risk. Today, numerous industries are coming to terms with how to proactively prevent employee misconduct and manage company culture.

**Key trends**

**Enterprise view of conduct risk.**
Large US institutions are expected to have an enterprise-wide conduct risk management program and an enterprise-wide conduct risk function. The regulatory focus is on: (1) continuous monitoring of conduct and improvement and (2) detection and prevention mechanisms to influence how strategic objectives are being achieved.

The traditional focus on employee conduct is converging with a newer focus on market conduct, business practices, and impact on clients and markets. Also, there is significant focus on development of internal controls, creating a need to rationalize activities in order to efficiently manage the program. This may lead to some realignment of supervisory/surveillance activities.

**Analytics and predictive intelligence applied to conduct and culture.**
Firms are looking to generate meaningful insights on employee conduct for the board, senior management, and regulators. The ability to predict and prevent employee misconduct is a business imperative across institutional, retail, and wealth management sectors. Firms are looking to identify employees with poor conduct sooner; proactively identify the next population of at-risk employees and activities; and develop improved approaches for heightened supervision and targeted surveillance/monitoring.

**Challenges and opportunities from emerging technologies.**
Technology continues to disrupt how firms engage, deliver, monitor, and interact with customers. As a disruptor, technology gives rise to new business practices that can lead to new or increased conduct risks and challenges (e.g., digital banking, robo-advisers, electronic/algorithmic trading, new products such as bitcoin). However, it also creates opportunities to implement and refine controls that support sound conduct risk management (e.g., harnessing the increased availability of data to better predict—or more quickly detect—employee misconduct).

**Compensation and remuneration focus.**
This continues to be a significant area of attention for regulators. The Financial Stability Board (FSB) is planning to release recommendations on how firms can enhance their capacity to consider and monitor the effectiveness of compensation tools. The FSB’s recommendations will also likely highlight mechanisms for promoting good conduct and addressing misconduct risk. In Australia, the Banking Royal Commission reviewed a number of financial services institutions and identified remuneration as one of the root causes of misconduct.
The investment and wealth management industry is undergoing a transformation to harness the power of process-driven analytics capabilities and human insight to drive strategic and day-to-day decisions. As a result, investment and wealth managers are increasingly using models to enhance the speed and accuracy of their decision-making processes. Although models have historically been associated with facilitating investment decisions (e.g., quantitative strategies and asset allocation), the drive to enhance decisions and manage risk has led to increased model usage across several functions and processes, including digital investment advice, customized performance analysis and benchmarking, algorithmic trading, risk management, and human resources (e.g., employee screening).

**Regulatory scrutiny is intensifying**

Although many models in the industry have become very sophisticated, the processes for managing models are often not. In response to several high-stakes failures involving models—as well as new regulations that have required the development of models (e.g., the Liquidity Rule)—the SEC’s Office of Compliance Inspections and Examinations (OCIE) has increased its regulatory focus on the use of models. For example, the SEC’s routine examination questionnaires now include detailed questions and requests for information on registered investment adviser (RIA) model usage. The SEC has also started having technologists and quantitative specialists accompany examination staff during exams to test whether an RIA’s quantitative models and algorithms operate as described by disclosures and to probe whether they will likely continue to do so in various market environments. In addition, the SEC recently announced several mutual fund regulatory exam initiatives that may involve the use of models across key functions, including investments, compliance, and risk management. Focus areas include reliance on custom-built indices by index funds, aberrational performance in mutual funds vis-à-vis peer groups, allocations involving securitized products, and side-by-side management.

Another focus area for both the SEC and FINRA is the growing importance of digital investment advice tools that heavily rely on models to produce investment recommendations. For example, FINRA noted that firms are obligated to govern and supervise the models used in digital-advice tools and to assess whether a digital advice model is consistent with obligations to provide suitable investment advice. Similarly, with regard to investment advisers that offer digital investment tools, products, or services (e.g., robo-advice), the SEC noted that firms are required to adopt compliance programs—including relevant policies and procedures—tailored to address the unique risk exposures that models pose to their business.

Many organizations are still wrestling with these questions while struggling to implement a comprehensive program to manage model risk (e.g., the risk of economic and financial loss, harm to clients, erroneous financial statements, improper managerial decisions, or reputation damage from models that are poorly built, used, or controlled). For now, many organizations are still wrestling with these questions while struggling to implement a comprehensive program to manage model risk (e.g., the risk of economic and financial loss, harm to clients, erroneous financial statements, improper managerial decisions, or reputation damage from models that are poorly built, used, or controlled).

**Defining “model” in investment management**

In the investment and wealth management sector, a standard definition for the term “model” has yet to formally emerge. However, in our experience, many firms begin with the definition provided by regulatory guidance from banking and securities regulators (Office of the Comptroller of the Currency 2011-12/Federal Reserve Board SR 11-7, SEC Release No. 34-81485), which defines a “model” as “a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.” Investment and wealth managers then tailor the definition to align with their model-use environment. For example, organizations with heavy robo/algorithmic trading platforms might tailor the definition to highlight those specific technologies.

**Model risk management**

To mitigate the potential adverse impact of the model-use environment, MRM has emerged as a discipline of risk management that provides a structured approach that defines roles, responsibilities, policies, procedures, and controls to mitigate model risk. In this context, MRM helps to define the shared roles, responsibilities, and accountabilities (including decision rights) across the three lines of defense. Also, it facilitates development of an effective control environment,
including policies, procedures, and corollary/complementary controls. Although MRM activities should be tailored for each organization’s model-use environment and risk appetite, there are a number of recognized leading practices for the design and implementation of critical MRM framework elements (figure 2).

As a starting point, investment managers should consider first identifying and analyzing their current MRM practices to uncover enhancement opportunities and determine where they need to expand their efforts to capture all the relevant models used throughout the business.

**Common challenges with managing model risk**

Although organizations may already have some foundational elements of MRM leading practices in place, they often face several common challenges in lowering their model-related risk profile (figure 3).

These challenges and risks can be mitigated through the design and implementation of a robust MRM framework.

---

**Figure 2. Critical elements for MRM**

**Board of directors**
- Ultimate responsibility
- Remains apprised of key events

**MRM committee**
- Oversees MRM activities
- Informs board of directors

**Internal audit**
- (Third line of defense)
- Holistic MRM program focus

**GOVERNANCE AND OVERSIGHT**

- Development and implementation
- (First line of defense)
- Validation
- (Second line of defense)
- Use and ongoing monitoring

**Operating environment**
- Policies and procedures
- Model definition
- Use of vendors
- Inventory and attestation
- Independence
- Resources demands
- Model risk-rating
- Risk aggregation
- Data consistency
- Technology
- Disaster recovery
- Reporting and analytics
- Roles and responsibilities
- Regulatory interpretation
- Stakeholder credentials
- Change control/security
- Documentation

---

**Figure 3. Common challenges in MRM**

**Governance and policy development**
- Key stakeholders are not involved
- Lack of understanding around individual model failure consequences
- No adherence to formal policies/procedures

**Model life cycle and workflow challenges**
- Poor quality of ongoing monitoring plans
- Lack of rigorous vendor model testing
- Limited understanding of interconnectedness with other models

**Documentation challenges**
- Poor quality of model documentation
- Inadequate investor and regulatory disclosures

Model risk at organizations is significantly increased where second and third line of defense functions rely on the output of models that have not been properly developed, validated, and documented.
Where to start
With so many areas to focus on, creating an MRM program can seem overwhelming. Here are some leading practices to consider when getting started:

• Define what a model means to your organization, leveraging lessons learned from the banking and securities sectors
• Establish a well-defined governance structure to oversee model usage, including roles, responsibilities, and decision rights
• Undertake an initiative to identify, inventory, and risk-rank the relevant models that are used across the enterprise
• Establish a consistent process for developing and implementing models, including standard procedures for vendor-purchased models (particularly high-risk models) to promote consistent performance against expectations
• Confirm model outcomes against expectations by establishing ongoing monitoring requirements
• Review investor and regulatory disclosures to align them with expected model usage, outcomes, and risks

Although there is no “one size fits all” MRM framework, investment and wealth managers interested in establishing an MRM framework should consider involving stakeholders from across the organization to discuss the underlying factors of model risk, including the nature, number, and riskiness of existing models, as well as the effectiveness of the existing control environment.

MRM maturity is a continuous spectrum (figure 4). Depending on their model-use environment—and degree of existing MRM activities (formal or informal)—investment and wealth managers can establish a plan and road map to achieve an MRM program that best fits their business needs and risk appetite.

A well-managed MRM program can help reduce the risk of errors that could lead to economic and monetary loss. The result? More effective and efficient decision inputs—and more effective and efficient decisions that drive competitive advantage and enhance an investment and wealth manager’s reputational resiliency.

Figure 4. Illustrative MRM program maturity matrix

<table>
<thead>
<tr>
<th>ELEMENT OF MRM</th>
<th>Basic MRM “Table stakes”</th>
<th>More advanced MRM “Leading the industry”</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOVERNANCE, POLICIES, AND CONTROLS</td>
<td>• MRM policy • Model definition • Risk-rated inventory</td>
<td>• Development and validation procedures • Documentation templates • Reporting and analytics cadence • Aggregation of model risk • Broader set of procedures (i.e., interconnectedness; monitoring) • Technology/automation</td>
</tr>
<tr>
<td>DEVELOPMENT, IMPLEMENTATION, AND USE</td>
<td>• Execution of development, procedures for new models using standard templates</td>
<td>• Application of procedures/templates for legacy models • Ongoing monitoring • Real-time calibration • More sophisticated modeling (ML/AI)</td>
</tr>
<tr>
<td>MODEL VALIDATION PROCESS</td>
<td>• Validation of critical models</td>
<td>• Validation of broader model inventory/queue • Adjacent validation activities • Use of auto-testing/validation technology • Streamlined validations</td>
</tr>
</tbody>
</table>
At many investment management firms, the maturity and sophistication of their operational risk capabilities have not kept pace with the rapidly increasing sophistication and complexity of their business environment. This capability gap exposes firms to a wide range of risks, from business disruptions and cyberattacks to reporting anomalies and regulatory fines. And while investment managers have traditionally not received the same level of regulatory scrutiny as their peers in banking, operational risk in the investment management industry is an area likely to receive significantly more attention in the future.

Key drivers
Trends and market forces driving the increased focus on operational risk include:

- **Pressure to improve efficiency and do more with less.** Investment managers focus a lot of time, money, and resources on risk management and compliance. Yet many of those resources end up focusing on data collection and manual processing instead of risk decisioning and analysis. Improved risk management can reduce operational risk while also improving efficiency, enabling organizations to allocate resources toward higher-value activities.

- **A need to quantify risk and generate actionable insights.** Investment managers generally understand the importance of managing operational risk; however, in most cases they just don’t have the right data to take action. Existing data are either too high level and generic to provide useful insights, or too detailed to comprehend. In both cases, the net result is the status quo.

- **A challenge in addressing an evolving risk landscape.** In addition to dealing with traditional risks such as business continuity and IT risks, investment managers now face challenges and risks that were nonexistent or relatively insignificant just a few years ago. These include everything from the growing risk of cyberattacks and the need to protect data privacy, to the legal and reputational risks associated with chatbots and artificial intelligence.

**Leading practices**
When tackling the challenge of holistic operational risk management, there are a number of leading practices that companies should consider.

- **Make risk management an integral part of the business, not an afterthought.** Weave risk management into your firm’s business strategy, day-to-day operating processes, and organizational culture. Managing operational risk is everyone’s responsibility, not something solely relegated to the second and third lines of defense.

- **View risk holistically.** Don’t just focus on individual types of risk in silos, which is often a result of a more functional breakdown of risk with a lack of coordination. Think about how all of your firm’s risks fit together; then develop integrated processes and systems that can help you effectively tackle the entire risk challenge.

- **Give risk management a seat at the executive table.** Designate a chief risk officer or other representative to ensure the risk function’s perspective is included in every C-suite discussion. Risk organizations suffer without clear accountability.

- **Get the business involved early and often.** Work side by side with the business to develop controls and risk management capabilities in the first line of defense. Getting the business involved improves risk acumen enterprise-wide, creates a sense of collective ownership, and helps make risk management part of your corporate culture.

- **Develop a risk taxonomy to define and prioritize risks.** Clearly identify and define the risks facing your business, and then determine which ones are most critical to success.

- **Determine your firm’s risk appetite and risk thresholds.** Work with the board and risk governing bodies to explicitly determine your firm’s appetite for risk, and then establish specific thresholds for operating within those boundaries. When determining risk appetite, firms can start with identifying what their key business processes are and then identify the risks related to them.

- **Get the right technology tools.** Integrated GRC platforms and other technology tools can help identify and quantify risk in a consistent way across the enterprise.

**Taking action**
Adopting robust practices and tools is a key to improvement; however, they don’t add much value unless you act on the resulting insights. Proactively addressing your operational risks can help reduce the risk of business disruption, cyberattacks, and regulatory penalties. With the business environment growing more complex every day and our dependency on data increasing, the need for effective risk management has never been greater.
Best interest rules

Although the Department of Labor Fiduciary Rule was vacated in 2018, there continues to be a strong and consistent regulatory focus on conflicts of interest in the retail wealth management industry. This is illustrated by the SEC’s Regulation Best Interest rule proposal, FINRA’s proposal around “quantitative suitability,” and the variety of state securities regulators who have proposed or passed their own rules that mandate a best interest or fiduciary standard. While all of these rules, if adopted and enforced, could potentially create a complex web of differing standards that would require compliance, it remains to be seen which ones will become reality—and to what extent they will affect how business is actually done. What is clear, however, is that the focus on conflicts of interest (and sales practices that emanate from them) will not be going away anytime soon.

The continued focus on conflicts—in addition to the ongoing shift from brokerage models to fee-based advisory programs, increased pressure on pricing and fees, and burdensome financial advisor (FA) workloads to meet regulatory obligations—is causing many organizations to rethink how they supervise and oversee FAs and their businesses. The convergence of all these pressures at a moment when the stances of many regulators has softened provides a unique opportunity to recalibrate and holistically transform how supervision is done. Organizations now have a chance to prepare for where their businesses will be in the next 5–10 years. Wealth management organizations should use this opportunity to rethink how they perform their supervisory and oversight functions, with a focus on:

- Holistic supervision of FA activities that is client- and portfolio-centric, rather than account- and transaction-centric
- Analytics and reporting tools that combine client, FA, branch, and region data to provide the required holistic view
- Increasing the efficiency and effectiveness by which regulatory compliance can be evidenced
- Use of data and analytics to detect emerging supervisory issues
- Use of automation to replace manual work on a large scale, while improving the effectiveness of supervision programs
- Deployment of new tools that increase financial advisers’ productivity and empower them to serve investors better
Cryp\textsuperscript{t}ocurrency

Cryptocurrency is a hot topic that is generating a lot of excitement—but also a lot of confusion and uncertainty. At the moment, some early adopters are betting on cryptocurrency’s potential upside as a disruptive innovation and are not necessarily subjecting it to the same level of scrutiny and rigor as other more established asset classes—particularly as regulators and legislators in the United States and around the world struggle to get their arms around the subject. However, for cryptocurrency to gain widespread acceptance, it will eventually need to comply with similar regulatory standards as traditional asset types.

What is cryptocurrency?
Cryptocurrency does not currently have a universally accepted definition. Adding to the confusion, terms are often used interchangeably (e.g., cryptocurrency, virtual currency, digital currency, digital tokens, digital assets). The term generally used by US regulators (Financial Crimes Enforcement Network [FinCEN] and NYDFS) is virtual currency, but digital assets also include tokens that are regulated as securities, commodities, or utilities.

In general, the term can be used to describe a medium of exchange, an investment product, a technology, or an emerging economic sector. For the purposes of this article, it refers to the investment product or asset class.

The purpose and method of distribution of a particular token will largely determine who regulates it—and how. In the United States, four different regulators have different perspectives. The SEC generally views tokens issued for funding as securities, but does not consider bitcoin and similarly designed tokens to be securities. The Internal Revenue Service views cryptocurrencies as taxable property; FinCEN views them as a currency equivalent; and the CFTC views it as a commodity.

As an aside, it is important to note that while blockchain is the underlying software innovation (distributed ledger technology) that makes bitcoin possible, it is by no means limited to bitcoin. Rather, blockchain technology is a broadly applicable innovation that is increasingly being used for a wide range of applications not related to cryptocurrency, including everything from digital IDs and digital voting to copyright protection, data sharing, and title transfers for vehicles and real estate.

Regulating cryptocurrency
In order for cryptocurrency to gain widespread acceptance as a mainstream asset class—not just a speculative investment and disruptive innovation—it will likely need to satisfy the standard requirements of a recognized and regulated asset class, such as:

- Liquidity (ability to get your money out)
- Market infrastructure (e.g., regulated exchanges; transfer agents; custodians)
- Operational resiliency, including cybersecurity
- Customer protection/suitability and fraud protections

Lawmakers and regulators in the United States and abroad are struggling to decide whether cryptocurrency is truly a new kind of asset, or simply a variation on an asset class that already exists (and thus subject to existing regulations). In most cases, particularly in the United States, the latter view seems to be the default. For example, the SEC has recently taken a strong stance that some “initial coin offerings” (ICOs) are actually securities offerings and need to be regulated as such.

This has sharply curtailed the volume of ICOs and steered entrepreneurs toward issuing “tokenized securities” in compliance with certain private placement exemptions available under federal securities law. Regulatory efforts to date have focused largely on exchanges through which cryptocurrencies are traded.

Despite the natural tendency to apply existing regulatory frameworks to cryptocurrency (e.g., treating exchanges as money service businesses subject to federal registration and state licensing requirements), a number of regulatory bodies outside the United States are moving aggressively to implement comprehensive and prudential regulatory frameworks intended to foster a supportive business environment for innovation. Several nations (including Switzerland, Singapore, Malta, Bermuda, and Liechtenstein) have actively recognized and embraced cryptocurrency in an attempt to attract innovation and investment by providing greater regulatory clarity. Other nations, however, remain in wait-and-see mode—or are actively resisting cryptocurrency as being too risky. In the meantime, the Financial Action Task Force (FATF) is expected to release binding international standards for cryptocurrency in June 2019, which may help level the playing field globally from an anti–money laundering perspective.

In the United States, the evolution of the cryptocurrency space is complicated by the dual systems of federal and state regulation. For example, cryptocurrency exchanges are generally classified as money service businesses, requiring federal registration and state licensing, which impose numerous regulatory requirements with respect to consumer protection, anti–money laundering, and cybersecurity, among other things. NYDFS has been the most
proactive on this issue, offering virtual currency licenses (aka “BitLicenses”) to help legitimize and regulate exchanges; however, the results to date have been mixed, with many prospective licensees viewing the state’s requirements as too proscriptive.

The Conference of State Bank Supervisors (CSBS) formed the CSBS Emerging Payments Task Force to examine and identify areas for consistent regulatory approaches among states, which led to the CBS Model Regulatory Framework to help harmonize regulation among states.28 Similarly, the Uniform Law Commission issued the Regulation of Virtual-Currency Businesses Act, which provides a statutory framework for the regulation of companies engaging in “virtual-currency business activity.”29

Looking ahead
The rapidly evolving cryptocurrency space is beginning to see greater interest from professional investors, despite concerns over risk of hacking and regulatory uncertainty. However, there have been several recent developments with individual companies and stock exchanges announcing trading platforms and exchanges. These developments provide an instant boost to the credibility of cryptocurrency. As such developments provide a stamp of legitimacy for digital assets and make them generally more accessible to investors, lawmakers and regulators may be prompted to move from thinking/studying to taking decisive action. Despite clear signs that cryptocurrency is maturing, at the moment the market remains highly dynamic and uncertain—generating more questions than answers. Firms should closely monitor the domestic and global regulatory landscape for new and emerging trends that could inform and shape their business strategies in this ever-evolving but increasingly important area.
Taking the lead in times of change

Today's regulatory environment is in the midst of significant and unpredictable change, driven by a variety of forces including political shifts, new social norms and behaviors, and technological innovation. To succeed in this challenging environment, companies need to actively look for ways to improve the effectiveness and efficiency of their compliance strategies and operations. Technology is likely to play an increasingly important role in this pursuit. Robotic process automation, for example, is being widely adopted by compliance-related functions to help them do more with less. At the same time, emerging technologies such as artificial intelligence and advanced analytics are making it possible to do things that have never been done before. Innovations like these can create business value no matter which way the regulatory winds might shift—enabling leaders to take action confidently and decisively in times of significant and ongoing change.


4. Ibid., p. 8.

5. Ibid., p. 10.


20. “Surveillance-level tools” are defined as point solutions operating in the first line of defense that are fit for the purpose of monitoring specific risks or incidents.


Contacts

**Leadership**

Monica O’Reilly  
Regulatory & Operational Risk Leader  
Principal | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
omoreilly@deloitte.com

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

Chris Spoth  
Executive Director, Center for Regulatory Strategy, Americas  
Managing Director | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
cspoth@deloitte.com

**Authors**

Mike Brodsky  
Managing Director | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
mbrodsky@deloitte.com

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

Clifford Goss  
Principal | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
cgoss@deloitte.com

Mark Hornbrook  
Managing Director | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
mhornbrook@deloitte.com

Brian Merrill  
Managing Director | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
bmerrill@deloitte.com

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

Peter Poulin  
Principal | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
pepoulin@deloitte.com

Prakash Santhana  
Managing Director | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
psanthana@deloitte.com

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

Alexi von Keszycki  
Managing Director | Deloitte Risk and Financial Advisory  
Deloitte & Touche LLP  
avonkeszycki@deloitte.com

The Center wishes to thank the following Deloitte professionals for their insights, contributions, and support to this report:

Antonio Crombie, Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Kristen Gantt, Independent contractor to Deloitte & Touche LLP
Marin Knight, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Mary Obasi, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Shumona Roy, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Joshua Uhl, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
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.