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 capital markets 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>Conduct risk</td>
<td>8</td>
</tr>
<tr>
<td>LIBOR transition</td>
<td>9</td>
</tr>
<tr>
<td>Uncleared margin rules: Initial margin</td>
<td>12</td>
</tr>
<tr>
<td>Qualified financial contracts</td>
<td>14</td>
</tr>
<tr>
<td>Advanced technology for compliance</td>
<td>16</td>
</tr>
<tr>
<td>Liquidity</td>
<td>19</td>
</tr>
<tr>
<td>Best interest rules</td>
<td>21</td>
</tr>
<tr>
<td>Cybersecurity and privacy</td>
<td>22</td>
</tr>
<tr>
<td>Cryptocurrency</td>
<td>26</td>
</tr>
<tr>
<td>Consolidated Audit Trail (CAT)</td>
<td>28</td>
</tr>
<tr>
<td><strong>Taking the lead in times of change</strong></td>
<td>30</td>
</tr>
<tr>
<td>Endnotes</td>
<td>32</td>
</tr>
<tr>
<td>Contacts</td>
<td>33</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.

---


5 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.6

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.

---

**David Strachan**  
Centre for Regulatory Strategy, EMEA  
Deloitte UK

**Kevin Nixon**  
Centre for Regulatory Strategy, APAC  
Deloitte Australia

**Chris Spoth**  
Center for Regulatory Strategy, Americas  
Deloitte US
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 Banking Committee has indicated that it will continue to focus its legislative agenda on remaining refinements not already addressed in the Economic Growth, Regulatory Relief, and Consumer Protection Act (EGRRCPA) 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, capital markets organizations should continue to drive effectiveness and efficiencies across their risk and compliance programs so they can meet applicable laws, regulations, and supervisory expectations.
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 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 \(^2\) and Markets in Financial Instruments Directive [MiFID II] \(^3\)).

Within the United States, the Federal Reserve Bank (FRB) is most active around conduct in the capital markets space. The FRB Board of Governors is executing horizontal exams via its Large Institution Supervision Coordinating Committee (LISCC), with a focus on how firms are addressing business conduct and compliance risk, and on firms’ capabilities related to detection and prevention of misconduct. \(^4\)

As a concept, conduct risk has taken on greater meaning since the financial crisis. Ten years ago, “business practices” and “conduct” started becoming a more prominent topic. 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 the related cultural implications.

**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 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 are also expected to 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. \(^5\)
On April 3, 2018, the New York Federal Reserve launched a benchmark US rate called the Secured Overnight Financing Rate (SOFR) to replace the US dollar London Interbank Offered Rate (LIBOR), which is one of the most significant reference rates used by financial markets.

As shown in figure 1, LIBOR impacts organizations in numerous ways. Most obvious are impacts that are “product-based,” such as LIBOR-based loans or interest rate swaps. However, LIBOR can also affect core operating processes, such as accounting, pricing, hedging, and asset-liability-management. Depending on the nature of an organization and its business environment, the extent of LIBOR’s impact can be significant.

For a diversified financial services organization, there are impacts across a range of wholesale and retail products including floating rate notes, structured products, and syndicated loans, as well as others such as adjustable rate mortgages, student loans, and auto loans that reference LIBOR in their pricing or payoff profile. However, financial services firms also need to consider LIBOR’s impact on products used for internal risk management purposes, not just those made available to customers. Hedges executed and managed by an organization’s treasury department are a good example.

### Figure 1. LIBOR impacts

<table>
<thead>
<tr>
<th>Products</th>
<th>Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Loans</strong> including syndications and mortgage servicing</td>
<td><strong>Product and client processes</strong></td>
</tr>
<tr>
<td><strong>Bonds</strong> (floating rate notes) and <strong>structured products</strong> (CMBS)</td>
<td>– New product and services design</td>
</tr>
<tr>
<td><strong>OTC and exchange traded derivatives</strong>—from simple/high-volume products (e.g., interest rate swaps) to more complex</td>
<td>– Sales, pricing, and booking/onboarding</td>
</tr>
<tr>
<td>– Financial instruments discounted with a curve bootstrapped from a LIBOR-linked swap</td>
<td>– Client negotiations and communication</td>
</tr>
<tr>
<td>– Financial instruments discounted with curves that include cross-currency basis</td>
<td><strong>Accounting, valuation, tax, and risk management</strong></td>
</tr>
<tr>
<td><strong>Deposits</strong> linked to LIBOR</td>
<td>– Accounting and valuation policies, procedures and controls including hedge effectiveness</td>
</tr>
<tr>
<td><strong>Securities issued</strong> and other borrowing</td>
<td>– Model development and maintenance</td>
</tr>
<tr>
<td><strong>Interest rate/currency hedges</strong> managed by Treasury</td>
<td>– FV changes will impact direct/indirect taxes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Systems</th>
<th>Reports/models</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Loans</strong>—the landscape of loan systems and warehouses is often very broad and complex:</td>
<td><strong>Regulatory reporting</strong> (e.g., 2052a, FR Y-14M/Q/A, FFIEC 102)</td>
</tr>
<tr>
<td>– Origination/onboarding/pricing</td>
<td><strong>SEC reporting</strong> (quantitative and qualitative inputs for 10K and 10Q)</td>
</tr>
<tr>
<td>– Systems of records</td>
<td><strong>Risk reporting</strong> (Board and management reporting of interest rate sensitivities, market risk, etc.)</td>
</tr>
<tr>
<td>– Warehouses</td>
<td><strong>Models</strong></td>
</tr>
<tr>
<td><strong>Derivatives, trading, and securities</strong></td>
<td>– Valuation/hedging models</td>
</tr>
<tr>
<td>– SORs/booking</td>
<td>– Market risk models</td>
</tr>
<tr>
<td>– Warehouses</td>
<td>– Counterparty credit risk models</td>
</tr>
<tr>
<td>– Others: Collateral management, valuation</td>
<td>– ALM/transfer pricing/cost of funds</td>
</tr>
<tr>
<td><strong>Deposits</strong></td>
<td><strong>Collateral management</strong> (collateral disputes and resolution)</td>
</tr>
<tr>
<td><strong>Treasury</strong></td>
<td><strong>Legal</strong> (contracts, fallback provisions)</td>
</tr>
</tbody>
</table>

**Figure 1. LIBOR impacts**

**Systems**
- Loans—the landscape of loan systems and warehouses is often very broad and complex:
  - Origination/onboarding/pricing
  - Systems of records
  - Warehouses
- Derivatives, trading, and securities
  - SORs/booking
  - Warehouses
  - Others: Collateral management, valuation
- Deposits
- Treasury

**Processes**
- Product and client processes
  - New product and services design
  - Sales, pricing, and booking/onboarding
  - Client negotiations and communication
- Accounting, valuation, tax, and risk management
  - Accounting and valuation policies, procedures and controls including hedge effectiveness
  - Model development and maintenance
  - FV changes will impact direct/indirect taxes
- Legal (contracts, fallback provisions)
- Reporting (transformation logic, manual processes, controls)
- Collateral management (collateral disputes and resolution)

**Reports/models**
- Regulatory reporting (e.g., 2052a, FR Y-14M/Q/A, FFIEC 102)
- SEC reporting (quantitative and qualitative inputs for 10K and 10Q)
- Risk reporting (Board and management reporting of interest rate sensitivities, market risk, etc.)
- Models
  - Valuation/hedging models
  - Market risk models
  - Counterparty credit risk models
  - ALM/transfer pricing/cost of funds
To facilitate their operating processes and the valuation of financial instruments, many organizations have embedded LIBOR into their technological platforms—including data feeds, system networks, and engines. In addition, LIBOR can have an indirect impact on broader processes such as modeling, reporting, and analytics.

The LIBOR transition consists of four stages—three sequential stages, and one stage that occurs in parallel with the others (figure 2).

To ease the transition, many organizations have started to consider how to develop the right strategy, define the appropriate scope, and effectively execute the LIBOR transition program, while at the same time considering the potential impacts on the firm’s processes and controls, accounting and reporting capabilities, and overall risk profile. In 2019, many of the transition activities determined as part of the initial impact analysis will start to be actioned. These implementation activities will continue well into 2019 and 2020.

For more detailed information on LIBOR transition, read the recent paper from the Deloitte Global Center for Regulatory Strategy, “LIBOR transition: Setting up your firm for success.”

---

**Figure 2. The transition to LIBOR**

- **Identify and inventory exposure**
  - Perform an initial analysis
  - Identify/validate LIBOR-linked exposures
  - Determine impacted processes
  - Design the transition program

- **Plan and implement the transition of benchmark rates**
  - Products
  - Process
  - System and data feeds
  - Legal
  - Assets and liabilities
  - Regulatory
  - Accounting
  - Reporting

- **Decommission LIBOR**
  - Physical removal of LIBOR form:
    - Systems and feeds
    - Processes
    - Policies
    - Procedures
    - Client docs
    - Training material
    - Other
  - Transition implementation documentation archival

---

**Parallel analysis and transition monitoring**
Leading in times of change Capital markets regulatory outlook 2019

Alternative reference rate

The world’s most-referenced financial benchmark—LIBOR—is likely to be discontinued by 2021. In preparation, financial institutions and regulators around the world are developing alternate rates such as SOFR, SONIA (Sterling Overnight Index Average), TONAR (Tokyo Overnight Average Rate), SARON (Swiss Average Rate Overnight), and EONIA (Euro Overnight Index Average).

This alphabet soup of alternate reference rates will increase complexity for financial institutions operating globally, since the various rates are not uniform in terms of their underlying references, stages of implementation, and whether they are secured or unsecured. Early phases of the transition will likely be especially challenging.

Case in point: Determining how best to apply nearly risk-free rates to lending products that ideally should reflect reference rates with a credit risk component, similar to LIBOR now. For example, a key issue with SOFR is the absence of credit risk, since it is based on secured transactions. This limitation will force stakeholders of legacy loans to try and account for the credit spread between LIBOR and SOFR, which could be challenging—especially when LIBOR is no longer published.

Before the alternate reference rates can be adopted, a robust term-rates market needs to exist for most financial transactions. In the United States, SOFR futures could be a prerequisite for making a successful transition from LIBOR. Also, while documentation citing these alternate rates is beginning to take hold for new financial contracts, revising the language for legacy contracts could be one of the thorniest challenges.

Another issue specifically for the SOFR market is that trading is currently quite thin. While it is expected that the market will eventually develop and become more liquid, which may create trading opportunities, the future is still unknown and there may not be enough historical data to support modeling analysis for prepayment, default, or the like. This could result in the need for more frequent monitoring and testing of the markets to update a firm’s analysis.

Separately, the use of a new reference rate could introduce additional issues with interest rate risk such as basis risk, reinvestment risk, and market risk.
Uncleared margin rules: Initial margin

Following the financial crisis, the Basel Committee on Banking Supervision (BCBS) and the International Organization of Securities Commissions (IOSCO) created an initiative to establish global requirements for margining of non-cleared over-the-counter (OTC) derivatives. The rules are intended to reduce systemic risk by providing additional collateral that acts as a “buffer” to cover potential losses in a closeout scenario.

The initial margin (IM) rules apply to market participants that, together with their affiliates, have material holdings in OTC derivatives (notional holdings greater than $8 billion). Implementation of the IM rules is based on a phase-in schedule that starts with the largest firms and captures smaller firms each year. For 2019, firms with greater than $750 billion in notional holdings will be in scope; and for 2020, firms with greater than $800 billion in notional holdings will be in scope. There have been some recent papers submitted to the regulators requesting they review and increase the notional thresholds, and revisit the timelines in light of the clearing incentives and systemic risk that was originally intended for the IM rules.

While fewer than 50 counterparties were affected by earlier compliance dates in 2016, 2017, and 2018, industry bodies estimate that ultimately more than 1,000 market participants will be subject to the US regulations. Adequate planning is needed to ensure all moving parts are addressed for a smooth transition.

IM regulations will have a significant impact on the interactions between OTC swap counterparties, and on processes related to collateral posting. Firms will be required to:

- **Identify in-scope legal entities** and calculate legal entities’ aggregate average notional holdings to determine the correct implementation phase.
- **Identify impacted counterparties and custodians**, including any affiliates, and develop an outreach plan to repaper relevant agreements and schedules.
- **Determine and implement a methodology to calculate IM** that is acceptable under regulations; implement and exchange the initial margin; and develop an approach for counterparty dispute resolution, considering cross-border requirements.
- **Establish or update relationships with custodians** and implement new operational processes to segregate, post, and collect collateral by T+1 each day.
- **Contact and execute required agreements such as IM Credit Support Annexes (CSAs)**, control agreements, and custody agreements with counterparties and custodians, and build comprehensive contract life cycle management processes/tools.
- **Enhance systems/processes** and implement operational, technology, and data processes so that relevant data attributes can flow upstream and downstream and enable timely straight-through processing.

Firms implementing IM in the later phases (2019 and 2020) can leverage insights gained from earlier phases to address specific challenges, such as:

- **Identification of financial end users.** There are limited public reference data sources to support scoping of potential financial end users, both within a company and at counterparties.
- **Dual collateral and portfolio management.** Portfolios will likely include swaps that are subject to pre- and post-initial margin collateral arrangements. Operational processes will need to support multiple overlapping requirements, with sufficient reference data to segment swaps into categories that have not existed prior to regulatory IM requirements (e.g., legacy vs. in-scope, regulatory vs. nonregulatory IM).
- **Complexity of custodial arrangements.** Separate custodial accounts are required for posting and receiving IM. Each account will need to be opened at a custodian, subjected to relevant anti-money laundering (AML) and know-your-customer (KYC) processes, and then recorded in firm control accounts. According to relationship estimates, this could represent 37,000+ new accounts.
- **Lack of cross-border harmonization.** Portfolios may be governed by multiple jurisdictions, or regulators within a single country, with conflicting product rule sets.

Firms should act quickly to establish a broad program with key stakeholders; assess compliance dates; and draft, negotiate, implement, and test the various documents, models, and processes necessary to achieve compliance.
Qualified financial contracts

Qualified financial contract (QFC) recordkeeping rule
The DFA gives the Federal Deposit Insurance Corporation (FDIC) authority to take control of a failed financial company and make decisions regarding financial contracts with counterparties. The QFC recordkeeping rule requires that banks in the United States with over $50 billion in assets (and a sizable derivative portfolio) prepare details of all their financial transactions—information that can be provided to the resolution authorities in case of resolution, so it can make better-informed decisions. This is one of the last remaining DFA rules to help ensure orderly resolutions of financial companies in case of a crisis.

The recordkeeping rule will have a significant infrastructure impact on the largest banks, prompting them to capture all required QFC positions, collateral, and related contract information on a daily basis.

Key preparation activities:
- Identify and prioritize QFCs and related data (e.g., entities, counterparties, collateral, agreements).
- Capture and organize 200+ QFC-related data elements across products and business units, including position level data, collateral and netting, counterparties, and legal agreements/governing documents. Digitize information that is not in electronic format.
- Standardize, remediate, and structure QFC-related data in the defined reporting format.
- Establish an infrastructure and central repository for QFC positions and related data.
- Establish processes and capabilities for extraction, aggregation, reconciliation, and reporting.
- Roll out a production process for near real-time updates from multiple systems and data sources.

Ongoing activities:
- Update records daily (capturing previous end-of-day values, and up to five business days of history) in the specified format.

Firms should take action early to establish a broad program with key stakeholders, assess compliance dates, map the various sources of data necessary for generating the reports, resolve any existing gaps and issues, and then build out the infrastructure and straight-through processing necessary to produce the required near real-time reports.

Contract life cycle management
Many upcoming regulatory requirements—including the QFC recordkeeping rule, QFC stay rule, IM, LIBOR, and GDPR—revolve around repapering or extraction of information from contracts, creating the need for organizations to efficiently and effectively digitize and process contracts in addition to measuring, monitoring, and understanding the breadth and depth of their contracts.

In addition to digitizing existing contracts to comply with the regulatory rules, contract life cycle management (CLM) systems should be strongly considered to enable “straight-through” processing in near real-time—not only helping organizations comply with the new regulations in a timely manner and making BAU processes sustainable, but also generating powerful insights from contracts that can inform business strategy while paving the way for self-service and other operational and governance improvements. Many organizations have begun to look at streamlining contracts through the use of CLM tools in various parts of their organization while embarking on their enterprise digital journey.
QFC stay rule
The stay rule builds on DFA regulations by limiting counterparties’ termination rights to a global systemically important bank (GSIB) operating company in the event of a resolution and bankruptcy proceeding. Under the rule, GSIBs must amend their qualified financial contracts with counterparties, or they will not be eligible to trade or transact with those counterparties.

The goal is to reduce the risk of liquidity strain on the entity in resolution and to curb the domino effect that occurs across multiple counterparties/entities in a contract due to financial interconnectedness.

Complying with the stay rule will require significant effort for a bank to identify all of its existing financial contracts with counterparties and to understand and capture the detailed contract terms.

Key preparation activities:
• Identify and capture relevant QFC information (e.g., governing law, jurisdictions, products covered in the contract, default/cross-default provisions). Digitize information that is not in electronic format.
• Prioritize counterparties and financial contracts that need to be amended.
• Create a strategy to negotiate and establish applicable adherence methods—universal protocol, jurisdictional modular protocol, US protocol—with counterparties in different jurisdictions.
• Establish an approach for enhancing existing agreements with counterparties.
• Define a strategic operating model for managing financial contracts and ongoing compliance activities, including digitization of contracts, near real-time monitoring, and connectivity to various downstream systems.

Firms should mobilize resources early to establish a broad program with key stakeholders, assess specific compliance dates based on the type of counterparty, finalize the strategy for compliance (either through protocol adherence or bilateral negotiations), and establish the necessary technology and operational procedures to monitor and maintain compliance.
Advanced technology for compliance

The convergence of more than 20 years of AI research, improvements in big data, and massively increased computing power present considerable opportunities for improved regulatory compliance and risk management in the capital markets sector.

Compliance organizations typically find it challenging to keep pace with increasing internal changes and shrinking budget cycles, as well as external pressures to improve margins or increased demands from the regulators. However, future demands and expectations require a fundamental shift toward greater efficiency and effectiveness, enabling the compliance function to protect the business more effectively and deliver measurable business value.

Emerging use cases
Advanced technologies such as AI, natural language processing (NLP), and robotic process automation (RPA) are spurring innovation and improvement through a wide range of use cases in the business and legal domains.

### Business use cases
- Change management redefined
- Augmented reality
- Virtual assistants
- Chatbots
- Fraud detection
- Purchase prediction
- Recommendation engines
- Security surveillance
- Virtual personal assistants
- Online customer support

### Legal use cases
- e-Discovery
- Compliance/legal expert systems
- Legal research/chatbots
- Contract management/analytics
- Documents generation and workflows
- Matter intake/early case assessment
- Multijurisdictional compliance
- Foreign Corrupt Practices Act (FCPA) risk evaluation
- Litigation readiness/analysis
- M&A activity
Swap dealer capitalization

The Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) mandated that security-based swap dealers register with the US Securities and Exchange Commission (SEC), and that other swap dealers register with the Commodity Futures Trading Commission (CFTC). Both agencies have proposed—but not yet adopted—their own capital rules.

In March 2017, the CFTC reproposed its rule for comment. The CFTC reproposal incorporates (by reference) numerous sections of the rule that the SEC had proposed for comment in October 2012. Given this reliance on the SEC proposal, it is likely the SEC will need to adopt its own rule first before the CFTC can follow suit.

In October 2018, the SEC reopened the comment period for its proposal in order to “provide interested parties with an opportunity to submit comments that take into account regulatory and market developments since the publication of the proposals.” The reopening of the comment period can be seen as a signal that the SEC is preparing to move forward with its rule.

Both the SEC and CFTC proposals offer swap dealers alternatives about how they compute their regulatory capital. The most significant choice is whether a dealer should use standardized charges for market and credit risk, or apply to the agencies for permission to use its own quantitative models to compute those charges.

Many swap dealers have compared these charges and have generally found that, for dealers with a significant book of swaps, use of the standardized charges requires a much higher amount of capital. Thus, swap dealers in that position should, if they have not already done so, start preparing to apply for SEC and CFTC approval to use their own models.

Key technologies

Use cases for broker-dealers (BDs) are enabled by a number of innovative technologies that enable their compliance organizations to do more with less.

- **AI**—Programs that can interact, act, and understand. AI uses a broad array of technologies to mimic or extend human functions. To successfully deliver business value, AI requires a holistic approach that encompasses strategy, data, technology, people, and processes. AI can be deployed with humans “in the loop” or as part of fully automated solutions, and can be applied to a wide range of decisions.

- **NLP**—Software that processes any kind of human language. NLP enables computers to work with language and text similar to how humans do. This includes extracting meaning from text and creating readable text. NLP does not enable computers to fully understand text in the way humans do; however, it allows computers to manipulate text in highly sophisticated ways.

- **Machine learning (ML).** Algorithms that improve over time through exposure to more data. ML uses a diverse collection of methods to process data and extract meaningful information, enabling systems to get smarter as they are used.

- **Deep learning.** Subset of ML that uses neural networks and massive amounts of data. Deep learning uses multiple cascading layers of nonlinear processing units for feature extraction and transformation.
Enhanced capabilities in three strategic areas

Advanced technologies can be used individually or collectively to boost a compliance organization’s capabilities across the three strategic levers of risk, revenue, and cost.

Risk-related capabilities:

- **Proactive risk management.** Advanced monitoring of product portfolios for early risk detection and predictive risk modeling.
- **Holistic supervision.** The ability to bring together different compliance functions and connect the dots across compliance programs provides more clues to enhance the decision support process for supervision.
- **Improved accuracy.** Larger data sets combined with cutting-edge risk algorithms to identify nonlinear patterns.
- **Reduced human error.** Automation using technology and consistent process execution to make the risk function less prone to human error.

Revenue-related capabilities:

- **Cross-selling.** Proactive system triggers and front-line staff notifications to help identify and capitalize on cross-sell/up-sell opportunities.
- **Dynamic pricing.** Real-time adjustment of product pricing based on multivariables.
- **24/7 availability.** ML algorithms running around the clock; cognitive agents handling customer inquiries any time of the day.

Cost-related capabilities

- **Workforce management.** Predictive algorithms that enhance workforce staffing models and drive high full-time employee (FTE) utilization with minimal excess capacity.
- **Inventory management.** Enhanced procurement driven by enhanced inventory supply tracking and customer demand forecasting.
- **Technology optimization.** Rationalization of redundant systems and decreased data storage costs, driven by automated workflows.

Elevating the compliance function

Advanced technologies can improve efficiency by rationalizing line-of-defense execution and reducing the compliance organization’s dependence on human capital. Also, they can improve the decision support effectiveness by better leveraging consistent tools/processes and embedding compliance activities directly into business processes. In addition, they can make compliance activities more proactive and predictive through advanced analytics/reporting, as well as through targeted testing.

These enhanced capabilities enabled by technology can elevate the compliance function’s stature, helping it become the organization’s ethical voice as well as a source of sustained competitive advantage and business value.

Advanced technologies can improve efficiency by rationalizing line-of-defense execution and reducing the compliance organization’s dependence on human capital.
The regulatory landscape has significantly evolved over the past decade with new and updated regulations attempting to address the liquidity risk at BDs, swaps dealers, and futures commission merchants (FCM).

**Proposed FINRA Rule 4521 Supplemental Liquidity Schedule**

The proposed amendments introduce new liquidity events for which firms are required to notify Financial Industry Regulatory Authority (FINRA) within 48 hours. Proposed changes include a Supplementary Liquidity Schedule (SLS) related to specified financing transactions and other sources or uses of liquidity.

**Criteria for covered institutions.** The new requirements would apply to BDs with more than $25 million in free credit from their 15c3-3, and to BDs with more than $1 billion in secured lending on their balance sheets as reported on the monthly FOCUS report.

**Liquidity triggers.** FINRA proposed many new liquidity notifications for in-scope firms, including: (1) significant reduction to access of funding through repurchase or securities lending activities; (2) increased collateral haircuts from the BD’s largest counterparties; (3) reduction in access to funding from the BD’s largest counterparties; (4) reduction in lines of credit; and (5) trigger of a loan covenant.

The proposed regulation describes a formal process for reporting these triggers as part of the FOCUS report. However, discussions with FINRA have addressed the sensitivity and interpretation of a trigger that may not be a liquidity event but rather a change in a firm’s relationship. Many aspects of the liquidity triggers are in a contingency funding plan that may already require regulatory notification. Therefore, reporting such data on or around the 15th day could be redundant and may include stale data that would not support timely liquidity risk management.

**Liquidity reporting.** Attributes of the proposed SLS:

**Secured lending schedule:**
- Reverse repurchase/repurchase and securities lending activities
- Overnight, term, and weighted average maturity
- Underlying collateral class (US government securities; agency mortgaged backs; equities; corporate bonds and other)
- Detail of top five counterparty types by reverse repurchase/repurchase and securities lending activities

**Bank lending:**
- Committed versus uncommitted facilities
- Current utilization
- Term duration

**Other designated clearing organizations (DCO):**
- DCO margin requirements
- Box information
- Non-DCO cleared derivatives
Changes to capital and margin regimes for swap dealers (SDs) and security-based swap dealers (SBSDs)

The SEC and CFTC have proposed regulations that would impose capital and margin requirements on nonprudentially regulated SDs and SBSDs. The proposed regulations include liquidity requirements and a compliance regime.

In particular, SDs and SBSDs would be subject to a liquidity requirement in addition to a capital requirement—with the specific requirements possibly hinging on the regulator whose capital requirements they follow. Also, SDs and SBSDs may be subject to stress testing.

The liquidity requirements are designed to ensure a swap dealer holds an adequate level of highly liquid assets to meet its operating needs under stressed environments, and that it has a liquidity funding plan in place. The proposed rules may require significant tangential compliance requirements including regulatory reporting, attestation, and periodic review by senior management.

Municipal securities

The three federal banking agencies jointly released an interim final rule\(^1\) that amends their respective liquidity coverage ratio (LCR) rules to treat any municipal obligation that is both “liquid and readily marketable” and “investment grade” as a level 2B high-quality liquid asset (HQLA). The impact will likely be greatest at the BD level where many institutions hold municipal securities as part of their investment portfolios.

There might be additional benefits to the municipal bonds market itself as financial institutions seeking greater yield have a need to utilize qualifying securities for their liquidity buffer, which could create additional demand.

Institutions trying to leverage the new rule will face three significant challenges:

- Determining if there is proper Treasury control
- Properly categorizing securities for regulatory reporting
- Determining if each security meets the liquid and readily marketable requirements

These are difficult tasks to perform on more broadly known assets, and municipals pose an even greater challenge as the underwriting and market processes are different than the processes used for more standard assets used in a liquidity buffer, such as government securities, mortgage-backed securities, and publicly traded corporate bonds and equities.

What can firms do to get ready?

FINRA’s Guidance on Liquidity Risk Management highlights the need for BDs to review their respective liquidity conditions under possible stress events, and to develop and implement the appropriate governance frameworks and corresponding processes. The expressed purpose of the regulatory notices was to better understand firms’ current practices for liquidity risk management, and to raise awareness of the need for sound liquidity stress planning.

FINRA conducted an assessment and survey of selected mid-size and large BDs to gauge their readiness for a broad range of adverse circumstances—including extraordinary credit events—from a liquidity risk management and operational perspective. Based on the survey, FINRA recommended that organizations:

- Conduct a self-assessment of their businesses, and incorporate firm-wide liquidity stress testing into their risk and business planning
- Continuously monitor and evaluate liquidity needs in both idiosyncratic and market-wide stress scenarios (FINRA intends to review firm liquidity risk planning and stress tests)
- Have sufficient resources to measure risk applicable to their businesses, and implement sufficient mechanisms for escalating and reporting issues to senior management
- Develop a contingency funding plan to address identified liquidity risks, and implement mitigating processes
- Conduct necessary operational tests and other reviews to evaluate the effectiveness of the contingency funding plans
Although the Department of Labor Fiduciary Rule met an untimely death 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 adviser (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 have 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 five to ten years, when the regulatory environment may be less relaxed. 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

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 adviser (FA) workloads to meet regulatory obligations—is causing many organizations to rethink how they supervise and oversee FAs and their businesses.
Cybersecurity and privacy

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 Advisory 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 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 current administration in the United States has placed renewed emphasis on 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.

Key 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 ML 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 market 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 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 nonpublic 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. 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 AICPA Cybersecurity Attestation Reporting Framework (figure 3).

Figure 3. the AICPA Cybersecurity Attestation Reporting Framework

Key stakeholders

| Board of directors | Regulators | Cyber insurance carriers | Customers |

AICPA Cybersecurity Attestation Reporting Framework

1. Management’s description of the cybersecurity risk management program

2. Management’s assertion on:
   • The presentation of the description
   • The operating effectiveness of the controls to achieve the cybersecurity objectives

3. Practitioner’s opinion on:
   • The presentation of the description
   • The operating effectiveness of the controls to achieve the cybersecurity objectives

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).

Flexible criteria

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.
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
Leading in times of change  
Capital markets regulatory outlook 2019

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.27 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.”28

**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.
In the time since our 2018 regulatory outlook was published, a great deal of progress has been made to implement the Consolidated Audit Trail (CAT). A year ago, many self-regulatory organizations (SROs) were not in compliance with the CAT requirements. SEC Rule 613 required participants to begin submitting data to the CAT repository, which was supposed to be available for querying and regulatory purposes. However, a number of factors—including security and data protection—had delayed the industry’s efforts.

Now, as this year’s outlook is being written, the exchanges should have begun submitting older life cycle data to the CAT repository, which was supposed to be available for querying and regulatory purposes. However, a number of factors—including security and data protection—had delayed the industry’s efforts.

What does this mean for the BD community? First, it provides firms with an opportunity to recalibrate their CAT readiness and implementation programs. Second, it allows for more industry input about technical specifications and industry testing. For CAT to be successful, each firm individually must have a robust technical and control environment and provide error-free, quality data to CAT.

To achieve this, firms need to focus on data acquisition within their own systems to ensure completeness, accuracy, and quality. Firms should be considering and anticipating all of the traditional nonfinancial regulatory reporting issues that have nagged the industry, and then developing a robust reporting environment.

Figure 4. Proposed CAT phased implementation timeline

<table>
<thead>
<tr>
<th>Phase 2a (equities reporting: Part 1)</th>
<th>The regulatory conformance period will end by February 24, 2020</th>
<th>Phase 2c (equities reporting: Part 2)</th>
<th>Customer and account system reporting go-live by November 15, 2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>go-live by November 15, 2019</td>
<td></td>
<td>go-live by September 1, 2020</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2019</td>
<td></td>
<td>2021</td>
<td></td>
</tr>
<tr>
<td>The regulatory conformance period will begin by November 15, 2019</td>
<td>Phase 2b (options reporting: Part 1) go-live by May 31, 2020</td>
<td>Phase 2c (equities reporting: Part 2) go-live by May 15, 2021</td>
<td>Non-OATS small industry member reporting go-live by November 15, 2022</td>
</tr>
</tbody>
</table>

Timeline for implementation
On August 9, 2018, the CAT NMS LLC Operating Committee proposed a phased approach for industry member reporting, starting with the reporting of equities data to CAT in November 2019. With the publication of this revised approach and timeline, large BDs face firm deadlines (figure 4) for CAT reporting and must continue to implement a regulatory operational model to comply with CAT reporting.

However, CAT has been a lightning rod for BDs and industry groups such as Securities Industry and Financial Markets Association (SIFMA), Financial Information Forum (FIF), and Security Trade Association (STA). In particular, because of issues related to personal identifiable information (PII) and cyber events, it has been a priority of the SROs and Thesys CAT to make the security model and operations robust in order to earn the industry’s confidence that information will be protected. To that end, as of November 2018, the SROs are currently in discussions with the SEC staff for a recalibrated timeline.

What does this mean for the BD community? First, it provides firms with an opportunity to recalibrate their CAT readiness and implementation programs. Second, it allows for more industry input about technical specifications and industry testing. For CAT to be successful, each firm individually must have a robust technical and control environment and provide error-free, quality data to CAT.

To achieve this, firms need to focus on data acquisition within their own systems to ensure completeness, accuracy, and quality. Firms should be considering and anticipating all of the traditional nonfinancial regulatory reporting issues that have nagged the industry, and then developing a robust reporting environment.
Key focus areas and challenges for 2019

2019 is the year for BDs to build and implement their CAT solutions. Data acquisition and data lineage from source systems to the destination platform should be the primary focus. In the past, it has been challenging for firms to understand how data flow from the order management systems (OMS) to the reporting platforms. Also, it has been difficult to understand the data transformation that takes place in order to meet the reporting requirements. This is a focus area for firms to mobilize on.

The other focus area for BDs is customer data, which pose a significant challenge. Most firms store customer data in a central repository, an AML platform, and disaggregated in their trade order management systems.

When preparing for CAT, the following high-impact challenges should be top-of-mind:

PII-related challenges

Personally identifiable information is likely to represent one of the greatest step changes in the regulatory requirements. Major challenges related to PII include:

- Determination of PII “golden sources.” What are the purest validated sources for PII data?
- Data obfuscation. What data need to be masked or encrypted, and how will that be done?
- Third-party risk management for PII. Do third-party vendors that store PII data have adequate controls?
- Security and data management. Are there appropriate controls to ensure PII data are well secured from end to end?
- Internal escalation processes for PII breaches. Are the necessary controls in place to detect, monitor, and address internal and external PII data breaches?
- Determining access to PII within the regulatory ops team. Which team roles need PII access to satisfy CAT reporting requirements, and how will data access be monitored?
- Training and handling PII. What training is needed for the regulatory ops team to ensure proper handling of PII?
- Scalability and the moving target for PII. Are systems flexible and scalable enough to adapt to changing requirements?
- Determination of access to PII within the regulatory ops team. Which team roles need PII access to satisfy CAT reporting requirements, and how will data access be monitored?
- Training and handling PII. What training is needed for the regulatory ops team to ensure proper handling of PII?
- Scalability and the moving target for PII. Are systems flexible and scalable enough to adapt to changing requirements?

Other key challenges

When preparing for CAT, firms may also face a number of high-impact challenges not directly related to personally identifiable information:

- Firm-designated IDs. CAT specifications require industry members to generate a unique identifier for each trading account used to place an order, notably restricting the use of an actual account number or any other identifier that could be used to affect a transaction in the account.
- Trade data linkages. CAT specifications require firms to link all reportable events using certain “linkage keys” that connect disparate events within an industry member and across industry members and exchanges.
- Planning for the unknown. The requirements associated with CAT’s later phases (2B–2D) remain uncertain; firms will need to develop foundational capabilities for phase 2A equities reporting while remaining flexible to the evolving requirements for later stages.

Moving forward

The CAT’s transformative impact will require firms to reassess their operational models, particularly those related to technology, data, and operational reporting oversight. We believe the increased regulatory complexity will lead firms to centralize, simplify, and automate their reporting models, and to consider how they might right-size controls to meet the requirement for more stringent error handling response times.

Achieving the ideal model will likely require a current-state assessment, followed by future-state visioning that seeks to leverage technology enablers wherever possible—including automated reconciliations, defined workflows, RPA, and ML. However, the most fundamental step in developing base-level CAT capabilities is to understand and develop the underlying data. If this is not tackled early, it will likely cause major problems down the road.
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.
Endnotes

Contacts

**Leadership**

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

Vik Bhat
Advisory Banking & Capital Markets Leader
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
vbhat@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**

Elia Alonso
Elia Alonso
Global Conduct Risk Leader
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
elalonso@deloitte.com

Susan Ameel
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
sameel@deloitte.com

Michael Bolan
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
mbolan@deloitte.com

Nitish Idnani
Banking & Capital Markets Operational Risk Leader
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
nidnani@deloitte.com

Mike Jamroz
Independent Senior Advisor to Deloitte & Touche LLP
mjamroz@deloitte.com

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

Alexey Surkov
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
asurkov@deloitte.com

Bob Walley
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
rwalley@deloitte.com

Gowri Zoolagud
Managing Director | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
gzoolagud@deloitte.com

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

Michael Corwin, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Nitin Pandey, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Vibha Patil, Senior Manager | Deloitte Risk and Financial Advisory, Deloitte & Touche LLP
Stefan Safsten, 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, healthcare, 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.