KPMG

Ten key regulatory challenges

Facing the financial services industry in 2017

Americas FS Regulatory Center of Excellence

The U.S. election on November 8, 2016 has introduced a new level of uncertainty into the challenging regulatory environment for financial services firms. By solidifying its control of both houses of Congress and gaining the presidency, the Republican Party could potentially effect a series of policy changes that could lessen the regulatory burden, reduce enforcement activity, and redirect the trajectory of U.S. financial services regulation since the financial crisis.

While the financial services industry was not a central focus of Mr. Trump's campaign, public statements made by him and his aides since the election indicate that the new administration is considering significant changes to the Dodd-Frank Act as well as to other financial regulatory reforms. The new administration's goal is to reduce the financial burden on banks by repealing and reducing various provisions of the Dodd-Frank Act and replacing them with new policies to encourage growth and job creation. Congressional Republicans have similarly suggested repealing or significantly changing the Dodd-Frank Act as well as modifying the structure and authorities of the Consumer Financial Protection Bureau (CFPB or Bureau), the Office of the Comptroller of the Currency (OCC), and the National Credit Union Administration (NCUA); delaying or eliminating altogether the Department of Labor's Fiduciary Rule; repealing the Volcker Rule; and exempting certain banking organizations from Basel capital requirements and/or the Enhanced Prudential Standards.

Even with the expected reductions in the regulatory burden, many of the key regulatory issues identified last year remain important and relevant for the coming year although some have taken on a different focus. The tenets of risk governance and conduct and culture are likely to continue to dominate the expectations of regulators and consumers across the financial services industry. In addition, cybersecurity, the protection of consumer data, and the competitive pressures from financial technology (FinTech) firms will only grow in importance.

Regardless of the regulatory environment, all indications suggest financial institutions of all sizes should "stay the course," recognizing that, for now, the scope of anticipated change is speculative and will take time to enact, implement, and operationalize. In the meantime, building a strong customer-oriented corporate culture, developing a holistic approach to enterprise risk governance, improving data management, embracing technological changes, and streamlining regulatory change capabilities will help prepare and position institutions for any new regulatory requirements.

Recognizing that during 2017 the new administration may change elements of the existing regulatory landscape, we offer our perspective on some of the key regulatory issues currently facing financial services firms.

1. Strengthening enterprise risk governance and culture

While issues around conduct and culture continue to be a major challenge for financial services organizations, high-profile instances of misconduct demonstrate that firms will have to widen their focus and look at enterprise risk governance more broadly. Regulators are conducting horizontal reviews of large bank "Conduct and Culture" programs and examining sales practices, employee sales goals, and compensation practices along with the effectiveness of banks' risk governance across the organization. Continued interest in these areas will likely be supported by the new administration, which has criticized senior management compensation packages, questioned board independence, and voiced concerns over sales practices that could be harmful to consumers. This focus increases the potential for emphasis on and action to enhance corporate governance and pushes firms to strengthen their enterprise-wide approach to risk governance.

Although most financial institutions have established processes and collect data in various parts of the organizations, there is a need to connect disparate processes in order to analyze key risk indicators and key performance indicators more holistically and improve the monitoring capabilities and information that can be used to inform management and the board. Some of the processes and metrics that need to be connected include an organization's code of conduct; complaints; whistleblower hotlines; issues management; employee, customer, and vendor surveys; performance management; compensation; internal investigations; sales practices; business strategies; key internal and external communications; and management and board reporting. Leading firms are looking to an enterprise-wide risk governance framework that links risk strategy and appetite, risk governance, assessments, monitoring and reporting, control testing, and data and technology. They are also embedding their values, goals, expectations, and priorities into their three lines of defense, while making enhancements to the transparency, independence, and oversight within this structure.

The three lines of defense model is designed to form a system of checks and balances between the first line ownership of the design and execution of controls, the second line independent monitoring and oversight of the effectiveness of those controls, and the third line independent review by internal audit of how the first and second line control functions are performing. Regulators are also providing more specific guidance in this area. Notably, the OCC's Enhanced Risk Management Standards outline "heightened expectations" for enterprise-wide risk governance, and changes to the Federal Reserve Board's (Federal Reserve) SR 08-8 Compliance Risk Management Programs and Oversight at Large Banking Organizations with Complex Compliance Profiles will focus on conduct and culture as well as testing and monitoring.

2. Transforming the effectiveness and sustainability of compliance

Financial services organizations are intensifying efforts to enhance compliance effectiveness and sustainability in response to evolving regulatory expectations. Updates to the Federal Reserve's SR08-08 are expected to include guidance on culture, conduct, board roles and responsibilities, and technology-enabled compliance. In addition, expectations of new oversight of business and sales practices and enhanced compliance risk governance are leading firms to use advanced analytics and technology in their compliance efforts. Financial services firms must demonstrate compliance program sustainability through enhanced monitoring and testing, demonstrable accountability, and supporting management information systems (MIS). Many organizations are pivoting towards compliance automation tools that deliver operational value, increased efficiencies, and decreased costs by transforming compliance into an increasingly integrated part of a forward-looking business strategy. Key trends in this context include: building adaptability into the inter-relationships of the people, processes, and technologies that support compliance activities; augmenting and automating monitoring and testing processes in order to self-identify compliance issues and expand root cause analysis; and integrating compliance accountability into all facets of the business.

3. Examining possible new approaches to managing capital and liquidity

Given the new administration's view that the Dodd-Frank Act is an obstacle to economic growth, legislation directed at regulatory restructuring is possible. Most changes will likely be aimed at reducing elements that are not accretive or supportive of effective supervision. This will likely include regulation impacting the supervision of capital and liquidity. The Financial CHOICE Act promoted by congressional Republicans during 2016 would permit well-capitalized, well-managed institutions in the United States to be exempt from certain capital and liquidity requirements, including stress testing, resolution plans, and related reporting. The exemption would be effective only if firms satisfy a threshold leverage ratio requirement (proposed as ten percent). Institutions failing to meet the threshold would need to continue stress testing as well as maintaining capital and liquidity buffers, though the exercises, as proposed, would be less frequent and so less burdensome. Although there have been no explicit indications with respect to capital and liquidity relief, it should be noted that current and proposed capital and liquidity regulations could be open for discussion.

Under current Enhanced Prudential Standards, financial institutions are required to demonstrate their ability to develop internal stress testing scenarios for both capital and liquidity that properly reflect and aggregate the full range of their business activities and exposures as well as the effectiveness of their governance and internal control processes in both a business-as-usual (BAU) scenario and a stressed environment. In addition, the largest financial institutions must provide information for both capital and liquidity demands, both before and after resolution.

Prior to the election, several efforts to formalize the link between capital and liquidity management were made in the United States, such as the proposal for the total loss-absorbing capacity (TLAC) held by global systemically important bank holding companies (GSIBs), the Recovery Guidance issued by the OCC, and the Resolution feedback issued by the Federal Reserve and FDIC. Together, these encourage large financial institutions to estimate and position pre- and post-resolution capital and liquidity resources to manage and resolve their material legal entities effectively. Additionally, the Federal Reserve has been conducting a review to enhance capital stress testing and its macro-prudential supervisory regime.

Despite a possible debate on capital and liquidity relief, our perspective is that the landscape is unchanged regarding capital and liquidity integration. Current capital and liquidity requirements as well as integrated management support safe and sound banking practices and should continue unchanged to promote economic growth and financial stability.

4. Managing the complexities of cross-border regulatory standards

While it is unclear how the new administration will address application of international standards and accords, the risks associated with cross-border issues, including divergent policies, will continue to be relevant. There is speculation that, given its antiglobalization sentiment, the new administration could slow implementation or ignore higher capital and liquidity requirements developed by the Basel Committee on Banking Supervision. Some in the United States view international capital requirements as requiring banks to hold more capital than needed and that could otherwise be used to stimulate domestic economic growth.

Additionally, congressional Republicans have supported the Financial CHOICE Act, which proposes elimination of the Financial Stability Oversight Council's (FSOC) authorities to designate nonbank systemically important financial institutions (SIFIs). This would remove non-bank SIFIs, primarily insurance companies, from Federal Reserve Board oversight and the associated capital and liquidity requirements. The possible divergence from Basel, the new administration's possible exemption from Enhanced Prudential Standards (EPS) and higher capital and liquidity standards, and the potential elimination of the FSOC's authorities would increase differences in cross-border regulatory requirements for internationally active financial institutions.

Increasing cross-border regulatory policy divergences will require internationally active financial firms to undertake more strategic and comprehensive assessments of their regulatory policy risks. These challenges underscore the importance of developing a centralized process for assessing current and potential future regulatory demands using advanced governance, risk management, and compliance regulatory change tools. A centralized framework facilitates coordination across operating silos that can generate insights that deliver benefits beyond the core compliance function. Centralized assessments of cross-border risks can help improve overall performance, help ensure risk management frameworks and compliance controls are integrated into strategic objectives, reduce redundancy, and enhance the ability to address regulatory expectations.

5. Adjusting to the changing scope of consumer financial protection

Over the past five years the perimeter of the CFPB's enforcement actions continued to expand. For example, the CFPB's focus on addressing unfair, deceptive, or abusive acts or practices has been expanding to keep pace with financial innovations that are reaching more consumers. This includes sales practices, auto-finance companies, payment platforms, elder financial protection, first-party debt collectors and creditors, and financial technology, or FinTech, firms in addition to banks.

The recent U.S. election, however, brings some uncertainty regarding the CFPB's role and structure. In particular, congressional Republicans will likely scale back the Bureau's authority and place it under tighter congressional control, including shifting the leadership from a single director to a five-person commission and subjecting the Bureau to the appropriations process. This change may also move the CFPB from its current single mandate of consumer protection to a dual mandate of consumer protection and increased competition in markets. The Bureau's broader consumer protection role, however, seems to be consistent with Mr. Trump's position on promoting fairness to consumers in the financial markets and authority under federal consumer protection laws. This makes it unlikely that the mandate of the CFPB would be eliminated entirely, but its scope is unlikely to expand and may even be scaled back.

While the Federal Trade Commission (FTC) has been the primary agency regarding data security issues, the CFPB filed its first consent order concerning data privacy in 2016 by alleging that a firm stored and transmitted unencrypted personal information and failed to implement appropriate data security policies and procedures. The order demonstrates that all companies that collect, store, and use customer information must take measures to represent their security practices and noncompliant data protection procedures accurately. We also expect an increased regulatory focus on bank third-party relationships and compliance with bank regulatory requirements from those third parties regarding retail consumer protection issues. Importantly, this focus on third-party relationships will align with the general heightened focus on cybersecurity and related concerns.

6. Emphasizing cybersecurity while protecting consumer data privacy

Cybersecurity and consumer data privacy concerns continue to generate strategic business challenges for financial institutions. Policymakers are addressing data security issues at the federal, state, and regulatory levels. Notably, the New York Department of Financial Services proposed rules to establish a regulatory cybersecurity framework. The framework includes principles set out by other regulators, such as the NIST Cybersecurity Framework and the FFIEC Cyber Assessment Tool, but is considered to be more comprehensive than these other currently applicable rules. It is expected to become effective during 2017 and to set a new, higher cybersecurity standard across financial services. The federal banking agencies (Federal Reserve, OCC, and FDIC) have also issued an advanced notice of proposed rulemaking seeking to establish an enhanced set of cybersecurity management standards for large, interconnected banking organizations. In addition, the CFPB and FTC have taken enforcement actions against financial services firms for data security issues, relying on prohibitions against unfair and deceptive acts or practices rather than issues of data security/data privacy issues under the Gramm-Leach-Bliley Act.

As attentions are turning to cybersecurity, financial institutions continue to acquire significant amounts of personal, identifiable data from clients. Investments in technologies along with cost reduction initiatives have increased exposure to data vulnerabilities and generated incentives for boards and senior executives to assess carefully the adequacy of controls and technology used by external vendors as well as how technology investments can reduce cyber risks while delivering improved efficiency gains and client experiences. Many compliance leaders are reevaluating their overall approach to privacy and compliance within their organizations. This includes a focus on continuous improvements to data security, IT infrastructures, enterprise provisioning, and scalable data management controls both locally and globally.

In the global environment, data sovereignty laws are emerging to regulate how organizations may transfer personal data outside of a country or region. Countries increasingly seek to protect the personally identifiable information of their citizens by asserting jurisdictional control over this information, as exemplified by the EU-U.S. Privacy Shield completed in July 2016.

The new administration has placed a priority on reviewing and minimizing vulnerabilities in the nation's infrastructure related to cybersecurity and cyber threats—encompassing broadly the military, law enforcement, and private industry sectors. Early indications from the new administration suggest that data privacy may be less of a focus in an effort to enhance cybersecurity.

7. Addressing pressures from innovators and new market entrants

2016 has been the year in which FinTech emerged as a significant market force to challenge the financial services industry and its regulatory structure. Innovations such as mobile payments, distributed ledgers, crowdfunding, online marketplace lending, peer-to-peer lending and virtual currencies hold the potential to transform financial services into platforms for intermediation by third parties. They also hold the potential to expand intermediation services to underserved individuals and communities. Regulators are also recognizing the potentially disruptive force of FinTech and are actively pursuing regulatory oversight. While FinTech companies involved in consumer finance fall under the CFPB's purview, the OCC's recent proposed rule outlining a receivership framework for uninsured non-depository national banks as well as its forthcoming Office of Innovation point to the agency's growing involvement in FinTech through its support of "responsible innovation." Separately, statements by representatives of the SEC suggest that the SEC should take the lead regulatory role with FinTech firms. Regardless of who takes the lead, any form of regulation and supervision will likely have a light touch to encourage innovation.

Banks are actively responding to this rapidly changing competitive environment. Many have partnered with FinTech firms to support key business processes, develop a lower cost operating model, and provide new services. FinTech firms can offer cost savings for banks facing margin pressures from low interest rates. They can also offer opportunities to update legacy IT systems. However, partnership with FinTech firms can create regulatory risks. Third-party service providers for banks (including FinTech firms) are already subject to indirect federal banking regulation, and regulatory scrutiny regarding FinTech third-party providers is increasing. Notably, the OCC and the Financial Industry Regulatory Authority (FINRA) are both revising guidance regarding the use of third-party contractors. With the new administration's focus on competitive markets and a reduced regulatory burden, however, it is unclear if efforts to pull FinTech under the regulatory umbrella will continue with the same urgency.

8. Managing compliance surveillance and financial crimes

Driven largely by regulatory requirements and industry pressures for increased speed and access, trade and transaction reporting has become increasingly complex. Capturing and analyzing vast amounts of data in real time remain massive challenges for the financial services industry, as regulators continue to initiate civil and criminal investigations and levy heavy fines on broker-dealers, investment banks, insurance companies, and retail and commercial banks based on failures to completely and accurately report required information. In addition, ensuring compliance with federal and state laws prohibiting money laundering, financial crime, insider trading, front running, and other market manipulations and misconduct remains critically important. The new administration has indicated an increased focus on surveillance, especially around financial crimes and laws (anti-money laundering (AML) and know your customer (KYC)) to fight terrorism financing.

All of this is occurring during a time when financial institutions are challenged to manage resources and spend and the prospect of increased scrutiny on consumer sales practices. This could drive firms to seek automated or digital solutions to supplant or supplement manual processes. In the coming year, it will be essential for financial institutions to employ a systematic and comprehensive approach to developing a sustainable compliance program in order to better manage both known and emerging regulatory and legal risks and proactively respond to prospective market structure reforms. Additionally, in all areas, financial institutions are reviewing, strengthening, and implementing controls in the first, second, and third lines of defense to help ensure that they are calibrated and effective across domestic and global financial regulations.

9. Reforming regulatory reporting

Regulatory expectations regarding financial, trade, transaction, and position reporting continue to increase, creating challenges for financial institutions. Regulators are expressing particular concerns about the lack of progress in eliminating manual processes and reconciliations, addressing data integrity issues, negotiating resource and other constraints that impact accuracy and timeliness, and fixing weaknesses in data governance. Leading firms are responding by developing a more holistic approach to financial and nonfinancial data management that harnesses the use of data collection for risk management and decision-making purposes in addition to regulatory compliance. The continued expansion of the examination process related to regulatory reporting also poses a significant challenge for 2017. The Federal Reserve's FR Y-14 Horizontal reviews, conducted in 2016, involved detailed examinations of organizations' program and data governance, internal controls, and transaction-level testing. Examiners also reviewed a range of other regulatory reports in assessing the accuracy of an organization's reporting processes and traced line items back to data sources for trades and transactions. Examination results showed that the Federal Reserve is becoming less tolerant of manual processes, particularly in areas that lack sufficient oversight and documentation. In parallel, leading firms are also implementing next-generation processes that will further automate the regulatory reporting process in an effort to achieve more efficient and accurate reporting outcomes.

10. Using risk data aggregation and reporting for improved enterprise risk management and transparency

As expected in 2016, financial regulators devoted increased attention to risk data aggregation issues and increased pressure on financial institutions to enhance internal data-related systems and processes. Data-related issues have dominated Federal Reserve requirements for banks in matters requiring attention (MRA) and matters requiring immediate attention (MRIA). In addition, the Federal Reserve is conducting reviews during 2016–2017 of how financial institutions have implemented the Basel Committee on Banking Supervision (BCBS) principles regarding risk data aggregation. There is also an increased focus on both financial and nonfinancial regulatory reporting and the recognition by firms that data must be mapped to authorized data sources. Adding to this focus are growing regulatory concerns over counterparty credit risk and credit risk concentrations. Financial institutions, especially the largest organizations, may be challenged to create systems that are needed to adequately manage this risk, including the capabilities to identify, aggregate, and monitor gross exposures across the consolidated institution and by industry.

For broker-dealers and investment banks subject to the jurisdiction of the Securities and Exchange Commission (SEC), enhanced process controls, data tracing, and risk reporting for both financial and nonfinancial risk reporting requirements remain the focus of attention. Improved data governance and quality is simultaneously becoming a strategic initiative for executive leadership and boards as banks strive to create an integrated framework that can drive significant and holistic enhancements to data quality and data governance across the enterprise. For example, reconciling finance and risk data makes it possible to use unified data for a range of internal decision making that helps increase operating efficiency while supporting increased accuracy in stress testing and capital allocation as well as in regulatory reporting. It also helps generate insight into the strengths and weaknesses of risk management activities.

Evolving technologies are making it possible to integrate contextual data (through semantic technology) and machine-learning (cognitive technologies) to assess dynamically a range of both structured and unstructured data, allowing institutions broader insight into operating and business strategies. The challenge is creating the foundation to unlock the value of these data.

For additional information, please contact:

Deborah Bailey
Managing Director
Americas Financial Services Regulatory Center of Excellence
Financial Services Regulatory Risk Practice
T: 212-954-0897
E: dpbailey@kpmg.com

Amy Matsuo
Principal and National Lead
Financial Services Regulatory Risk Practice
T: 919-380-1509
E: amatsuo@kpmg.com

Greg Bell
Principal and National Lead
Information Protection
T: 404-222-7197
E: rgregbell@kpmg.com

Brian Murrow
Principal
Credit Risk
T: 703-962-5925
E: bmurrow@kpmg.com

Phillip Bray
Principal
Operations Risk
T: 704-371-5228
E: pbray@kpmg.com

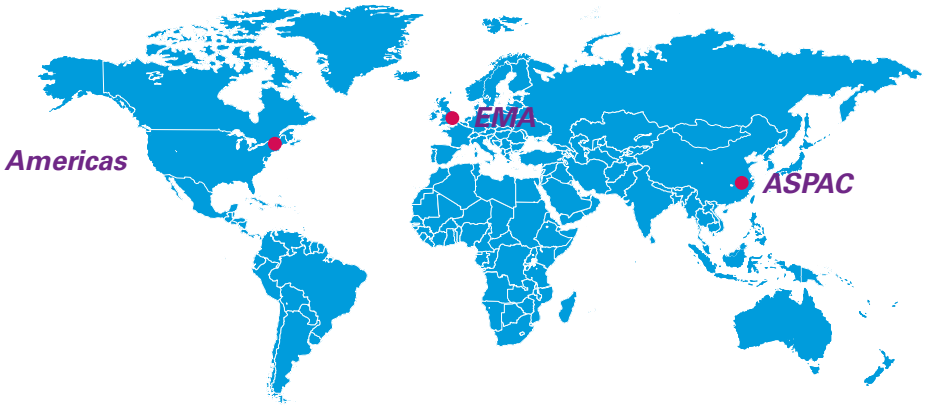
Teresa Pesce
Principal
Financial Crimes and Enforcement
T: 212-872-6272
E: tpesce@kpmg.com

Christopher Dias
Principal
Market/Treasury Risk
T: 212-954-8625
E: cjdias@kpmg.com

Authors:
Philip MacFarlane, Associate Director, Financial Services Regulatory Center of Excellence

Karen Staines, Director, Financial Services Regulatory Center of Excellence

The Americas Financial Services Regulatory CoE is based in Washington, DC and comprised of key industry practitioners and regulatory advisers from across KPMG's global network.



kpmg.com/socialmedia