KPMG

Ten Key Regulatory Challenges for 2018

Actions to Drive Effective Change in Financial Services

December 2017

KPMG Financial Services Regulatory Insight Center

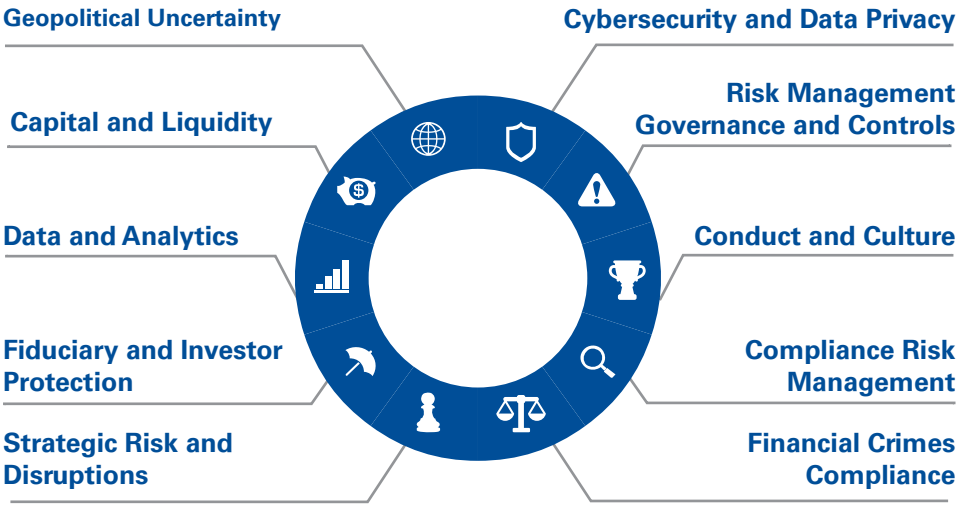
kpmg.com

Introduction

Effects from the anticipated deregulatory policy agenda have not resulted in the dramatic lessening of regulatory challenges for financial services providers that had been predicted. In 2018, regulators clearly will continue to expect an overall strengthening of core risk management governance, controls, practices, and reporting, particularly in the areas of cybersecurity, third-party risk management, and conduct and culture. Continued adoption of automation and innovative technology will help drive sustainable and effective change across these regulatory challenges.

This report from KPMG offers a high-level look at ten key regulatory challenges we believe will influence and impact the financial service industry in the coming year. The report also highlights the drivers behind these challenges and serves as a guide to actions financial services companies can take to address them. The ten key regulatory challenges include:

Ten Key Regulatory Challenges for 2018



The KPMG Ten Key Regulatory Challenges for 2018 can help financial services companies allocate valuable resources and investment to manage risk. 2018 will be a time of geopolitical uncertainty coupled with continued technological and automation advances. Companies have a unique opportunity to enhance their practices in a more sustainable and ultimately more efficient manner. As they address the challenges through effective action, they will continue to drive what is core - customer trust in the financial market and their organization.

Cybersecurity and Data Privacy

Drivers:

- Greater use of emerging technologies and connected customer channels
- Increased incidence and impact of cybersecurity attacks
- Financial and reputational risks resulting from cyber incidents
- Heightened public sensitivity to data privacy and data protection
- Evolving state, jurisdictional, and global privacy regulations and regulatory expectations

Because data breaches can have a severe impact on organizations, trusted third parties, and individuals, cybersecurity and the protection of data are a top priority to organizations and a great concern to regulatory bodies. However, KPMG has found integrating cybersecurity and data privacy compliance to be a top challenge for many financial institutions facing perpetual and evolving risks from cyber threats. Cybersecurity and data privacy compliance are now integral to any organization's business strategy and must be embedded into enterprise risk management programs and IT decisions.

Key operational issues include:

- Cyber risk governance
- Internal and external risk assessment and management
- Policies, procedures, and controls
- IT and data asset management
- Prevention, detection, and mitigation of vulnerabilities
- Incident response
- Regulatory reporting and notifications
- Resilience, including disaster recovery and business continuity planning
- Third-party risk management

Increased sensitivity to data privacy and data protection necessitate that all organizations look to regulations such as the European Union's GDPR (General Data Protection Regulation) for key practices by which to evaluate and revamp their data privacy and data protection programs.

Key privacy concerns include:

- Expanded definition of personal data
- Strengthening privacy rights for individuals
- New privacy compliance control and reporting requirements
- Potential for large fines and penalties
- Need to assess privacy compliance prior to introducing high-risk, material business and IT changes

Key actions:

- Evaluate and strengthen identity and access management capabilities
- Establish and operationalize cybersecurity and data privacy governance channels
- Identify and address at-risk business processes and data
- Conduct data protection impact assessments
- Identify and introduce data subject related capabilities
- Establish or enhance incident response protocols, business resilience framework, and communications plans
- Consolidate and converge cyber and privacy technologies
- Perform internal and external threat assessments

KPMG

Risk Management Governance and Controls

Drivers:

- Risk management focus on Three Lines of Defense (3LOD)
- Heightened standards and expectations for Internal Audit
- Growing importance of a sustainable third-party risk management infrastructure
- Regulatory focus on electronic trading controls
- Evolving regulatory requirements for recording and reporting information (financial and nonfinancial)

In the wake of what regulators deemed to be large misconduct and manipulation by financial services providers, financial services companies are facing a renewed rigor to risk management governance and controls. The 3LOD model, consisting principally of the business, independent risk management (inclusive of Compliance), and Internal Audit, while firmly in place in the financial services industry, has undergone regulatory scrutiny well beyond the organizational construct itself. This heightened standard applies directly to the roles and activities of Internal Audit and to areas such as risk identification, scenario analysis, business line accountability, issues management, third-party management, and reporting.

Areas of focus include:

- Established accountability for controls and processes
- Issue identification and escalation to management, board governance, and demonstration of critical challenge
- Data and controls (with associated mapping to regulatory requirements or obligations).
- Electronic trading controls and processes (including the need for enhanced data lineage, automated controls, and quality checks)
- Models-driven decision making and execution
- Regulatory reporting (financial and non-financial)

Key actions:

- Conduct enhanced risk identification and scenario analyses
- Develop and implement management accountability matrices
- Assess and address clarity of risk statements and risk reporting (across risk disciplines)
- Establish and operationalize nonfinancial risk (e.g., conduct, reputational) management frameworks, including data analytics/modeling and reporting
- Develop demonstrable processes and evidence to document issue management identification, escalation and remediation, inclusive of critical challenge

> "The intent is to enable directors to spend … more [time] on core board responsibilities: overseeing management as they devise a clear and coherent direction for the firm, holding management accountable for the execution of that strategy, and ensuring the independence and stature of the risk management and internal audit functions. These were all areas that were found wanting in the financial crisis, and it is essential that boards get these fundamentals right."
>
> **—Jerome H. Powell**

Conduct and Culture

Drivers:

— Continued regulatory and supervisory focus on financial services companies' abilities to effectively monitor and manage conduct risk

— Enforcement actions related to sales practices, client suitability, market manipulation, and fraud

> "Without an understanding of root causes, how can you know that a particular behavior is random, or that its breadth will remain limited?"
>
> **—Michael Held**

Conduct and culture remain a key supervisory priority, as multiple transactions viewed as instances of misconduct have shaken public trust in the financial services industry. In many cases, the regulatory agencies have addressed this misconduct with public enforcement actions and promises of continued prioritization. Regulators will continue to focus on institutions' efforts to establish and operationalize a measurable conduct risk management framework that identifies and prevents misconduct at its root. This framework will be expected to include:

— Centralized oversight and a governance structure with a defined conduct risk appetite, controls, and consistent conduct risk taxonomy, assessments that capture conduct risk, and specific examples of conduct expectations

— Clear roles and responsibilities for conduct risk between the 1st and 2nd lines of defense that ensure its management is embedded in the business

— Conduct risk assessments supported by metrics, monitoring, and testing

— The use of quantitative conduct risk measures to integrate conduct risk into existing risk assessment processes and scenario analyses

— Business-level dashboard metrics covering elements such as client conflicts of interest, market conduct, sanctions, and breaches.

As conduct risk management requires both a top down and bottom up approach, establishing effective and strong controls that include diligent and continuous governance, oversight, and monitoring are the key to preventing future instances of misconduct and deploying an effective conduct and culture-related risk mitigation strategy.

Key actions:

— Establish and operationalize the conduct risk management framework

— Align and integrate conduct risk programs with the existing risk and compliance program

— Perform business practice activity reviews

— Assess behavioral and root cause drivers and values

— Define culture and conduct governance, metrics, and reporting standards

— Set up and execute communication plans

— Conduct change impact assessments

KPMG

Compliance Risk Management

Drivers:

— Heightened regulatory focus on overall compliance risk assessments and programs as an extension of regulatory findings related to sales practices and conduct risk

— Expected updates and changes to regulatory guidance for organizations with complex compliance profiles highlighting conduct risk and required automation

— Competition to meet industry and consumer demands for digital applications and increased automation

— Need for increased effectiveness, efficiency, and agility forced by the cost-cutting, resource-constrained environment

Faced with an onslaught of regulatory requirements and supervisory actions in the wake of the financial crisis, most companies responded by implementing processes to address specific requirements as they were made known. In many cases this has resulted in overlapping, duplicative, and sometimes inconsistent, efforts to assess risk. As the pace of new regulations slows, companies have opportunity to improve their compliance risk management activities, and in particular, to strengthen their ability to identify and manage relevant risks and controls as well as to operationalize compliance and better partner with the business and functions across the organization. Key areas to consider include:

— Integrating compliance into operational processes, including business and support functions

— Automating compliance activities, to support regulatory change management, investigations, reporting, testing and monitoring, and risk assessments

— Holding employees, contractors, and third parties accountable to the organization's compliance standards

— Formalizing risk assessments to further inform compliance enhancements and priorities, as well as to promote a convergence strategy that moves toward a single methodology and taxonomy for risks across the company

— Continuously improving the compliance program through monitoring and root cause analysis

An integrated compliance risk management program allows for greater coordination and collaboration between compliance and the rest of the organization, ultimately leading to a more concerted and consistent approach to risk management. To be successful, however, compliance must have the visibility and authority to confidently contribute as a partner to the risk management process, including actively managing, escalating, and resolving issues from the first line up through the board of directors.

> "Larger, more complex banking organizations tend to conduct a wide range of business activities that are subject to rigorous compliance requirements that frequently transcend business lines and legal entities and, accordingly, present risk management and corporate governance challenges."
>
> **—Federal Reserve Board**

Key actions:

— Conduct compliance program "front to back" assessment

— Plan and execute regulatory compliance technology and automation

— Integrate/converge compliance and operational risk methodologies, taxonomies, and processes

— Develop delineated accountability matrices across the 3LOD for compliance

Financial Crimes Compliance

Drivers:

- Regulatory changes to Know Your Customer (KYC)/ Customer Due Diligence (CDD), transaction monitoring, and screening requirements
- Increased competition, including from FinTech companies
- Technology advances, disruption, need for speed in innovating
- Demands for cost reduction
- Reputational and cost implications from regulatory enforcement or supervisory actions, third parties, and/or business model changes

Financial Crimes compliance is facing significant regulatory change with the new customer due diligence rule going into effect and the first certifications for the New York Department of Financial Services transaction monitoring and screening programs due. Many Institutions have already committed considerable time and investment to comply, including changes to update their technology infrastructure; enhance policies, procedures, processes, and controls; revise training; and adjust governance. System validations or tuning exercises may also have been conducted. Continuous monitoring and improvement of compliance should be ongoing.

> Financial fraud, money laundering, and the financing of terrorism "pose a critical challenge to the integrity of our financial system and the public's confidence in that system. They threaten the security of the system and, indeed, our national security more broadly."
>
> **—Martin J. Gruenberg**

The need for integration and automation of Financial Crimes activities is also an increasing necessity to facilitate accurate and complete data and reporting as well as effective and efficient mitigation of Financial Crimes risks through predictive analytics and strategic deployment of resources. Cost containment is another pressing issue, and many are considering options such as shared platforms, more intelligent due diligence engines, and further operational convergence.

Areas of focus include:

- Know Your Customer compliance
- Transaction monitoring and screening
- Shared platforms
- Integration and automation
- Strategic planning

Key actions:

- Assess compliance preparedness for regulatory changes and address gaps
- Develop a strategic plan for Financial Crimes compliance, with established priorities
- Evaluate technology infrastructure capabilities for regulatory change, predictive analytics, and data integrity and accuracy

KPMG

Strategic Risk and Disruptions

Drivers:

- Regulatory focus on strategic risk in low rate environment
- Regulatory caution on dramatic changes and speed to innovate
- Technology advances and disruption
- Reputational and cost implications from regulatory enforcement or supervisory actions, third parties, and/or business model changes

> "Strategic risk is elevated, as management teams consider M&A, business model changes, and the potential need to adapt in an uncertain regulatory climate."
>
> **—OCC National Risk Committee**

The search for sustainable returns on capital in highly competitive lending markets and the persistently low interest rate environment coupled with technology advances via FinTech and digital have forced financial services companies to re-think strategic business and delivery model changes. While still needing to focus on rising customer expectations, providers must look to technology change adoption to innovate. Such changes come with risks, including adoption risk and compliance risk, and the potential for large changes to areas like tax and human resources. Financial services companies face anxiety with respect to strategic risk and technology, competitive and FinTech disruption. Most institutions recognize the potential for enhanced automation and regulatory technology (RegTech) in compliance, yet are cautious to quickly adopt without first establishing change governance, quality testing, and capacity and needed skills base changes.

Areas of focus include:

- Leverage customer behavioral data, complaint, and social media data
- Leverage platform economies to reach digital user data with traditional financial service product base
- Engage in "coopetition" between financial services companies and FinTech companies

Key actions:

- Develop and execute digital and FinTech operational strategies
- Evaluate behavioral, complaint, and other data model execution
- Assess commercial and retail customer experience metrics
- Conduct change impact assessments

Fiduciary and Investor Protections

Drivers:

- Heightened regulatory focus on investor protection and "best interest" standards
- Enforcement actions related to retail investor fraud
- Uncertainty surrounding form, timing, and ultimate adoption of the recently promulgated Department of Labor (DOL) Fiduciary Rule
- Focus on protecting seniors and other vulnerable adults from potential financial exploitation

Broker dealers, asset managers, insurance companies, banks, and other financial services investment providers continue to execute against enhanced fiduciary and investor protection expectations and standards. Regulatory rule drivers include the DOL Fiduciary Rule and MIFID II (Markets in Financial Instruments Directive). Supervisory and enforcement activities of the Securities and Exchange Commission, Commodity Futures Trading Commission, and Financial Industry Regulatory Authority remain focused on investor protections against potential misconduct and fraud. And, initiatives related to the aging demographics of the United States population, including financial protections for seniors and other vulnerable adults, also remain a priority for regulators as well as Congress.

Areas of focus include:

- Establishing and executing controls and governance relative to the "best interest" of the customer, including best execution and appropriateness of investment program enrollment
- Enhanced controls related to sales and trading practices
- Fraud risk management and suspicious activity surveillance and reporting
- High risk and/or recidivist brokers
- Conflicts of Interest

In addition to enhancements to the entity's integrated risk management (compliance, operational, and regulatory) and conduct programs, market participants (regardless of fiduciary definitions and timelines) will need to continue to: enhance transactional, regulatory, and employee data integrity and reporting protocols and technology; implement effective controls to mitigate, detect, and respond to potential misconduct or investor harm; and drive demonstrable effective challenge and accountability for investor protections for both commercial and retail clients and portfolios.

Key actions:

- Execute fiduciary and/or best interest standards
- Conduct investor and fraud protection assessments, particularly related to sales practices, fees, and vulnerable client portfolios
- Perform complex fiduciary reviews and remediation
- Evaluate and enhance surveillance and monitoring
- Enhance focus on trends and pattern metrics
- Establish and operationalize strong governance and tone from the top programs

"The issues we see in this space are extensive and often involve widespread incidents of misconduct, such as charging inadequately disclosed fees, and recommending and trading in wholly unsuitable strategies and products..... We are increasingly able to identify threats to retail investors – everything from registrant-based threats to microcap-based threats – through the use of data analytics."

—Stephanie Avakian

Data and Analytics

Drivers:

— Heightened expectations for data capture, governance, analysis, and reporting, inclusive of customer, financial activity, employee, and third party

— Evolving regulatory requirements for recording and reporting information (including equities and options)

— Large financial and reputational impacts associated with regulatory reporting

— Increased regulatory expectations for nonfinancial data accuracy and completeness on management, Board of Directors, and regulatory reporting

— Competitive pressures for cost reduction

— Maintenance and management of models

Regulators recognize the power in effective data analytics to help drive strong risk management and regulatory compliance, and have regularly included it in their own supervision and enforcement processes. In addition to data management integrity principles set forth in BCBS 239, implementation of the SEC's Consolidated Audit Trail (CAT) further demonstrates the evolving requirements for recording and submitting information on financial activity and the importance of enhancements to technology, automation, quality checks, and reporting processes. Model risk management processes in the development and validation of models and digital automation will be an evolving area of focus as the industry adopts continued intelligent automation to front and back processes.

Areas of focus include:

— Hiring, contracting and/or redeploying employees with skills to advance risk data analytics and digital transformation including intelligent automation

— Investments in platforms, systems, tools, and algorithms to capture, aggregate, govern, and analyze data from customers, financial activity, employee behavior, and third party transactions

— Implementation of descriptive and predictive metrics, aggregating disparate data across an organization in order to assess risk severity

— Ownership of models and algorithms, necessary transparency and responsibilities associated with model and system biases within the regulatory space

— Model–driven decision making across banking and capital market financial services providers, including commercial and retail as well as buy and sell sides

— Use of models to meet capital planning regulatory obligations

— Documentation and tracking of data lineage, including origin and authentication

— Use of enhanced data capture and visualization tools

Key actions:

— Invest in technology and automation for data feeds, pulls, aggregation, and effective usage to drive enhanced regulatory and compliance reporting, analysis, and monitoring

— Conduct enhanced root cause and predictive risk analysis

— Expand loss scenario analyses to enhance operational controls and predictive analysis

— Establish and operationalize enhanced data and model risk governance and management, including data management and integrity as well as model development and validation

— Utilize data to predict and/or identify potential risks in real time

Capital and Liquidity

Drivers:

- Regulatory and legislative uncertainty with regard to proposed rules
- Actions driven by findings from coordinated examinations conducted across multiple companies
- Recommended changes to systemically important financial institution (SIFI) and capital and liquidity thresholds
- Enhanced regulatory focus on financial market utilities and clearinghouses

Amendments to the capital and liquidity requirements for all institutions have been featured in the Treasury's recommendations for regulatory reforms as well as various legislative proposals. Generally, there appears a move toward fewer requirements for smaller and less risky institutions, including mid-size and regional banks, and more streamlined requirements for large institutions. Considerations include:

- Amending the SIFI designation process to limit the enhanced prudential standards, including the more stringent capital and liquidity requirements, to a more narrow group of institutions based on a combination of size and activities.
- Allowing certain well-capitalized institutions (e.g., as measured by a leverage ratio) to by-pass many of the more detailed capital and liquidity requirements. Other measures would decrease the scope and frequency of Dodd-Frank Act stress testing and regulatory reporting requirements.
- Delaying implementation of multiple rules, including the proposed Net Stable Funding Ratio, and U.S. rules on intraday liquidity risk and interest rate risk in the banking book.
- Potentially strengthening regulatory supervision to financial market utility and clearinghouse providers.

The Comprehensive Liquidity Analysis and Review (CLAR) and other coordinated examinations for large financial institutions have focused on measuring and managing liquidity risk, as well as the role of risk management and Internal Audit.

Areas of focus include:

- Pivoting from foundation building to management
- Leveraging capital data management processes for liquidity risk management
- Operations and strategic business planning
- Use of developed and developing emerging technologies

Key actions:

- Develop strategies for optimizing the balance sheet under multiple binding constraints
- Align data sourcing process for capital, liquidity, and other finance use cases
- Implement consistent processes for risk identification and scenario design across risk areas

> "The proposed rating system includes a new rating scale under which component ratings would be assigned for capital planning and positions, liquidity risk management and positions, and governance and controls."
>
> **—Federal Reserve Board**

Geopolitical Uncertainty

Drivers:

- Existing and evolving policy and regulatory differences across jurisdictions
- Protectionist public policy
- Global regulatory implications to strategy and operations

> "Financial markets were confronted by a changing political environment as the economic background brightened. Political events surprised market participants, who quickly needed to take views on the shifting policy direction and its economic implications. Attention shifted away from monetary policy, and political events took center stage."
>
> **—Bank for International Settlements Annual Report**

Regulatory and policy geopolitical uncertainty always has potential consequences for the business. New strategic and operational challenges are likely to continue to be faced in the years ahead. Companies with global reach may be affected by perceived protectionist public policy, forcing a reassessment of capital and staffing allocations and third-party relationship management. For example, companies are implementing strategies on the structure and conduct of their overseas businesses as the United Kingdom exits from the European Union. Likewise, financial institutions are executing regulations (such as GDPR and MIFID II) with direct impacts to areas of global operations, as well as compliance and tax functions. Finally, the use of global platforms, such as those facilitating cryptocurrencies (including Bitcoin) and market utilities, are capturing the attentions of governments and regulators.

Areas of focus include:

- Regulatory Change Management and automation
- Data management and lineage
- Scenario analysis and modeling
- Reputational risk exposure and assessment
- Incident and issues analysis, escalation and remediation
- Third party and outside business activity

Key actions:

- Conduct enhanced scenario and risk analysis, inclusive of financial and nonfinancial risks
- Integrate regulatory inventory and rule mapping to operational controls
- Reassess capital and human resource strategies and allocation
- Evaluate tax implications to changing regulatory policies
- Complete change impact assessments
- Re-tool risk assessments as appropriate
- Formalize incident and issues management governance, processes, escalation and reporting

Attribution

Page 3
Jerome H. Powell, The Role of Boards at Large Financial Firms, the Large Bank Directors Conference, Chicago, IL, August 30, 2017, https://www.federalreserve.gov/newsevents/speech/files/powell20170830a.pdf

Page 4
Michael Held, General Counsel and Executive Vice President of the Legal Group at the Federal Reserve Bank of New York, Reforming Culture and Conduct in the Financial Services Industry: How Can Lawyers Help?, March 8, 2017, https://www.newyorkfed.org/newsevents/speeches/2017/hel170308

Page 5
Federal Reserve Board, Corporate Compliance, https://www.federalreserve.gov/supervisionreg/topics/compliance.htm

Page 6
Martin J. Gruenberg Chairman, Federal Deposit Insurance Corporation, Fostering Financial Integrity – The Role of Regulators, Industry, and Educators, Case Western Reserve University School of Law Financial Integrity Institute, New York, March 23, 2017, https://www.fdic.gov/news/news/speeches/spmar2317.html

Page 7
OCC National Risk Committee, Semiannual Risk Perspective, Spring 2017, https://www.occ.gov/publications/publications-by-type/other-publications-reports/semiannual-risk-perspective/semiannual-risk-perspective-spring-2017.pdf

Page 8
Stephanie Avakian, Co-Director, SEC Division of Enforcement, The SEC Enforcement Division's Initiatives Regarding Retail Investor Protection and Cybersecurity, October 26, 2017, https://www.sec.gov/news/speech/speech-avakian-2017-10-26

Page 10
Large Financial Institution Rating System; Regulations K and LL, A Proposed Rule by the Federal Reserve System, August 17, 2017, https://www.federalregister.gov/documents/2017/08/17/2017-16736/large-financial-institution-rating-system-regulations-k-and-ll

Page 11
Bank for International Settlements Annual Report, June 2017, p.11, https://www.bis.org/publ/arpdf/ar2017e.pdf.

KPMG

Contact Us

Amy Matsuo
Principal
Regulatory Insights
T: 919-664-7302
E: amatsuo@kpmg.com

Dave Remick
Partner
Cybersecurity and Data Privacy
T: 404-222-3138
E: jremick@kpmg.com

Homer Hill
Principal
Risk Management Governance and Control
T: 212-872-6731
E: homerhill@kpmg.com

Deborah Bailey
Managing Director
Financial Services Regulatory Insight
Conduct and Culture
T: 212-954-0897
E: dpbailey@kpmg.com

Todd Semanco
Partner
Compliance Risk Management
T: 412-232-1601
E: tsemanco@kpmg.com

Michael Lamberth
Managing Director
Compliance Risk Management
T: 804-241-2795
E: mlamberth@kpmg.com

Terry Pesce
Principal
Financial Crimes Compliance
T: 212-872-6272
E: tpesce@kpmg.com

Dave Reavy
Partner
Strategic Risk and Disruption
T: 212-763-1622
E: dreavy@kpmg.com

Tracy Whille
Principal
Fiduciary and Investor Protection
T: 212-954-2691
E: twhille@kpmg.com

Brian Hart
Principal
Data and Analytics
T: 212-954-3093
E: bhart@kpmg.com

Chris Dias
Principal
Capital and Liquidity
T: 212-954-8625
E: cjdias@kpmg.com

Frank Manahan
Managing Director
Capital and Liquidity
T: 212-954-3660
E: fjmanahan@kpmg.com

Jitendra Sharma
Principal
Geopolitical Uncertainty
T: 212-872-7604
E: jitendrasharma@kpmg.com

Contributing Authors
Amy Matsuo
Principal
Regulatory Insights

Karen Staines
Director
Financial Services Regulatory Insight Center

kpmg.com/socialmedia