10 Key regulatory challenges for 2018 & Third Party Risk Management

Presenters:
Edmund Green, Managing Director
Homer C. Hill, III, Principal

February 28, 2018
Discussion Outline

• Overview of Top Ten Key Regulatory Challenges 3-4
• Cybersecurity and Data Privacy 5
• Risk Management Governance and Controls 6
• Conduct and Culture 7
• Compliance Risk Management 8
• Financial Crimes Compliance 9
• Strategic Risk and Disruptions 10
• Fiduciary and Investor Protections 11
• Data Analytics 12
• Capital and Liquidity 13
• Geopolitical Uncertainty 14
• Third Party Risk Management 15 - 20
• Open Q&A
Ten key regulatory challenges for 2018

The dramatic lessening of regulatory challenge expected to result from the deregulatory policy agenda has not been realized. We anticipate regulators will expect companies to continue to strengthen their overall core risk management governance, controls, practices, and reporting throughout 2018.

Cybersecurity and Data Privacy
Cybersecurity and the protection of data are a top priority to organizations and a great concern to regulatory bodies because data breaches can have a severe impact on organizations, trusted third parties, and individuals. The use of third party vendors adds an additional risk dimension to this issue.

Risk Management Governance and Controls
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. Third party risk management (TPRM) is amongst the chief concerns in this area.

Conduct and Culture
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.

Compliance Risk Management
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. Strong focus by regulators on TPRM

Financial Crimes Compliance
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.
## Ten key regulatory challenges for 2018 (continued)

<table>
<thead>
<tr>
<th>Number</th>
<th>Challenge</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>06</td>
<td><strong>Strategic Risk and Disruptions</strong></td>
<td>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.</td>
</tr>
<tr>
<td>07</td>
<td><strong>Fiduciary and Investor Protections</strong></td>
<td>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.</td>
</tr>
<tr>
<td>08</td>
<td><strong>Data and Analytics</strong></td>
<td>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.</td>
</tr>
<tr>
<td>09</td>
<td><strong>Capital and Liquidity</strong></td>
<td>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.</td>
</tr>
<tr>
<td>10</td>
<td><strong>Geopolitical Uncertainty</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
Cybersecurity and data privacy

In 2018, firms should make embedding cybersecurity and data privacy compliance into enterprise risk management programs and IT decisions a priority.

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Key actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greater use of emerging technologies and connected customer channels</td>
<td>Evaluate and strengthen identity and access management capabilities</td>
</tr>
<tr>
<td>Increased incidence and impact of cybersecurity attacks</td>
<td>Establish and operationalize cybersecurity and data privacy governance channels</td>
</tr>
<tr>
<td>Financial and reputational risks resulting from cyber incidents</td>
<td>Identify and address at-risk business processes and data</td>
</tr>
<tr>
<td>Heightened public sensitivity to data privacy and data protection</td>
<td>Conduct data protection impact assessments</td>
</tr>
<tr>
<td>Evolving state, jurisdictional, and global privacy regulations and regulatory expectations</td>
<td>Identify and introduce data subject related capabilities</td>
</tr>
<tr>
<td></td>
<td>Establish or enhance incident response protocols, business resilience framework, and communications plans</td>
</tr>
<tr>
<td></td>
<td>Consolidate and converge cyber and privacy technologies</td>
</tr>
<tr>
<td></td>
<td>Perform internal and external threat assessments</td>
</tr>
</tbody>
</table>

“Cybersecurity is maybe the single most important risk that our financial institutions, our economy, our government institutions face.”

—Jerome H. Powell
Risk management governance and controls

To respond to heightened regulatory expectations, financial services companies must improve risk identification, scenario analysis, business line accountability, issues management, third-party management, and reporting.

**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)

**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

In 2018, regulators will focus on institutions’ efforts to operationalize a measurable conduct risk management framework that prevents misconduct at its root; Establishing strong controls that include continuous governance, oversight and monitoring is critical.

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Key actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Continued regulatory and supervisory focus on financial services companies’ abilities to effectively monitor and manage conduct risk</td>
<td>— Establish and operationalize the conduct risk management framework</td>
</tr>
<tr>
<td>— Enforcement actions related to sales practices, client suitability, market manipulation, and fraud</td>
<td>— Align and integrate conduct risk programs with the existing risk and compliance program</td>
</tr>
<tr>
<td></td>
<td>— Perform business practice activity reviews</td>
</tr>
<tr>
<td></td>
<td>— Assess behavioral and root cause drivers and values</td>
</tr>
<tr>
<td></td>
<td>— Define culture and conduct governance, metrics, and reporting standards</td>
</tr>
<tr>
<td></td>
<td>— Set up and execute communication plans</td>
</tr>
<tr>
<td></td>
<td>— Conduct change impact assessments</td>
</tr>
</tbody>
</table>

"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
Compliance risk management

Now that the pace of new regulations has slowed, companies should turn their attention to creating an integrated compliance risk management program that drives greater collaboration between compliance and the rest of the organization.

### 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

### 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

“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
# Financial crimes and compliance

Financial services companies face an increasing need to integrate and automate Financial Crimes activities to facilitate data and reporting requirements and effect cost containment measures.

## 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

## 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

---

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
Strategic risk and disruptions

Adopting new innovations, including enhanced automation and regulatory technology, is a key focus area for 2018 that necessitates companies establish change governance, quality testing, and capacity and skills base changes to reduce technology change risk.

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

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

“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
Fiduciary and investor protections

Market participants must enhance risk management and conduct programs, improve data integrity and reporting protocols, implement effective misconduct controls, and drive greater accountability in their clients and portfolios.

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

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."

—OCC National Risk Committee
Data and analytics

Evolving regulatory requirements along with increasing competitive pressures are driving the need for enhanced technology, automation, quality checks and reporting processes at all levels of an organization, including customers, financial activity, employee behavior, and third party transactions.

<table>
<thead>
<tr>
<th>Drivers</th>
<th>Key actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Heightened expectations for data capture, governance, analysis, and</td>
<td>— Invest in technology and automation for data feeds, pulls, aggregation, and effective usage</td>
</tr>
<tr>
<td>reporting, inclusive of customer, financial activity, employee, and</td>
<td>to drive enhanced regulatory and compliance reporting, analysis, and monitoring</td>
</tr>
<tr>
<td>third party</td>
<td>— Conduct enhanced root cause and predictive risk analysis</td>
</tr>
<tr>
<td>— Evolving regulatory requirements for recording and reporting</td>
<td>— Expand loss scenario analyses to enhance operational controls and predictive analysis</td>
</tr>
<tr>
<td>information (including equities and options)</td>
<td>— Establish and operationalize enhanced data and model risk governance and management,</td>
</tr>
<tr>
<td>— Large financial and reputational impacts associated with regulatory</td>
<td>including data management and integrity as well as model development and validation</td>
</tr>
<tr>
<td>reporting</td>
<td>— Utilize data to predict and/or identify potential risks in real time</td>
</tr>
<tr>
<td>— Increased regulatory expectations for nonfinancial data accuracy</td>
<td></td>
</tr>
<tr>
<td>and completeness on management, Board of Directors, and regulatory</td>
<td></td>
</tr>
<tr>
<td>reporting</td>
<td></td>
</tr>
<tr>
<td>— Competitive pressures for cost reduction</td>
<td></td>
</tr>
<tr>
<td>— Maintenance and management of models</td>
<td></td>
</tr>
</tbody>
</table>

"[T]he increasingly important role played by data and the movement of data on computer platforms means that the stakes around ensuring data integrity are even higher. This will be one of the primary risks we must solve for in a digital world."

— J. Christopher Giancarlo, CFTC Chairman
Capital and liquidity

Recent regulatory reform and legislative proposals appear to focus on risk management and a move toward fewer capital and liquidity requirements for smaller firms and more streamlined requirements for larger firms.

**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

**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

Companies with global reach may be affected by perceived protectionist public policies that could force a reassessment of capital and staffing allocations and third party relationships. Global regulations such as GDPR and MIFID II will directly impact areas of global operations, including compliance and tax functions.

### Drivers

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

### 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

"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."

— Federal Reserve Board
Regulatory Focus: Third Party Risk Management
What is TPRM?

• A process of [proactively and consistently] identifying, analyzing and treating potential threats resulting from third party relationships

• Includes risks to strategy, operations, finances or reputation

• “…A third-party relationship is any business arrangement between [a bank] and another entity, by contract or otherwise”

• It is an ongoing activity, beginning with strategy, and including initial screening, contracting, ongoing monitoring and exit planning over the entire TPM relationship lifecycle
Why Focus on TPRM? - Regulatory Drivers

OCC 2013-29

• Comprehensive guidance requiring banks to proactively manage ALL risk to ALL Third Parties

• Sets expectation that [banks] will practice effective risk management, regardless of whether an activity is performed internally or through a Third Parties

• Use of Third Parties does NOT diminish responsibility of Mgt and BoD to activities are performed in a safe and sound manner
Why focus on TPRM? - Business Drivers

- ~40-60%+ of Breaches
- ~70% of Companies Fail to adequately manage TP risk
- ~90%+ planned to increase us of TPs
- Interconnectedness
- Interdependency
- Mobile/Open Architecture
- Innovation/Speed to Market/Omni-channel
Why Focus on TPRM?- Business Justification

Reduce likelihood of:

- Data breaches and related costs
- Operational Failures
- Reputation risk
- Adverse Financial impact due to vendor bankruptcy, counterparty default or unplanned termination
- Adverse customer experience
### TPRM Implementation - Key Success Factors

<table>
<thead>
<tr>
<th>Establish strong governance structure</th>
<th>To provide clear and consistent tone from the top (i.e., communication from senior management and the Board) and drive implementation efforts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sufficient Funding/Headcount</td>
<td>Ensure sufficient funding and staffing</td>
</tr>
<tr>
<td>Enterprise-wide adoption and implementation</td>
<td>Consistent processes are followed across the organization to drive efficiency and scale in managing third party risks</td>
</tr>
<tr>
<td>Technology enablement</td>
<td>Timely configuration/implementation of a technology platform to support the third party risk management lifecycle processes</td>
</tr>
<tr>
<td>Quality data</td>
<td>Availability of quality data to support the monitoring and reporting of risks associated with the third-party portfolio</td>
</tr>
<tr>
<td>Establish a realistic timeline for implementation</td>
<td>Management needs to be aware and establish a realistic implementation timeline</td>
</tr>
</tbody>
</table>
Questions and Answers
Edmund Green

Professional and industry experience
Edmund is a Managing Director in KPMG LLP’s Risk Consulting practice with nearly 30 years of cross-functional experience, including commercial and consumer credit, treasury operations, risk management, and internal controls, primarily with Fortune 500 Financial Services companies. His main focus at KPMG is on assisting clients with implementing or improving their Enterprise Risk Management (ERM) programs and processes, with emphasis on governance, risk assessment, reporting and training. He has also assisted clients in area of third party risk Management (TPRM), risk culture and incentive compensation risk assessment. His clients include both the commercial and government sector organizations.

Prior to joining KPMG in 2006, Edmund was a First Vice President in the CFO Risk and Control Division of a consumer credit card bank with assets of $189 Billion, where he led the implementation of SOX §404 for several functional areas including Treasury, Investment and Funding, Third Party Risk Management and Affinity Compensation. His previous experience includes nine years in commercial banking specializing in commercial credit and cash management for large corporate and middle market companies in the manufacturing and distribution industries. He also served four years as a Division Treasurer and Director of Treasury Process and Technology for a multi-line Fortune 500 insurance company with assets of $99 Billion. Edmund successfully led the development and implementation of the company’s first corporate-wide treasury Business Continuity Program and shared services strategy development process. His prior experience includes nine years in commercial banking, lending to large corporate, middle-market customers, as well as specialized lending in transportation and equipment finance, construction and commercial leasing and commercial cash management.

Representative clients
Publications and speaking engagements


Other activities

Board memberships: United Way of Delaware (2006 to Present) – Chairman, Audit Committee (June 2013 to Present), Finance Committee Chair (2008 to 2013)
Homer C. Hill, III

Professional and industry experience
Homer is a Principal in KPMG’s Regulatory Risk Services practice with more than 29 years within the Federal Reserve System distinguished by extensive supervisory and operations management leadership. He has a proven record of handling some of the most complex supervisory relationships including guiding three top global banks through significant regulatory changes and actions. His broad supervisory experience spans SIFIs, major foreign banks, regional and community banks. Furthermore, he has ability to transform organizations with proficiency in developing and managing large, multi-function teams.

His past and current experience includes:

- Selected to develop and manage the supervisory program for a foreign Systemically Important Financial Holding Company faced with significant turmoil and numerous regulatory actions.
  - Directed a team of 22 examiners including Deputy SSO, business line specialists, risk specialists and analysts.
  - Assessed the institution’s financial condition, revenue drivers, risk exposures and risk management framework, as well as developed risk indicators and risk assessments based on supervisory expectations and industry best practices.
  - Presented supervisory findings and regulatory compliance to the supervised firm’s Senior Management and Board of Directors, as well as FRBNY Management and the Board of Governors.
  - Consulted with Home Country Regulators, the European Central Bank’s Joint Supervisory Team, UK PRA, Federal Reserve Board Staff, other Reserve Banks and other regulatory agencies to ensure effective supervisory oversight.
  - Challenged the firm’s management on its business model, liquidity risk management assumptions, robustness of its stress testing techniques and preparedness to meet Intermediate Holding Company regulatory requirements.
Homer C. Hill, III (continued)

— Served in similar lead roles supervising several SIFI’s and foreign banks with specific focus on Enterprise Risk Management, Governance, and Enhanced Prudential Standards.

— Served as Chief Operating Officer working directly with the Executive Vice President of Supervision to manage day-to-day operations of the largest group in the Federal Reserve Bank of New York with more than 725 employees.
Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.