KPMG

Ten key regulatory challenges of 2019

Resiliency amidst innovation

kpmg.com

Contents

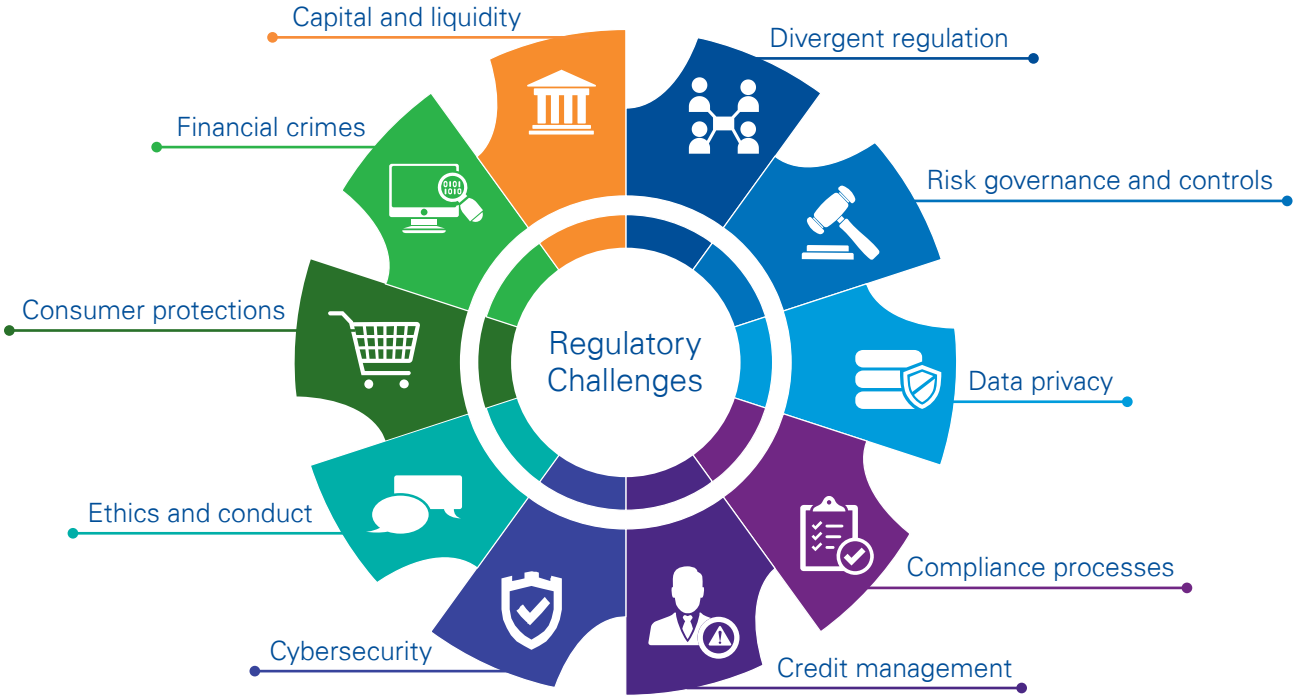
Introduction

The financial services industry is experiencing dramatic transformation, challenging both regulators and traditional financial services firms to keep pace.

Fueled by rapid emerging technologies, global interconnectedness, changing economic and jurisdictional factors, competition and consumer demand, firms are innovating—embracing new business models and adopting automation to support their operations and regulatory obligations. As firms pursue greater agility and resiliency, they are expanding their use of advanced data analytics, artificial intelligence, and innovative technologies, triggering further risk governance adjustments and regulatory attention in areas including safety and soundness and consumer protections.

In 2019 and beyond, regulators will assess how firms are adapting to market pressures and managing the associated risks, focusing on firms' operational resilience, governance and controls, data security, and consumer protections—and expecting all to align with ethical and sound conduct practices.

KPMG highlights the key drivers and actions for firms in the following Key Ten Regulatory Challenges for 2019:



Divergent regulation

Drivers

- Regulatory focus on recalibrating existing federal regulations
- New state financial services legislation and regulation
- State attorneys general actions
- Global divergence in regulation
- Implications of jurisdictional policies and actions
- Growing awareness of reputational and strategic risk

Challenges

Federal financial services deregulation has moved to "recalibrate" the requirements and "tailor" application of existing regulations. Notable examples include efforts to amend the enhanced prudential standards and Volcker Rule implementing regulations. Regulators will continue to focus on supervision and horizontal reviews. Consumer and investor protection issues, including suitability, affordability, and fair treatment as well as the role of the CFPB will be prioritized in legislative dialogue, with any new regulations via bipartisan support. There is potential for increased Congressional oversight investigations in areas such as large bank supervision, workplace retirement accounts, community reinvestment, and antidiscrimination and diversity issues.

Regulatory activity will be driven via:

- **Individual state-enacted laws and promulgated regulations**—Examples include California's privacy law, New York's cybersecurity regulation, and New Jersey's fiduciary rule proposal. In other actions, states have filed lawsuits to thwart federal actions (such as the OCC's new fintech charter) and created new supervisory units, such as Pennsylvania's Consumer Financial Protection Unit. State attorneys general are also pursuing actions, inclusive of coordinating with the DOJ, to enforce consumer protection laws in areas such as elder financial exploitation, fair lending, and data privacy and data security.
- **Other federal agencies**—These include the FTC and the FCC in areas such as data privacy and mobile payments. The DOC is actively engaged in setting up national standards for cyber security, and the DOL's original fiduciary rule continues to influence the expectations of legislators, regulators, and consumers.
- **Nonbank supervision**—Payday lending is largely state regulated; however, there is renewed interest from federal banking agencies in short-term, small-dollar loans after many banking entities exited the market. Fintech firms are providing services such as payments processing and data aggregation, but can operate outside of prudential bank supervision. The OCC fintech charter remains opposed by states. Evolving regulatory coverage and standards are of key importance in areas of high innovation such as artificial intelligence and cryptocurrencies.
- **Jurisdictional policies** —These include sanctions and tariffs, which trigger the potential for retaliation, not only to countries but to global financial service providers and to a globally connected market. Such policies often force changes to business strategies, staffing, and capital allocations. Other jurisdictional events, such as the U.K.'s Brexit, necessitate similar reassessments.

KPMG

Key actions

- Integrate regulatory inventory and rule mapping to operational controls.
- Operationalize and assess controls to address varying legal and regulatory requirements across jurisdictions, including state versus federal and cross-border.
- Identify interdependencies in business, product, and vendor process and controls for potential jurisdictional risks.
- Assess strategic, operational, and reputational impacts of emerging financial and nonfinancial risks.
- Retool risk assessments, as appropriate.
- Formalize incident and issues management governance, processes, escalation, and reporting.
- Reassess capital and human resource strategies and allocation.
- Evaluate tax implications to changing regulatory policies.
- Complete change impact assessments.

> "The fragmented nature of the U.S. financial regulatory system undercuts efforts by regulators to support innovation…Fragmentation also raises the likelihood of inconsistency among regulators. To be effective, a coordinated effort is needed…"

Source: U.S. Department of the Treasury, Report on Nonbank Financials, Fintech, and Innovation, July 2018

Risk governance and controls

Drivers

- Heightened regulatory standards and expectations for the strong risk management practices
- Examiner focus on conduct, reputational, and strategic risks
- Agile business adoption of new technologies, new products, and new market entrants (e.g., fintech, regtech)
- Cost containment initiatives driving risk convergence and transformational initiatives
- Continuing market and consumer/demographic shifts
- Third-party providers, aggregator, and partner risks

Challenges

Financial service providers must maintain governance and controls within their risk management frameworks for sustainability, resiliency, and efficiency.

Key areas of focus include:

- **Strengthening of risk management practices**—Examiners expect firms to strengthen oversight and assign specific accountability for the management of risks facing the firm, including enterprise risk identification, risk assessment, scenario analyses, issues management, controls, and reporting capabilities. Examiners assess how well operational controls enable appropriate risk management practices in practice.
- **Third-party risk management**—Third parties, aggregators, and partners can present significant reputational risks to firms, even when acting seemingly independently from the financial institution (e.g., fraud, sanctions, human trafficking). Furthermore, regulators are concerned about firms' abilities to manage and mitigate their exposures from third parties (e.g., compliance failures, cybersecurity weaknesses, data privacy breaches). Proper risk management must be supported through controls—initial and ongoing due diligence, risk assessments, monitoring, and auditing of third-party relationships, proper staffing allocations—and governance.
- **Risk governance**—Risk governance (inclusive of risk committees) is central to helping assess risks. Firms must demonstrate an ability to effectively measure and mitigate risks but also anticipate and prevent risks, demonstrate resiliency and an ability to timely adapt to market shifts. Regulatory guidance reconfirms the role of the Board of Directors and management in the risk governance structure.
- **Change management**—Change management capabilities must support firms as they pivot business models, delivery models, automation, and reliance on third parties, among others shifts. Critical change management efforts—across people, processes, and technology—are critical to successful risk awareness and mitigation execution.
- **Information technology and data governance** —Technology is elevating firms' ability to aggregate data (structured and unstructured) in real time and providing a deeper appreciation of risks enterprise-wide, including through dashboard visualization capabilities. Regulatory expectations for model risk validations of technology systems, data governance, and for the validation and reporting of data for regulatory purposes are growing.
- **Additional risks**—The Federal Reserve's inaugural Supervision and Regulation Report identifies deficiencies and focus areas to include: Conduct, reputational and strategic risks (*see Section 7*); cybersecurity (*see Section 6*); BSA/AML (*see Section 9, Financial Crimes*) and Internal Audit functions.

KPMG

Key actions

— Determine if operational controls, particularly for high-risk regulatory requirements, are functioning effectively.

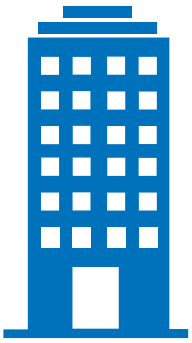
— Engage with stakeholders to evaluate ways to enhance agility in risk management.

— Build change management components/steps into project plans.

— Identify processes or controls to converge in support of a stronger risk management approach enterprise-wide.

— Revisit data governance programs and protocols and refine them as necessary to meet regulatory scrutiny and to prepare for future automation efforts.

— Further integrate third-party risk management efforts across performance-based areas, jurisdictions, risk functions, and disciplines for improved governance and oversight.



40% of large financial institutions are rated "less-than-satisfactory"

Over **50%** of examiner findings for LISCC firms are related to governance and controls weaknesses.

Source: Supervision and Regulation Report, November 2018. Board of Governors of the Federal Reserve System.

Data privacy

Drivers

- Heightened public awareness of the value of and risks to consumers' personal data
- High-profile, widescale, publicized breaches
- Heightened expectations regarding the breadth of consumer information to be protected and consumers' rights to control use of their data
- Highly interconnected financial systems with multiple entry points
- Complexity of legal and regulatory landscape

Challenges

Recent high-profile data breach and data sharing incidents have put a spotlight on how, through digital transformation and the rise of the internet, companies and consumers around the globe have become significantly interconnected. There is a general consensus, here in the U.S. as well as globally, that the privacy of data, both for companies and consumers, should be protected. There is not, however, consensus on the parameters of a data privacy framework, including scope, protections, and oversight. In the U.S., this is further challenged by the fact that, at present, there is not one overarching law or regulation governing data privacy; many lawmakers and companies are seeking to influence the debate. The potential for global application of the EU's GDPR is causing all to focus on options.

Accordingly, expectations regarding data privacy and security are evolving on all fronts:

- **Federal standards being considered**—The DOC has requested comment on behalf of the Administration regarding a principles-based approach to consumer data privacy. As outlined, the plan would look to realize certain key outcomes benefitting users/consumers including transparency, control, security, minimization, access and correction, risk management, and accountability. The FTC would generally have the enforcement authority for consumer privacy violations even though the banking, financial, and healthcare regulators have rules in place governing the collection, storage, and use of personal data. The Administration's effort is largely viewed as an initial step toward drafting a federal data privacy law. Concurrently, numerous Congressional hearings have focused on data privacy issues, including a federal standard, consumer rights, and the EU's GDPR. Support for federal legislation is building in order to preempt and simplify a multilevel patchwork of standards from the states and federal regulators. Notably, multiple nonfinancial companies, including major technology companies, have advocated for a federal privacy law.
- **State laws being enacted**—State laws being enacted – California has adopted AB 375, the California Consumer Privacy Act of 2018 (CCPA), which draws upon many of the provision of the EU's GDPR. It is considered to be the most stringent consumer privacy law in the U.S. and will apply to California residents (beginning January 1, 2020). Other states will likely follow California's lead; currently, all 50 states have data breach notification laws in place, and some are adding requirements to expand the scope of personal information and impose specific data security requirements. Based on the obligations laid out in the CCPA, the burden for companies to comply if other states implemented similar but nonunified legislation would be substantial.

KPMG

— **Extraterritorial nature of GDPR**—The EU's GDPR is applicable to all companies globally that handle the personal data of individuals in the EU and subjects those firms to large fines and penalties for failure to protect an individual's privacy rights. Such broad application is forcing firms, on an individual level, to reconsider privacy policies (holding all customers to the same standards rather than tracking a few) and their operating models (where they do business).

— **Customer demands**—Millions of customers affected by the high-profile data breaches now seek greater control over the collection, use, and retention of their personal information causing firms, independent of regulatory requirements, to reconsider policies regarding opt-in and opt-out procedures and the transparency of disclosure regarding the data to be collected, who may have access to it, and how it will be used.

The forthcoming changes will challenge firms to develop a thorough understanding of their data security and privacy risk assessments as well as the current mitigating controls (across the firm and by third parties), and to identify areas where additional efforts are needed to strengthen the effectiveness of their programs.

Key actions

— Inventory the personal data that is collected, processed, stored, and shared; identify data that is "critical" to the organization.

— Implement data mapping capabilities that can tie all data processing activities to data records of individual consumers.

— Perform root-cause analyses of prior known inappropriate data sharing or data breaches.

— Develop, implement, and maintain written policies and procedures for data protection and security, to include:

- Identity and access controls
- Data lineage governance
- Third-party data stewardship
- Monitoring and testing, and escalation and reporting protocols
- Communication and notice
- Customer protections/rights.

— Link data privacy programs with programs focused on cybersecurity, information lifecycle, legal hold and discovery, and incident management.

— Implement culture-change protocols to reinforce employee responsibilities with regard to third-party data sharing.

89% prioritize protecting customer data.

Source: Growing Pains: 2018 U.S. CEO Outlook, KPMG

Compliance processes

Drivers

- Increased market competition and pressure to cut operating costs
- Expanded role of ethics and compliance, requiring greater diversification of skill sets
- Regulatory expectations of stronger compliance management in the first line
- Expectations by leadership for more "real time" compliance risk management, including upon trigger events, and consistent view of compliance risks enterprise-wide
- Renewed regulatory focus on trade reporting, and record and data retention

Challenges

Firms are focused on bridging business and compliance objectives while avoiding regulatory, compliance, and ethical risks. At the same time, compliance leaders face an expanded mandate that increasingly includes culture/conduct, data privacy, and financial crimes among other regulatory obligations, a cost cutting corporate environment and regulatory priorities that include compliance and operational resiliency.

Yet, advances in artificial intelligence and automation present opportunities to incorporate digital transformation to meet their challenges—operationalizing compliance within first line processes and controls, while simultaneously enabling organizations to respond with greater agility to shifts in consumer behavior and a tight employment market. To take advantage of such technology, firms must first reassess their core processes and controls to determine where more streamlined governance and enhanced risk management might add the most value.

In particular, firms should look at:

- **Increased governance expectations for the board of directors**—The Federal Reserve has made clear that it views compliance breakdowns as weaknesses of governance and board oversight and it will hold the board accountable for its responsibilities. Firms must actively manage the flow of information to the board to keep it properly informed of aggregate compliance risks and to enable the board to provide clear, aligned, and consistent direction on the firm's strategy and risk tolerance.
- **Converging compliance risks and controls**—To further drive consistency in managing ethics, compliance, and reputational risks, firms are further converging their risks and controls across operational and business units and also across governance, risk, and compliance levels, enabling leadership to gain one consistent view of enterprise-wide risks, and pinpointing areas of highest risk. In addition, as regulators look to assess the strength of compliance risk-management practices in business lines, convergence and further operationalization of compliance controls orient employees to the firm's risk strategy and highlight risk outliers with greater specificity.
- **Required regulatory rule changes**—The OCC has specifically highlighted change management processes as a supervisory priority in 2019, noting that failure to properly and timely implement changes could result in compliance and reputational risk as well as statutory damages and civil liabilities in some cases. Other factors, such as complex regulatory structures and uncertainty, merger and acquisition activity, new products and services, and talent constraints, are further challenging firms' efforts to update supporting operating systems and manage existing compliance management systems. In response, firms can map their regulatory obligations (previously inventoried) and risks to the appropriate functional level

KPMG

of business controls, facilitating a quicker impact analysis, strategic plan, and implementation of changes. In addition, anticipated reforms to CRA will necessitate a focus on impacts to service, lending and investment strategy, inclusive of property optimization, tax implications, and data quality and reporting.

— **Consolidating testing, surveillance and investigations**—Firms need to further integrate and coordinate across disparate compliance activities inclusive of testing, surveillance, and investigations, and deploy data analytics and metrics that are multidimensional across these for a more comprehensive understanding of compliance risks and pockets where gaps exist. Data must be de-duplicated for an accurate perspective of where risk is pervasive, to assess the materiality of risks and to evaluate trends, root causes and systemic issues for further addressment. Automation and integration can break down silos and consequently drive positive cultural and ethical changes, in a more cost efficient way.

Firms face additional compliance challenges from:

— **Renewed regulatory focus on trade reporting**—Regulators are renewing their focus on nonfinancial regulatory reporting, specifically looking for timely, accurate, and complete information on a continuous basis, propelling firms to evaluate process automation options. Furthermore, as the "second phase" of CAT (Consolidated Audit Trail) reporting commences for large broker-dealers, budgets and resources are expected to remain challenged.

— **Attention to records/data retention**—The SEC and the CFTC are both examining firms' awareness of where their data is stored, the format in which it is stored, how to retrieve it in a timely manner, and how and when it is destroyed. The two agencies do differ on expectations regarding the format in which data is stored, and firms subject to supervision by both agencies must assure they meet the relevant requirements.

— **Third-party relationships**—Third-party relationships can present reputational or financial risk to the firm, particularly when they engage in fraud or misconduct.

— **Charismatic leaders**—Charismatic leaders can be a hindrance if they do not allow for effective challenge and/or they restrict the flow of information and data about risks.

Top compliance automation challenges

Only 1 in 5 CCOs and CIOs have an enterprise-wide strategy for compliance automation. Compliance automation is challenged by:

Misunderstood and/or insufficiently managed dependencies	39%
Leadership and/or stakeholder attention	36%
Insufficient metrics for measuring progress	35%
Unavailable resources	32%
Unavailable data or data did not have the anticipated integrity	26%

Source: KPMG Compliance Automation Survey 2018

Key actions

— Refine compliance metrics and data analytics to provide more valuable, and consistent, risk information to the board.

— Identify opportunities to converge controls across the three lines of defense for more streamlined compliance, improved risk management, and enhanced first-line ownership of compliance risks.

— Evaluate regulatory change management processes in place, including agility and resiliency of those processes.

— Determine where silos between discrete compliance activities can be further broken down for a more integrated compliance risk management approach, and enhanced effectiveness.

— Develop a plan to achieve more "real-time" compliance based upon compliance risks, data availability, and integrity.

Credit management

Drivers

— Economic shifts and increasing interest rates

— Changes to accounting standards and regulatory requirements

— Heightened regulatory concern for trends in leveraged lending and securitization

— Identified supervisory priority for banking organizations

Challenges

While it is difficult to predict the peak of a market and the beginning of a recession, financial services firms must always be prepared for market shifts. Some industry participants have begun to voice concern as well as speculation that the U.S. economy might experience a shift in 2019. With interest rates rising, the financial services industry could be faced with increasing credit-related risk—and a heightened regulatory focus aimed at ensuring firms' practices are evolving to respond to those risks as they emerge. The OCC and the Federal Reserve have each identified credit risk among their top supervisory priorities.

Key areas of focus include:

— **Commercial and retail loan underwriting and concentration risk management**—Supervisory findings indicate firms are seeking interest income and loan growth to meet strategic objectives, causing intense competition in the market and leading to eased underwriting standards (as firms move downstream in credit profiles), complacent loan administration, and increased credit risk.

— **Credit Risk Management**—Emerging risks, loosened underwriting standards, policy exceptions, rapid loan growth, rising interest rates, and commercial real estate concentrations have all contributed to an increased need to monitor and assess credit risk management practices. In addition, due to low loss numbers, many organizations have placed less focus on the importance of credit risk management and its role within their organizations.

— **Moving toward lifetime loss estimates**—The new CECL standard will impact a firm's operations (including accounting/finance, IT, risk, pricing, and business units) and financial results (through impairment estimates, capital ratios, and profits and losses). Firms should be cognizant of and follow the development of the federal banking regulators' proposed rules that would permit all banking organizations the option to elect a three-year phase-in of the "day 1" regulatory capital effects from adopting CECL if they experience a reduction in retained earnings.

Additional considerations related to credit risk might include the following:

— **Shift away from LIBOR to alternate risk-free rates (RFR)**—The transition from an uncollateralized rate to an RFR will necessitate changes to market pricing and give rise to risk management considerations. There will be a fundamental change in how new loans, swaps, and other new products are priced, with the key changes rooted in how pricing desks treat credit-basis adjustments. Going forward, pricing cash or derivatives products that previously referenced LIBOR

KPMG

will need to reflect that the starting point for RFR products is an RFR rather than an AA bank rate. To the extent any models used a LIBOR curve, whether for pricing or risk management, a basis adjustment will be required to reflect the credit difference between LIBOR and the RFRs.

— **GAO finding regarding leveraged lending guidance**—Although the banking regulators have agreed not to enforce their Guidance on Leveraged Lending following the GAO finding that the guidance was a general statement of policy and a rule (which must be submitted to Congress for review), they have recently noted concern in this regard based on deals that have exceeded the previous set guidelines. In addition, they note concern for growth in loan products that are more risky for creditors, including so-called "covenant-lite" loans and loans that feature "collateral stripping."

— **Internal Controls and process infrastructure**—Supervisors will continue to focus on firms' efforts to build and implement better controls and infrastructure throughout the organizations covering the end-to-end processes necessary for product and service delivery.

Key actions

— Create an environment that embraces a strong credit culture that welcomes reasonable challenge of loan structures, approvals, and risk rating. Firms should place enhanced emphasis on their credit strategy and ensure it aligns with their credit risk appetite.

— Evaluate current underwriting processes and ensure that strategic objectives do not undermine asset quality and increasing risk in the cycle.

— Full parallel runs of CECL should begin in earnest in 2019. Firms should understand the full impact of the implementation of CECL and begin making adjustments to practices (including models, pricing, systems, and people) as necessary. Performance of parallel runs will ensure accuracy and adequacy of process to comply with CECL adoption.

— Perform gap assessments to ensure that strong processes are in place to manage the increasing risk though the next credit cycle.

Commercial and retail credit loan underwriting, concentration risk management, credit risk management, and the allowance for loan and lease losses, including preparation for CECL, are collectively one of the five supervisory priorities.

Source: OCC Fiscal Year 2019 Bank Supervision Operating Plan

Cybersecurity

Drivers

- Evolving and increasingly sophisticated technologies introducing new threat vectors
- Regulatory and consumer expectation for data protection, breach notification, and remediation
- Regulatory focus on operational resiliency
- Interconnected systems with multiple entry points
- Varying objectives for cyberattacks, including theft, destruction, and disruption

Challenges

Federal regulators repeatedly state that cybersecurity is a top regulatory priority, and yet, there is not one overarching national standard, federal law, or regulation addressing cybersecurity risks or information protection. Perhaps not surprisingly, the GAO has identified 10 "urgent" actions that it recommends the federal government take to address cybersecurity vulnerabilities.

Financial services firms are challenged to sustain a vigilant and focused defense against the ever-present and evolving threat to their proprietary data, consumer data, and operations as the regulatory environment also evolves.

Multiple forces are currently at work:

- **The Administration has released its National Cyber Strategy,** and the Pentagon has concurrently released its own Cyber Strategy. Multiple agencies are engaged in cybersecurity defense, though much of the guidance they develop is voluntary. These entities include the Department of Justice, the Department of Homeland Security, and the Department of Defense; the National Institute of Standards and Technology (NIST), which is part of the DOC, has established a Cyber Security Framework that is widely referenced,
- **Multiple federal financial services regulators have cyber requirements in place,** some of which are loosely aligned with the NIST Cybersecurity Framework. The federal banking agencies did publish an advance notice of proposed rulemaking on enhanced cyber risk management standards in 2016, but it has not yet moved forward. Financial institutions face layers of requirements and voluntary standards, including provisions of the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, state requirements, the NIST Cybersecurity Framework, the Payment Card Industry Data Security Standard, and the FFIEC's Cybersecurity Assessment Tool.
- **Individual states have stepped in to establish cybersecurity rules for their constituents,** most notably including New York's Department of Financial Services, which published Cybersecurity Requirements for Financial Services Companies. Key features include the designation of a chief information security officer (CISO), encryption of all nonpublic information in transit and at rest, multifactor or risk-based authentication, breach notification parameters, data retention/disposal policies, and annual reporting requirements.
- **Operational resiliency is a horizontal theme for 2019.** Considerations in that review will include a firm's key markets and products, key systems in place to support the business, and the security and resiliency in those systems against breach and/or failure. Firms will be expected to understand what a system or operational failure will imply for the firm, its counterparties, and the economy overall, and they should be to demonstrate solutions and controls to reasonably detect and

KPMG

mitigate cyber threats, including an ability to ring fence critical aspects of their program such as the security of systems access. Firms may be challenged to closely align cybersecurity risk management with their business and growth strategies.

— **The growing sophistication of cyber attacks** and the speed at which technologies are evolving can make it difficult for firms to keep up, increasing the risk of unauthorized access to operations and systems, and amplifying the risk of fraud, reputational damage, and an unavailability of key assets. Regularly maintaining and increasing the levels of preparedness is critically important to cyber defenses. Financial services firms have been challenged by:

  – Establishing cyber risk governance, including board oversight
  – Recruiting and retaining specialized talent, and training existing personnel to identify and report suspicious activity
  – Investing in new technologies, upgrading legacy systems, and integrating systems
  – Meeting incident response, notification, and disclosure requirements/expectations
  – Managing third-party data security and privacy risk.

Key actions

— Conduct cyber threat simulations to test controls and incidence response

— Evaluate cyber risk landscape and establish risk appetite alignment to drive effective mitigation prioritization

— Develop and implement a forward-looking comprehensive cybersecurity strategy based on this with flexibility to accommodate change (internal and external) and addressing:

  – Identification of the relevant laws, regulations, certifications and standards
  – Organization and governance, including board oversight, leadership, accountability, and reporting, and data science talent
  – Policies, procedures, and controls, including authentication and encryption protocols
  – Internal and external risk assessment and management
  – Integration with existing solutions and processes
  – Ongoing monitoring and testing, alert thresholds and triggers, trends analysis
  – Ongoing security and risk assessments
  – Incidence response, notification and reporting requirements, disclosures, and remediation, including identification of responsible/accountable personnel
  – Resilience and recovery measures for critical systems and data along with business continuity planning

— Design and layer multiple protective solutions to detect, prevent, and deter fraud.

The top three risks that threaten banking growth include:	**1**	Cybersecurity risk
	2	Operational risk
	3	Interest rate risk

Other risks include:	Emerging/disruptive technology risk
	Environmental/climate change risk
	Return to territorialism

Source: Growing pains: U.S. CEO Outlook 2018 Survey, KPMG

Ethics and conduct

Drivers

— Continued supervisory focus on the abilities of firms to effectively monitor and manage misconduct by employees, third parties, and partners/affiliates.

— High-profile regulatory enforcement actions and high-dollar civil money penalties involving sales practices abuses, client suitability, and trader misconduct.

— Increased awareness of nonfinancial risks, including reputational, strategic, and fraud risks, which can be tied to misconduct.

Challenges

Ethics and conduct remain a key supervisory priority for the financial services regulators. Following groundbreaking enforcement actions and related horizontal reviews, the regulators are focused on the efforts of firms to identify and prevent misconduct at its root. Key areas of concern include consumer data privacy, suitability of products sold to consumers, sales/trading practices, as well as general expectations for strong ethics and conduct in the offering and delivery of retail consumer and investment products and services. This supervisory focus is forcing firms to enhance governance, oversight, and monitoring activities across multiple processes, including trading activities, incentive compensation plans, and sales practices, in order to ensure they are not inadvertently incentivizing improper behavior.

Challenges to managing conduct risk include:

— **A broad definition**—Although industry participants and regulators can agree on and describe strong ethical behavior and conduct, they each define "conduct risk" very broadly. Larger firms are generally coalescing around a definition of conduct risk as any action of an institution or the broader industry that leads to consumer harm or negatively impacts market stability. The Federal Reserve Bank New York has defined "misconduct risk" as "the potential for behaviors or business practices that are illegal, unethical, or contrary to a firm's stated values, policies, and procedures." Regulators do expect the largest firms to establish a formal conduct risk management program/framework but have not yet published formal conduct risk standards or guidelines outlining their expectations.

— **Evolving frameworks**—The industry continues to mature in this area; many firms are actively working toward improving how they define, manage, measure, and report conduct risk. In particular, they are being challenged with:

- Defining the conduct risk appetite in quantifiable terms
- Identifying mechanisms to embed change and achieve conduct risk objectives
- Building up conduct risk tools, including capturing key components in the enterprise-wide taxonomy; providing or refreshing risk assessment tools to integrate conduct risk; and developing a controls inventory, data inputs, and evaluation approach
- Modeling metrics utilizing quantitative and qualitative conduct risk measures
- Streamlining investigations processes including complaint management, case documentation, root cause analysis, and remediation.

— **Expectations for governance**—Supervisors routinely evaluate the effectiveness of boards of directors and senior management charged with overseeing conduct

KPMG

and driving firm culture, the stature and investment in control functions such as internal audit, risk, and compliance, and the firm's response to incidences of misconduct. Their focus is directed toward decision-making practices and behavior as a core aspect of good governance, including risk identification, credible challenge, and early intervention. Lessons learned, and risk factors identified during investigations should be further integrated into the ethics/conduct risk program to facilitate root cause analysis across cases and the potential need for follow-up and remediation, as well as to reflect the degree to which incidences may be indicative of larger and/or systemic issues.

Large financial services companies are focused on:

Tone-at the top/governance	**91%**
Code of conduct	**73%**
Individual accountability	**55%**
Monitoring high-risk employees/surveillance	**55%**
Culture metrics	**55%**

Source: KPMG/RMA Operational risk management excellence survey, 2018.

Key actions

— Establish and operationalize a conduct risk and ethics management framework that:

  – Defines a measurable conduct risk program, including centralized oversight, governance and controls, and clear escalation protocols and reporting

  – Aligns and integrates conduct risk with the existing risk and compliance program

  – Clarifies responsibility for conduct risk management between the 1st and 2nd Lines of Defense

  – Includes risk assessments supported by metrics, triggers, and thresholds and monitoring and testing

  – Employs behavior analysis models for employees and consumers, including trends analysis

  – Reports business-level metrics covering client conflicts of interest, market conduct, training sanctions, and breaches.

— Revisit policies, procedures, and escalation protocols to ensure they are clearly documented and sufficiently robust.

— Invest in technology and/or tools to enhance surveillance, monitoring, and reporting.

— Enhance investigations processes to include complaint management, case documentation, root cause analysis, and remediation and further integrate with the conduct risk program.

— Develop and implement sales practices and incentive compensation risk assessments supported by testing and report results regularly to the board.

— Strengthen recruiting and hiring processes; expand employee exit interviews to include conduct and ethics questions.

Consumer protections

Drivers

— Heightened public awareness of the value and risks to consumer personal data and related regulatory scrutiny and change

— Consumer demand for integrated and personalized products and services (digital transformation—nonfinancial shopping experiences flowing through to financial experience expectations)

— Demographic shifts: younger consumers favor innovative technologies and have different "shopping" habits and expectations; senior consumers are a growing population demographic and source of risk from financial exploitation

Challenges

A heightened regulatory focus on consumer and retail investor protection will continue into 2019, led by challenges around the protection of consumers' personal data as well as "personalizing" their access to financial products and services. As previously discussed, throughout the industry there is a heightened awareness of the value of consumer personal data as well as the real potential for data breaches or misuse of information by organizations entrusted with it.

Expectations regarding consumer protection are evolving on all fronts with consumers' expectations adding to this challenge:

— **Consumers are seeking greater control** over the collection, use, and retention of their personal information causing firms to reconsider policies regarding opt-in and opt-out procedures and the transparency of disclosure regarding the data to be collected, who may have access to it, and how it will be used.

— **Younger consumers are demanding** an integrated, personalized experience that permits them to interact with firms through multiple platforms, increasing the data security and privacy risks at multiple entry points and pushing firms to invest in and implement new technologies or to enter into new third-party relationships.

— **Older consumers**, particularly those over age 65, are a fast-growing demographic that, on the whole, has a wealth of assets but may also struggle with technological advances, increasing their risk of misunderstanding, errors, complaints, and fraud. New protections permit firms to report suspected financial exploitation of seniors, potentially heightening consumer expectations for protections in this regard.

— **Expectations for a "personalized experience"** also anticipate that firms will know a consumer's preferences or needs and will be responsive to, and remember (i.e., document), their specific interactions and/or complaints. Similarly, firms must be cognizant of and comply with current guidelines for web content and mobile applications as set forth under ADA guidelines designed to improve information accessibility for disabled persons, including consumers and employees.

Firms may face additional customer protection challenges with regard to:

— **Data lineage, data quality, and automation**—The shift toward automation and cloud solutions highlights the importance of authenticating and tracking customer data across an organization, including its origins and integrity, the systems in which it resides, how it is used or shared, and governance. Notably, the DOJ discourages firms from using ephemeral, or self-deleting, communication streams that disappear after a certain amount of time, and firms should address the use of these communications methods both internally and externally in policies and procedures.

KPMG

— **Regulatory changes to consumer protection laws**—The EGRRCPA introduced new protections related to credit reports, service members, student loan borrowers, and seniors; additional changes were made to regulatory requirements under the HMDA, TILA, RESPA, and MLA.

— **Sales practices and trading activities**—Regulators' heightened attention to conduct risk includes a focus on the suitability of products and services sold to consumers, sales and trading practices more generally, incentive compensation programs, and controls to address broker-dealer misconduct.

— **"Fiduciary" and "Best interest" standards**—The DOL indicates it is "considering regulatory options in light of the Fifth Circuit decision" to vacate its Fiduciary Rule suggesting a new rulemaking may be forthcoming. The industry continues to await the SEC's Regulation Best Interest; a final rule is anticipated in 2019. Consumer protection issues surrounding "appropriate" fees and disclosures, suitability of products, and the differing responsibilities of broker-dealers and investment advisers will be ongoing.

Key actions

— Establish and operationalize strong governance and tone-from-the-top programs that adopt a customer-centric approach, require financial services representatives to act in the best interest of consumers and focus on fair consumer outcomes.

— Evaluate and strengthen the customer data protection program:

  – Revisit ability of consumers to opt-in or opt-out of data sharing.

  – Implement data lifecycle management capabilities that support individual rights such as data deletion and data portability.

  – Implement data mapping capabilities to identify all data records that relate to individual consumers.

  – Embed security and privacy principles within the innovation processes of the compliance framework to prevent data privacy abuses, reputation risk.

  – Design and implement a program of timely consumer communications on data issues, including the use of ephemeral apps.

  – Assess compliance with data privacy and consumer protection laws and regulations, including the ADA.

— Conduct consumer/investor and fraud protection assessments, particularly related to sales practices, fees, and vulnerable client portfolios, including seniors.

— Invest in tools and capabilities to better analyze employee and consumer behaviors as well as trends and patterns.

— Evaluate and enhance surveillance, monitoring, and testing.

Focusing on Main Street investors' long-term interests is a strategic goal, including:

1 Clarifying the standards of conduct governing investment professionals, and

2 Enforcement and examination initiatives related to misconduct.

Source: SEC Four Year Strategic Plan for 2018–2022

Financial crimes

Drivers

- Digital transformation overall
- Availability of new technologies, including by fintech vendors
- Regulatory expectations for increased integration and improved risk management abilities
- Closer partnership with the business to achieve agility and strategically align initiatives
- Market conditions (cost containment)
- Increased competition from new market entrants and need to innovate

Challenges

The digital transformation, changing how firms operate and deliver value to customers, is driving innovation across financial crimes compliance efforts. Greater agility, efficiency, effectiveness, and resiliency are required today, and firms are focused on automating and integrating their efforts to achieve these goals. Firms also continue to face intense regulatory pressures, increasingly coordinated across multiple regulatory jurisdictions and bodies, to contain attendant risks. In many cases, regulatory authorities expect firms to show greater ability to aggregate data across the enterprise, and understanding of their consolidated financial crimes risks, along with more consistency in their risk management approaches. Independently, firms are struggling to navigate the volume of data and multiplicity of sources and systems (both internal and external).

These challenges are forcing firms to work toward harmonizing financial crimes processes, reducing time per task, eliminating friction, enhancing coordination, and further embedding accountability within the business for financial crimes compliance.

Firms are considering a variety of approaches, including some that are targeted and others that are more extensive, including:

- **Increased standardization** of methodologies and tools across the enterprise
- **Convergence of controls and teams,** with refined responsibilities across the three lines of defense (for improved risk management)
- **Development of data analytics/ predictive analytics that are aggregated across various types of financial crimes** for a more holistic appreciation of current risks and to better predict future risk areas. Integrating business data and information into the financial crimes picture can provide valuable context as well, enabling greater predictive capabilities when viewed collectively, and optimally in real time
- **Further integration of financial crimes efforts**—AML, sanctions, antibribery and corruption (ABC), fraud, and human trafficking, including integration with the firm's overall compliance risk management efforts. When supported by formalized communication mechanisms, enhanced collaboration enterprise-wide, and aggregation of disparate data, integrated processes improve regulatory reporting abilities and risk monitoring, enabling firms to better predict emerging risks and implement preventive measures.
- **Automation of financial crimes processes**—Repetitive processes, especially due diligence processes related to customer onboarding, transaction monitoring, sanctions and fraud, are ripe for automation, including through use of blockchain technology. By automating aspects

KPMG

of these processes, firms may be able to identify misconduct and regulatory violations earlier in time, achieve greater consistency in output, and improve agility. As with any technology adoption, regulators remain keen to understand the firm's business decision-making process, whether the automation works as intended, any gaps and additional risks created by the technology, and the governance structures in place.

— **Resource sharing** through "collaborative arrangements" **by U.S. firms** with "less complex operations, and lower-risk profiles for money laundering or terrorist financing." Such collaborative arrangements will help firms that qualify to cover certain AML activities/requirements more cost efficiently. Firms opting into shared arrangements should utilize contractual agreements and expect regulatory examination of their arrangements. Globally, industry participants, including large banks, are looking to create such platforms, on a broader scale, bolstered by supportive regulators and innovative technology providers.

Firms face additional challenges from:

— Adjustments to U.S. economic and trade sanctions that arise from the U.S. foreign policy and national security goals, which impacts firms' compliance and operational risks

— Organizational needs for cost containment and other resource constraints

— Employees who are not "cultural fits"

— The quick pace of business changes that can present financial crimes risks outside firms' risk profile and tolerance, such as changes to asset classes (organic or through mergers/acquisitions), products and services, transactional activity including use of cryptocurrencies, or to the customer base— notably, the availability of large volumes of customer data and the growth of online transacting can present increased cybercrime risks and fraud risks in credit cards, which require more collaboration and coordination across the enterprise to manage and address.

> "Innovation has the potential to augment aspects of banks' BSA/AML compliance programs such as risk identification, transaction monitoring and suspicious activity reporting."
>
> Source: Joint Statement, December 3, 2018, FinCEN, Federal Reserve, FDIC, OCC, NCUA.

Key actions

— Evaluate what additional data analytics and emerging technologies can enable your firm to more predictively detect and respond to financial crimes risks, including from business data.

— Discuss the potential to automate certain compliance processes, such as fraud monitoring, in consideration of your firm's enterprise-wide strategy (if any), automation goals, timeline, regulatory risks, and availability of data.

— Determine how to further integrate financial crimes processes or structure for greater agility, cost savings, consistency, and refined risk evaluation.

— Plan for potential regulatory changes on the horizon—ongoing Sanctions refinements, expectations for monitoring and reporting human trafficking and for potential shared platforms/arrangements.

Capital and liquidity

Drivers

- Regulatory focus on recalibrating existing regulations to focus on risk, increasing the level of "tailoring" in current rules
- Generally strong capital and liquid assets levels across the industry
- Regulatory focus on financial stability risks associated with counterparty credit
- Proposed guidance has created further 'tailoring' of capital and liquidity rules

Challenges

Throughout 2019, most banking organizations will face a shifting landscape of capital- and liquidity-related regulatory requirements brought about by the Administration's plan to tailor supervision and regulation to the size, systemic footprint, risk profile, and business model of banking firms, including larger, nonglobal, systemically important banks. EGRRCPA raised the SIFI asset threshold and introduced new asset categories for large banking organizations, relieving many of them from annual stress testing requirements. The federal banking agencies are working toward a new framework that will further ease capital and liquidity requirements along with enhanced prudential standards based on these new assets categories and the agencies' efforts to recalibrate the regulatory approach. Additional revisions to a number of related rules may follow once the framework is finalized.

Despite the general trend toward less stringent requirements, the very largest banking organizations will generally experience limited relief and must prepare for compliance with the single counterparty credit limit (SCCL) rules which go into effect in 2020.

During this period of transition, banking organizations may be challenged in the following areas:

- **Higher SIFI asset thresholds and new asset categories**—New banking categories based on asset size and other factors, including global systemically important bank (GSIB) designation, will reduce the regulatory burden for the majority of financial institutions, though some institutions may find themselves forced to choose between growing their asset base and thereby increasing their regulatory burden, or sacrificing growth to remain below the threshold of a new tier of requirements. Those organizations nearing a new regulatory category may forgo growth strategies such as acquisitions or new product launches.
- **Liquidity coverage requirements**—Under new proposed capital adequacy rules, organizations with assets in the $100-$250 billion range will no longer be required to maintain a liquidity coverage ratio that allows them to operate for 30 days. Although the federal mandate may no longer be in place for these organizations, having an effective liquidity management plan is still a key part of ensuring the longevity of the organization, and may become a challenge for organizations that are reluctant to act without regulatory pressure.
- **Continued testing/supervisory reviews**—Despite the reduced frequency overall, completion of the stress testing and Comprehensive Capital Analysis and Review (CCAR) processes for those organizations required to do so still represent a large and complex effort. Many organizations struggle with a timely consolidation of all components needed to satisfy the stress testing requirements, even when the deadline is known far in advance. Firms should anticipate that agencies will

KPMG

conduct horizontal reviews focused on their capital planning strategy. In addition, supervisory priorities for the largest firms will focus on internal stress test assumptions and scenario design for capital and liquidity, governance of capital/liquidity models and data, and credit risk management.

- **Expanded application to certain Slices**—The federal banking agencies have proposed to extend the capital and liquidity rules and prudential standards to noninsurance, noncommercial SLHCs in the same manner as BHCs. SLHCs meeting the relevant criteria will need to prepare to ensure compliance once these rules are finalized.
- **IHC rules forthcoming**—IHCs are not covered by the agencies' proposed rulemakings to implement amendments to the capital and liquidity requirements; the agencies intend to proposed rules specific to IHCs but until such time IHCs must continue to operate under the current capital and liquidity requirements.
- **Additional rulemakings**—The Federal Reserve expects to finalize its Stress Capital Buffer proposal for application beginning in the 2020 stress test cycle though, based on comments from the Federal Reserve, certain elements of the rule could be considered for 2019. Further modifications to the Stress Capital Buffer rule might also be forthcoming. On the liquidity side, recent guidance has indicated the Fed is nearing a final rule on the Net Stable Funding Ratio.
- **Data Management**—Requirements stemming from the CECL, the recently finalized SCCL, and continued focus on liquidity data quality will create continuing demands on the capital and liquidity data management structures of financial institutions. Large firms are expected to continue to invest in the ability to measure capital, liquidity, credit exposures, and counterparty relationships in a more integrated fashion, allowing for more frequent and efficient reporting processes. Increased focus on data management and quality as a strategic initiative is expected to be a focal point.

Outstanding capital-related supervisory issues for LISCC firms include:

1. Methods for developing assumptions used in internal stress tests
2. Internal governance of capital models
3. Some areas of credit risk management.

Source: Supervision and Regulation Report, November 2018. Board of Governors of the Federal Reserve System.

Key actions

- Maintain effective liquidity management practices even as regulatory requirements are removed for institutions under the $250 billion threshold.
- Ensure effective stress testing practices and expertise remains in place with the reduced frequency of testing required.
- Enhance data management, including data materiality framework, data taxonomy, and data lineage, across credit products to enable real-time exposure monitoring and capital adequacy.
- Develop robust counterparty data management systems and frameworks to ensure compliance with rules around exposure to economically interdependent or connected counterparties.

Appendix of defined terms

Defined terms and abbreviations

ADA	Americans with Disabilities Act
AML	Anti-money laundering
BHC	Bank Holding Company
BSA	Bank Secrecy Act
CCPA	California Consumer Privacy Act
CECL	Current Expected Credit Losses
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CRA	Community Reinvestment Act
DOC	Department of Commerce
DOJ	Department of Justice
DOL	Department of Labor
EGRRCPA	Economic Growth, Regulatory Relief, and Consumer Protection Act.
FCC	Federal Communications Commission
Federal Reserve	Federal Reserve Board
FTC	Federal Trade Commission
GAO	General Accountability Office
GDPR	General Data Protection Regulation
GSIB	Global Systemically Important Banks
HMDA	Home Mortgage Disclosure Act
IHC	Intermediate Holding Company
LIBOR	London Interbank Offered Rate
LISCC	Large Institution Supervising Coordination Committee
MLA	Military Lending Act
OCC	Office of the Comptroller of the Currency
RESPA	Real Estate Settlement Procedures Act
SEC	Securities and Exchange Commission
SIFI	Systemically Important Financial Institution
SLHC	Savings and Loan Holding Company
TILA	Truth in Lending Act

KPMG

Contact us

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

Deborah Bailey
Managing Director
Operations and Compliance Risk
T: 212-954-0897
E: dpbailey@kpmg.com

Charles Jacco
Principal
Cyber Security
T: 212-954-1949
E: cjacco@kpmg.com

Michael Lamberth
Partner
Operations and Compliance Risk
T: 804-241-2795
E: mlamberth@kpmg.com

Adam Levy
Managing Director
Risk Analytics
T: 312-665-2928
E: adamlevy@kpmg.com

Orson Lucas
Managing Director
Cyber Security
T: 813-301-2025
E: olucas@kpmg.com

Frank Manahan
Managing Director
Risk Analytics
T: 212-954-3660
E: fjmanahan@kpmg.com

Teresa Pesce
Principal
Forensics
T: 212-872-6272
E: tpesce@kpmg.com

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

Steve Stein
Principal
Cyber Security
T: 312-665-3181
E: ssstein@kpmg.com

Tracy Whille
Principal
Operations and Compliance Risk
T: 212-954-2691
E: twhille@kpmg.com

Contributing authors:
Amy Matsuo, Karen Staines, Nicole Stryker, Phil MacFarlane, Dallas Bray, Anthony Guisti, and Brett Hayes

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

kpmg.com/socialmedia