



Ten key regulatory challenges of 2021

**The future of regulatory:
Altering our view**

[kpmg.com](https://www.kpmg.com)



Introduction

On behalf of KPMG Regulatory Insights, I am delighted to issue our annual Financial Services Ten Key Regulatory Challenges. This year's edition, which looks toward 2021, features our regulatory insights with those of the KPMG professionals focused in each of the regulatory challenge areas. We encourage you to reach out to us to learn more about the issues raised in the Ten Key Regulatory Challenges or to discuss your firm's unique challenges.

The disruptions that affected all industries in 2020 will forever reshape the financial services industry. Notable among these are the accelerated use of online and digital technologies, the long-term adoption of remote working practices, and the demand for business and risk strategies for climate and other ESG-related financial risks. Together they will impact all aspects of a financial services company's physical and strategic operations, technology systems and data security, products and services, customer interactions, and third-party relationships/affiliations. With such change comes regulatory and public policy challenges and concerns, which in 2021 will begin to set forth **the future of regulatory: altering our view.**

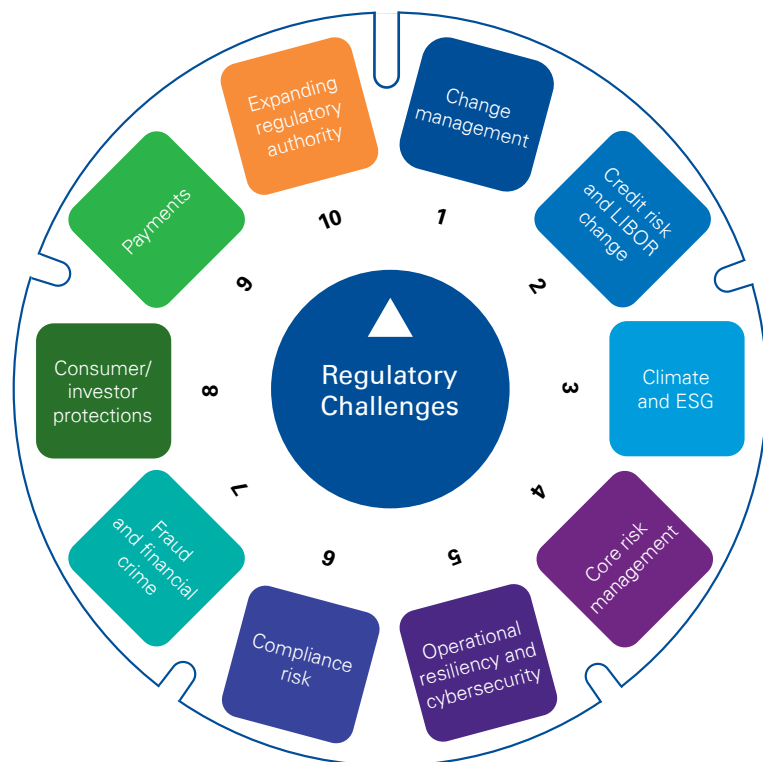
And so, our Ten Key Regulatory Challenges for 2021:

1. Change management
2. Credit risk and LIBOR change
3. Climate and ESG
4. Core risk management
5. Operational resiliency and cybersecurity
6. Compliance risk
7. Fraud and financial crimes
8. Consumer/investor protections
9. Payments
10. Expanded regulatory authority

Sincerely,

Amy Matsuo

National Leader, Regulatory Insights



FS Steering Committee



Peter Torrente
**National Sector Leader,
Banking & Capital Markets**
E: ptorrente@kpmg.com

Peter serves as KPMG's National Sector Leader for the Banking and Capital Markets practice. He has significant experience working with, communicating with, and reporting to executive management and audit committees on current business, accounting, auditing, and industry issues.



Joe Hargrove
**Principal, Head of Tax
Markets & Services**
E: jhargrove@kpmg.com

Joe serves as the Head of Tax Markets and Services and has worked with a range of investment banks and global companies, helping them through both economic expansions and downturns. With more than 30 years of experience advising clients on complex tax issues, he has in-depth industry knowledge focused primarily on taxation of financial instruments, international tax, mergers and acquisitions, and divestitures.



Kalpana Ramakrishnan
**Principal, Financial Services
Line of Business Leader**
E: kramakrishnan@kpmg.com

Kalpana focuses on driving innovation to meet the current and future market needs in the Financial Services industries and fostering an industry community that enables our teams to perform at their best. She has significant experience in aligning information technology strategy with business strategy to consistently maximize stakeholder value.



Ed Chanda
**Partner, National Sector
Leader, Insurance**
E: echanda@kpmg.com

Ed serves as KPMG's National Sector Leader for Insurance, leading the U.S. Firm's insurance audit, tax, and advisory practices. He has 30 years of experience serving the insurance industry, both property casualty and life. He has also helped lead the firm's efforts around the insurance contracts projects of the FASB and IASB and served as part of KPMG's Department of Professional Practice.



Amy Matsuo
**Principal, National Leader,
Regulatory Insights**
E: amatsuo@kpmg.com

Amy is KPMG's Leader for Regulatory Insights & Compliance Transformation. Nationally recognized for client delivery, she has extensive experience driving value to the business, risk, executive management, governance committees, and boards. Amy serves as US senior regulatory partner for financial services, across all facets of risk and compliance, and as the senior regulatory partner for KPMG's U.S. Sustainable Finance and ESG risk solutions. Her public policy and regulatory insight serve across the industry as leading indicators and practices.

Change management

Challenges

Volatility experienced throughout 2020 is expected to continue well into 2021, forcing financial services companies to demonstrate agility in their change management processes. Many of the changes necessitated by the response to COVID-19, such as temporary rule changes and moratoriums, will be short-lived. Changes which had been in process, such as the shift to digitalization and adoption of ESG considerations, were significantly accelerated. And certain unexpected changes, such as remote work requirements and limited in-person customer access, offered financial companies (and consumers) an opportunity to see the possibility of operating in a new way and will likely change the future of financial services. Execution of these changes—and the underlying variety of policies and procedures, technologies, products and services, partnerships and alliances, risk models and business strategies needed to effect them—will be scrutinized by many stakeholders (regulators, investors, counterparties, customers). Regulators will look for documented and sound change management, consistent with firms' governance structures, as well as ongoing compliance with laws and regulations, including consumer protections.

Regulators, too, have been forced to adjust their operations and will continue with frequent and ongoing requests to financial institutions given the voracity of change. Examination activities will include horizontal and firm-specific examinations (both targeted and full scope) based on a firm's size, complexity, risk profile, and the industry and business focus of its customers. For most firms, supervisory oversight will remain greatly elevated. In response to the heightened disruption, examiners may conduct "streamlined reviews" in select areas of supervisory attention in addition to broader examinations in areas such as data and issues governance, cyber security, enterprise-wide risk management, fraud and financial crimes, consumer protections, and modeling/scenario analysis. (See additional sections within this *Ten Key Regulatory Challenges for 2021*.) Notably, regulators are increasingly adopting SupTech techniques, including machine learning and natural language processing, to monitor emerging trends in documentation submitted by supervised institutions and to help increase the efficiency of their regulatory examination processes.

Common challenges to any change management process:

- Capturing change
- Organizing changes and determining what must be monitored or actioned
- Mapping requirements back to a relevant point in time
- Threading and capturing an audit trail of the impacts to business, processes, policies, procedures, and controls
- Communicating outcomes across the three lines of defense.

Regulatory pressures

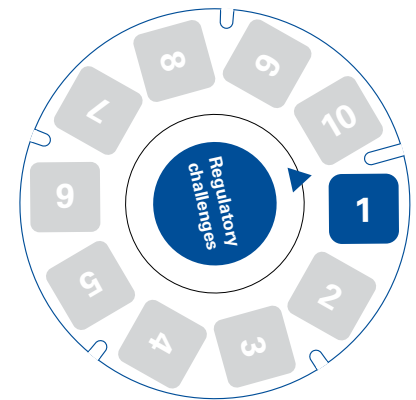
- OCC has specifically listed "change management over significant operational changes" among its bank supervision strategies for 2021. Areas of focus will include:
 - Governance over new technology innovation and implementation, including cloud computing, artificial intelligence, digitalization of risk management processes, and new products and services
 - Changes in strategic plans
 - Implementation of emergency stimulus programs
 - Response to COVID-19-related operating conditions

Amy Matsuo Principal, FS Regulatory & Compliance Risk

E: amatsuo@kpmg.com

Amy, a Principal and KPMG's Leader for Regulatory Insights and Compliance Transformation, is nationally recognized for providing regulatory-driven change services to large domestic and global organizations. With 27 years of direct risk and regulatory experience, she leads both thought leadership and client services across policy, regulatory, supervisory, and enforcement driven changes - helping organizations anticipate and mitigate impacts by designing and embedding sound and sustainable internal controls, automation and technology, data analytics and testing, and fair and responsible risk and compliance business practices.

- Accommodations provided by regulators related to temporary operational and compliance changes in response to COVID-19 were intended to also be temporary, but as remote work and economic hardships continue with uncertain duration regulators are beginning to expect firms to fully adapt their policies and procedures established during high operational shifts to assure safe and sound operations and compliance with consumer protection laws and regulations.
- Regulators are enhancing their supervisory processes with SupTech applications, including machine learning and natural language processing, and have been able to repurpose certain applications to improve the efficiency and effectiveness of supervisory processes, including continuous monitoring of institutions, during COVID-19.
- Heightened attention to data issues – sourcing, quality, storage, and privacy— as well as transparency in innovative technology applications and anti-trust concerns are focusing regulatory scrutiny on third-party acquisitions and relationships and new products and services.



What's next?

Given the continued and evolving change triggers, financial services companies need to establish firm governance and management routines to demonstrate their effective processes to identify and mitigate risks associated with transitions brought about by COVID-19. These processes, though established during times of high stress and operational impact, should be consistent with the firm's governance structures.

Key steps to effectively integrate organizational change include:

- **Identify drivers and applicability:** Conduct horizon scanning to monitor change drivers (e.g., new vendors, product, delivery channels, regulatory obligations); determine change applicability to lines of business and/or products; identify and link changes to existing business and risk data.
- **Assess impacts:** Assess change for consideration of new or changed regulatory obligations; determine gaps in coverage or consistency and identify opportunities for convergence; analyze downstream effects to people, process, and technology.
- **Design strategy:** Identify short-term and long-term goals; develop requirements for changes, including training and communication plans for impacted stakeholders; design dashboard reporting and management protocols.
- **Implement changes:** Update and enhance policies and procedures, mapping templates, process flows, RCSA, and testing programs; enhance existing technology infrastructure; communicate change expectations and execute implementation program.
- **Continuous monitoring and improvement:** Perform monitoring and testing procedures; review change success KPIs/KRIs and assess complaint data; determine enhancement opportunities and remediation approach for identified issues; continue to streamline and simplify business operations.

Regulators, too, have been forced to adjust their operations and will continue with frequent and ongoing requests to financial institutions given the voracity of change. Examination activities will include horizontal and firm-specific examinations...

Credit risk and LIBOR change

Adam Levy Principal, Modeling & Valuation

E: adamlevy@kpmg.com

Adam has nearly 20 years of experience delivering financial risk management services. He has professional experience in the consumer and commercial lending industry, stress testing and allowance for credit losses. He also has deep experience in model risk management including model development, remediation, and validation.

Chris Long Principal, Financial Services Solutions, Consulting

E: chrislong@kpmg.com

Chris leads the KPMG Global IBOR Campaign, assisting clients and market participants in developing the strategy, planning and execution of the transition from IBOR to Alternate Reference Rates. Chris has published articles and presented at industry symposia on the transition and is a member of the ARRC (Alternate Reference Rate Committee) Client Outreach & Communications sub-working group.

Challenges

The current pandemic has created an urgency and increased severity of credit risk impacted on all market segments, some worse than others. The uncertainty regarding COVID-19 and the magnitude and duration of the impact continues to be a major topic in credit risk discussions. Institutions are flanked with challenges as they are diligently working to help their customers and communities deal with the economic fallout from COVID-19, while at the same time dealing with increasing operating expenses, increased credit and other risks, and rapidly changing customer and employee expectations, while simultaneously changing operation and delivery models, all in a sustained low interest rate environment.

Federal programs, such as those established by the CARES Act, and changing customer behavior have made it very challenging for financial institutions to estimate the credit impact on their organizations. Compared to the last recession, the impacts of the current crisis emerged much more quickly and affect both consumer and commercial portfolios. As mentioned in the 2020 Spring Semiannual Risk Perspective from the OCC - "*nearly every asset class on banks' balance sheet has been or likely will be affected.*" This coupled with the remaining uncertainty will keep a sharp focus on credit risk management processes throughout 2021. In addition, while institutions have been encouraged to work with borrowers and perform loan modifications to mitigate the impact of COVID-19, the regulator's will still look at the rationale for these modifications as well as troubled debt restructuring (TDR) classifications, risk ratings, accrual status, allowance adequacy, and the impact of all of the above on bank capital.

Regulatory pressures

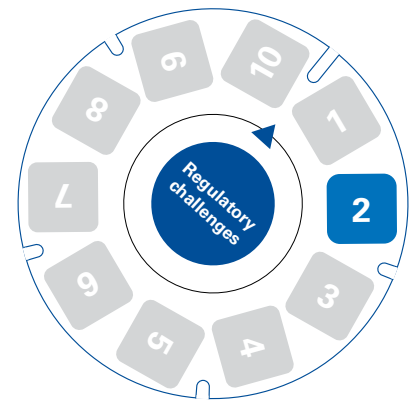
Adoption of CECL. Increasing delinquencies and elevated credit losses will continue to dominate the landscape in 2021 and a focus on CECL will remain top of mind as regulators assess institution's ability to estimate losses from an accounting perspective as well as their effectiveness in identifying and managing the increased risk profile to mitigate losses. The adoption of CECL has created a disconnect where some organizations have lowered their focus on traditional credit risk practices, such as credit review, as they focus more on the lifetime loan loss estimates. However, make no mistake, from a safety and soundness perspective, regulators will continue to be focused on credit risk management practices.

Supervisory priorities. As indicated in the OCC's 2021 Bank Supervision Fiscal Operating Plan, "*the OCC will adjust supervisory strategies, as appropriate, during the fiscal year in response to emerging risks and supervisory priorities.*" The OCC highlights that credit risk management will be a focus area given weaker economic conditions, emphasizing that examiner's should focus on: "*commercial and retail credit risk control functions, including portfolio administration and risk management, timely risk identification, independent loan review, risk rating accuracy, policy exception tracking, collateral valuation, stress testing, and collections/workout management.*" Additional focus will be on real estate concentrations and concentration risk management (both retail and commercial) and on other portfolios with "*material concentrations, especially those in sectors hard hit by the pandemic.*" The FRB similarly directs its supervisors to focus on these same issues.

Credit quality. While the results of the 2020 Shared National Credit Program have not yet been published, some information from the 2019 report may shed light on that market going forward. The 2019 report indicated that credit risk was elevated from the prior year, especially for Leveraged Loans, adding that “many of these Leveraged Loans possess weak structures,” and that many of these attributes including “high leverage, aggressive repayment assumptions, weakened covenants, and ability for borrower’s to draw additional funds” are the result of competitive market conditions and were not materially present in previous downturns.” These findings reflect increased risk and regulatory concerns, prior to the start of the COVID-19 pandemic, and will likely remain a primary focus through 2021. Recent regulatory reports note that offerings of proprietary relief and mandated programs along with stimulus efforts may mask credit quality issues. Credit risk will evolve based on the duration of assistance programs and economic factors such as unemployment.

LIBOR transition. With the expected phased discontinuation of LIBOR between end of 2021 to mid-June 2023, supervisory focus will increase for institutions with significant LIBOR exposure or less-developed processes. Regulators are looking for all institutions to have processes in place to identify and mitigate their LIBOR transition risks, commensurate with the size and complexity of their exposures. Regulators encourage institutions to determine, “without delay,” the appropriate replacement reference rates, including credit-sensitive alternatives, given their funding costs and customers’ needs. The expectation has been set that from the end of 2021 new contracts should not reference USD LIBOR. In addition, all new contracts should either utilize a reference rate other than LIBOR or include fallback language that includes a clearly defined alternative reference rate after LIBOR’s discontinuation. The federal banking agencies indicate the use of SOFR is voluntary and they will not criticize other rates, including a credit-sensitive rate, for loans. Disclosures should be made to credit customers in advance of rate changes to mitigate consumer protection and compliance risks.

Near zero rate environment. The current zero rate environment and economic uncertainty may ultimately make negative rates (e.g., negative yields, negative implied interest rates, and in some cases negative interest rate central bank policy) a possibility in the United States. The impacts of negative interest rates will vary among institutions based on business models and exposures, though financial services companies of all sizes may want to prepare by updating frameworks to adapt, inclusive of products and contracts with interest rate exposure (e.g., LIBOR), and models and systems (internal and third-party) that are interest rate dependent.



What's next?

- Leverage internal data and market data that help gain an understanding of increasing risk instead of relying solely upon lagging information.
- Develop early warning sign indicators within loan portfolios such as CRE which might be disproportionately impacted by COVID-19.
- Ensure loan risk ratings are commensurate with the risk of the current environment, loans which have moved from primary source of repayment to secondary or tertiary sources should be rated accordingly.
- Consider re-evaluating credit concentrations and risk appetite to align with increased risks associated with COVID-19 as well as potential losses which may occur in 2021; analyze and proactively manage concentration risk.
- Focus on risk controls, risk rating accuracy, and periodic risk assessments to evaluate, monitor, and measure emerging risk within respective portfolios.
- Stay abreast of local, regional, and national markets and the perceived impact on future revenues and fundamentals that drive borrower’s abilities to repay loans and the impact of changing market conditions on collateral valuations.
- Focus on credit risk fundamentals; maintain a strong credit culture; proactively monitor credit deterioration including identifying early warning signs.

The current pandemic has created an urgency and increased severity of credit risk impacted on all market segments, some worse than others. The uncertainty regarding COVID-19 and the magnitude and duration of the impact continues to be a major topic in credit risk discussions.

Climate and ESG

Challenges

Multiple standards and frameworks for measuring and reporting ESG risks currently exist, put together by international forums, central banks, academics, and private sector stakeholders. They are mostly voluntary and not directly comparable making it challenging for stakeholders, including financial services companies, regulators, and investors to objectively assess ESG risks – and commitment – among companies, products, and/or investments. Industry advisory groups are strongly encouraging the U.S. financial services regulators to adopt a standardized framework and consistent taxonomies. However, much like the industry itself, the regulators are just beginning to understand ESG risks and are in the early stages of exploring how to monitor, measure, and report them. For 2021, the regulatory focus is clearly centered on climate change, a sub-element of “E” factors, though consideration will also be devoted to diversity (an “S” factor) and corporate commitment (among the “G” factors).

Today, financial services regulators have the jurisdictional authority needed to set forth supervisory expectations for addressing financial climate-related risks, and ESG risks more generally, without requirement for additional rulemaking. Broadly, these authorities cover oversight of systemic financial risk, risk management of particular markets and financial institutions, disclosure and investor protection, and safeguarding of financial sector utilities. As regulators begin to set expectations, individual companies have publicly announced their commitment to ESG policies across their investment strategies, due diligence, and risk processes and are actively encouraging others to do the same. Examples include:

- Pledging to reduce reliance on fossil fuels and related products
- Promoting ESG disclosures aligned with the SASB and the TCFD
- Pledging to address racial inequality through financial products and investments
- Expanding product offerings that meet ESG expectations/standards
- Issuing bonds targeted to social equality and environmental sustainability
- Committing to adopt the metrics and disclosure in the Measuring Stakeholder Capitalism paper published by the International Business Council of the World Economic Forum
- Developing strategies to reduce exposure to clients that do not meet certain ESG criteria.

Regulatory pressures

The momentum to account for ESG issues is unmistakable and, although U.S. financial services regulators have been characterized as “reluctant participants,” they do engage with international ESG-related initiatives, including the FSB’s TCFD and the BCBS’s TFCR. Independently, the FRB and CFTC have specifically called out climate change as posing serious emerging risks to U.S. financial stability including spillover effects that may exacerbate vulnerabilities in the financial system unrelated to climate change.

Regulatory attention is being directed toward issues related to disclosure, reporting, and company policies and procedures; there is increasing pressure on regulators to:

- Fully participate in international efforts to establish ESG standards and metrics, with an initial focus on establishing uniform international measures for climate change risk

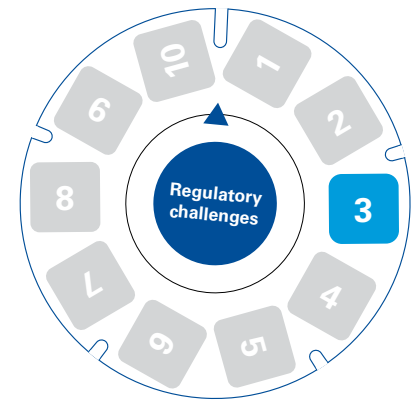
Steve Arnold Principal, Financial Services Solutions

E: stevenarnold@kpmg.com

Steve is a Principal in the Firm’s data management and financial services advisory practice. He has deep financial services experience with complex institutions and solving client challenges including data supply chain and storage, quality including control and attestation frameworks, and protection & privacy. Further, experience in finance and risk operations includes stress testing, CCAR/DFAST, interpreting complex regulatory requirements, and creating target operating models to coordinate regulations and enterprise risk management; more recently, he has focused on applying data and risk principles to ESG and related topics.



- Incorporate ESG-related risk management, and climate risk in particular, into bank and nonbank regulatory and supervisory frameworks where the regulators have authorities, including systemic financial risk oversight, risk management, and disclosure and investor protection
- Clarify the definition of “materiality,” including qualitative and quantitative factors, for purposes of meeting regulatory expectations to identify, measure, monitor, and control material risks as well as public disclosure requirements
- Mandate bank and nonbank financial services companies address climate risk and ESG issues through their existing risk management and governance frameworks, including stress testing (for climate, this includes assessment against a consistent and common set of broad risk scenarios, guidelines, and assumptions) and capital requirements
- Develop (for “E,” “S,” and “G” factors) common taxonomies and underlying definitions, risk data and data collection, analytical tools, and financial products to be used across financial and nonfinancial reporting with an eye to achieving standardized, comparable, and reliable disclosure
- Understand the roots of racial, social, and economic disparities and inequities within the organization and in the delivery of financial products and services, and implement changes.



What's next?

- Define the organization’s approach/responsibilities to Climate Risk and ESG, including customer and third-party relationships, across strategies, policies, practices, and mandates; establish targets and timelines to incorporate Climate Risk and ESG decisioning and reporting.
- Develop a roadmap and strategy to measure and assess Climate and ESG-related impacts across any or all key risk areas (e.g., operational, reputational, credit, compliance, liquidity, strategic, model, market, and due diligence).
- Assess exposure from physical and transition risks across asset classes and define how those exposures impact strategic planning for Climate and ESG risk management.
- Identify and procure needed data sets to forecast physical risk; incorporate into bank systems, scenario analysis, economic modeling and stress testing.
- Align internal definitions with evolving regulatory taxonomies to include Climate Risk and ESG-related impacts (e.g., what “ESG” encompasses, what is “green,” what is “sustainable”).
- As global standards evolve, focus on the integrity of Climate Risk and ESG-related financial data and controls (just like SOX).
- Establish policies and controls in the business and risk management processes to mitigate Climate and ESG-related reputational risks in a timely manner and through proactive monitoring and identification.
- Operationalize a disclosure and reporting framework, locally and globally, for consistency with the firm’s ESG mandate/policy aligned with SEC regulations, TCFD standards, SASB standards and others, as appropriate.

Today, financial services regulators have the jurisdictional authority needed to set forth supervisory expectations for addressing financial climate-related risks, and ESG risks more generally, without requirement for additional rulemaking.

Core risk management



Tim Phelps Principal, Financial Services Consulting Leader

E: tgphelps@kpmg.com

Tim has more than 20 years of experience advising clients and currently serves as Consulting's line of business leader for Financial Services. In this role, Tim is responsible for establishing our FS strategy and working with our teams to develop consulting services which are relevant at our priority clients across Banking, Capital Markets, and Insurance.

Cameron Burke Managing Director, Operations & Compliance Risk

E: cburke@kpmg.com

Cameron has a diverse background delivering risk consulting services to the financial services industry; he frequently assists clients execute large-scale initiatives that focus on enterprise/operational risk management, risk assessment convergence, business integration and separation, and data transformation while simultaneously minimizing risk and organizational impacts throughout transformation.

Challenges

The role of core risk management continues to evolve as financial services companies balance key priorities including increasing risk efficiency, modernizing technology, enhancing effectiveness, and building programs that are scalable and resilient all while maintaining regulatory compliance. Additionally, core risk management is under increasing regulatory focus which can result in severe, and potentially public, action including significant financial penalties if thematic, pervasive, or systemic risk issues are identified and categorized as inadequate risk management. Timely adoption and implementation of actions to correct identified risk issues is a key component of heightened regulatory attention to risk management.

Common challenges include:

Demonstrating risk management effectiveness and adequate oversight over the control environment

With the rapid pace of change at financial institutions, risks are continually evolving and the control environment is constantly changing. In an ecosystem where systems, processes and people change regularly, organizations can struggle with knowing, monitoring, and appropriately addressing risk. This can present challenges when articulating the effectiveness of the control environment. Furthermore, examiners are focused on the effectiveness of testing programs including methodology, testing techniques, coverage, and frequency in addition to clearly defined testing roles across the three lines of defense.

Maintaining or enhancing effectiveness while undertaking cost reduction and efficiency initiatives

As financial institutions explore efficiency levers including alternative sourcing strategies, consolidation of redundant risk functions and/or methodologies, rationalization of foundational risk data, integration of technology and automation use, and other risk-based scoping approaches to improve efficiency ratios, they must be careful to maintain the quality of risk outputs and identify and address any degradation of risk management effectiveness.

Establishing risk frameworks that are adaptable, are resilient and address areas of emerging regulatory focus

The adaptability and resilience of core risk management frameworks are under increased regulatory focus as firms manage through alternative/new business operating models and unexpected or severe events even as they also prepare for strategic growth through acquisition, the launch of new products and services, and integration of new or evolving regulatory expectations. *(Regulatory expectations related to operational resiliency and cybersecurity continue to evolve and are further explored in the Operational Resiliency and Cybersecurity section.)*

Moving to Data Driven Assessments

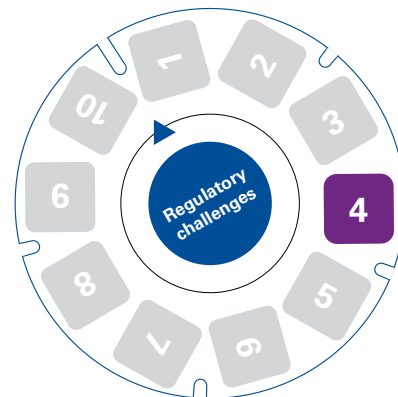
Financial services firms are increasingly aware of the limitations of classical, judgement-based risk measurement and management approaches. Collectively, firms are looking to the power of data to augment their capabilities, strengthen risk management protocols, and drive business value through better risk analytics. However, many institutions have found that a significant data uplift/cleanse is required to enhance the quality of data/inputs prior to implementing these data driven techniques in addition to evaluating and potentially supplementing the data quality controls to maintain assessment inputs.

Increasing Complexity

Large organizations have highly complex data and technology ecosystems that give rise to systemic risks and exploitable vulnerabilities. Once triggered, these risks can have runaway effect, with multiple, severe consequences. Furthermore, to meet enterprise level goals, organizations are using new innovative solutions and disruptive technologies but may lack adequate technology risk management processes, which can introduce new risks and business disruptions.

Regulatory pressures

- Demonstrating risk management effectiveness, not simply remediation activities
- Focusing on an integrated risk management approach across material risk types and lineage of risk data, outputs, and reporting
- Balancing cost take out initiatives while still delivering core risk management requirements
- Adequate monitoring, governance, and supervision over the internal control environment
- Examiner focus on conduct, operational resilience, and product lifecycle risk management
- Scaling core risk management activities to keep pace with growth, acquisition, or changing external conditions
- Evolving regulatory expectations for strong core risk management practices
- Moving to data driven and quantitatively supported risk and control assessments
- Enhanced management and board reporting to increase transparency and risk data consumption



What's next?

- Evaluate existing core risk management activities, framework, and coverage for effectiveness and potential redundancies.
- Identify and evaluate the intended or unintended outcomes, cost reduction and efficiency initiatives to ensure regulatory obligations are met or exceeded.
- Evaluate existing risk frameworks for scalability to support firm strategy and growth objectives.
- Review recent changes to business operating models to ensure new or elevated risks are adequately accounted for in risk inventories/profile.
- Evaluate existing internal control environment approaches, scope, coverage, and responsibilities and strengthen, as appropriate, any gaps, potential exposures, or escalation issues.
- Enable data interoperability. Data and technology target state should enable the sharing/linkage of risk data across key risk categories, support aggregation of data, eliminate redundancies or overlaps in source systems, and provide a single source of truth for reporting purposes.
- Review, inventory, and cleanse (as needed) existing data and quality of data to support data driven assessments.
- Integrate technology risk management capabilities with broader risk strategy and align with enterprise and operational risk priorities that are supported through the use of technology, data, and skilled technology risk professionals.

Timely adoption and implementation of actions to correct identified risk issues is a key component of heightened regulatory attention to risk management.



Operational resiliency and cybersecurity

Brian Hart Principal, FS Regulatory & Compliance Risk

E: bhart@kpmg.com

Brian is the leader of the KPMG Financial Services Regulatory and Compliance Risk Network and has experience leading efforts to transform operational risk management and compliance to align clients' cost and value, while simultaneously implementing new capabilities to significantly improve their ability to manage non-financial risks including the deployment of machine learning technologies and risk/compliance convergence.

Anand Desai Principal, Technology Risk Management

E: anandesai@kpmg.com

Anand focuses on technology risk management across all lines of defense within the financial services industry. He delivers services across the life cycle of technology risk management from regulatory and compliance, controls assurance to risk optimization. His focus is on digitizing and automating risk management functions and processes to enable institutions' transformative agendas.

Challenges

Recent events, including COVID-19, social unrest, severe market dislocation, and unprecedented governmental intervention, along with shifting regulatory focus and expanded cyber threats highlight the need to understand and plan for the possibility of multiple, converging tail events and their potential impacts on operational resilience. Additional attention and planning need to be placed on understanding how individual assets contribute to the ability of a financial services company to provide critical services on an end-to-end basis and what disruption anywhere along that value chain would mean to the firm's continued ability to provide those critical services.

Shortcomings in legacy risk assessment frameworks have highlighted the need for enhancements to firms' Resilience and Cybersecurity frameworks in order to effectively manage through these widespread events and keep pace with evolving regulatory focus and increasing vulnerability threats. Regulatory attention will focus on enhancements across traditional risk management areas of governance, operational risk, business continuity, third party risk, scenario analysis, information systems and cyber risk, and surveillance and reporting.

Common challenges in operational resilience posed by the current environment include:

- **Accountability for resilience:** A lack of ownership for operational resilience at the level of senior management and Board of Directors has been observed. Service ownership and accountability are currently not well defined, and there are concerns about whether senior management and the Board are adequately equipped.
- **Service management and execution:** There is a clear disconnect between the concept of an end-to-end service delivery model and the way businesses are currently managed. Organizations have multiple disconnected and/or redundant service, process, risk and control taxonomies. Also, international institutions often lack harmonization with and across legal entities.
- **Calibration of impact tolerances:** Firms will be required to construct and test against service level impact tolerances. These tolerance statements are intended to articulate the tolerance of external stakeholders to service disruption and any associated harm where stakeholders may be clients, counterparties, or market participants. Impact tolerances can only ever be subjective and aggregate measures that serve as crude approximations of external harm.
- **Scope of resilience assessments:** There is a gap between existing business continuity/ disaster recovery and incident management functions and a more recovery-centric framework that can be leveraged across end to end services.
- **Reporting, investment, and service enhancements:** Senior management is rarely equipped with the breadth and depth of insights required. Many firms have not appropriately addressed the full universe of resilience risk.
- **Tooling and data requirements:** Most organizations currently maintain multiple sources of data in varying degrees of detail, which results in significant data limitations particularly around loss data, events, and scenarios.

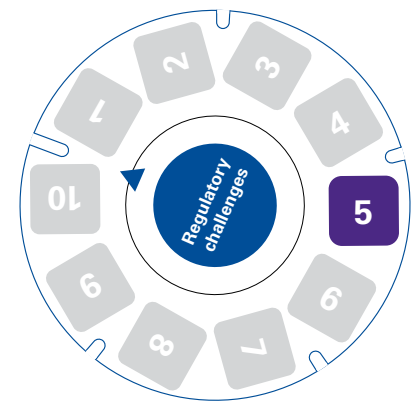
- **Third-party challenges:** Challenges posed by third parties that impede resilience include inadequate tracking and managing of concentration risk and fourth-party risk, lack of transparency into the interdependencies between third parties across the value chain of financial products, narrowly focused or appropriate disaster recovery and business continuity planning, and insufficient strategic vision when outsourcing business critical skills and functions.
- **Increased regulatory interest:** Regulators are placing an increased emphasis on various aspects of operational resilience. To date, we've seen a piecemeal approach to individual aspects, with a primary emphasis on system resilience as opposed to business continuity planning.
- **Return to work:** Uncertainty exists surrounding the return to the workplace approach and changes in ways of working. There is a need for an adaptable, risk-based approach to returning to work or adapting to an extended remote environment. It is also important to consider risks taken to accommodate widescale remote access or deployment of technology and that they are in line with the bank's risk appetite/risk tolerance for disruption.
- **Testing and scenario analysis:** There is a need for enhanced tabletop testing, scenarios, and simulation, which provide additional insight into tail events, and, in particular, multiple event sustained outage scenarios that can support future planning and preparation.

Regulatory pressure points

- Regulatory expectations for increased integration and improved operational resiliency capabilities, including cyber risk management
- Outdated risk assessment and resilience frameworks
- Closer partnership with the board and business functions to strategically align initiatives
- Focus on modern technology resilience across platforms, data and applications
- Expanded cyber and vulnerability threats resulting from increased use of digital platforms, including rapid cloud adoption and software deployment
- Regulatory focus on proprietary data, customer data, core processes, and exposure from third parties
- Availability of new technologies and tooling; increased focus on IT asset management; and the need for a complete and accurate view of the IT estate
- Enhanced integration of cyber risk management with enterprise risk management

What's next?

- Embed operational resilience as a key criterion across all management decisions and business activities.
- Develop an approach in which the relative calibration of impact tolerances across services is emphasized over absolute one-time calibration and ongoing, long-term calibration across reporting cycles.
- For critical business services, in addition to scenario execution and impact tolerances, consider assessing business as usual service resilience and service level assessments of all threat vectors.
- Consider assessing cyber and enterprise risks quantitatively using the FAIR methodology based on frequency and loss magnitude.
- Risk assess and then revisit thresholds and permissions (high risk to low) to ensure appropriate thresholds have been set.



Top Technology risks to manage

- Software development
- Obsolete technology
- Security of systems and data
- People and skills
- Third party technology and services
- Failed technology strategy
- Services and availability
- Emerging technology
- Data quality and management
- Regulations and compliance

Compliance risk

Challenges

The disruptions from 2020 caused an almost untenable pace of change to operations and risk within compliance departments. However, the prospect of additional “waves” in the COVID-19 pandemic as well as the likelihood of additional economic stimulus measures will push strains on compliance staff and governance processes well into 2021. So far, the most significant challenges include:

- Redeployment of resources to immediate operational needs/demands and a high degree of waivers/exceptions given immediacy of operational needs.
- Reprioritization of compliance activities due to quickly emerging and evolving disruption risks coupled with resource constraints (e.g., delayed accelerated training, testing/auditing schedules, remote workforce).
- Rapid roll-out of complex government stimulus programs with ongoing iterative changes and expedited delivery to market.
- Increased compliance risks (as some risk assessments rendered obsolete by emerging risks, requiring new ways to assess risk and leverage data/technology to enable real-time risk analysis) and misconduct risk (such as insider trading, PII use, fraud, and phishing).
- Providing additional/new communications, training, and monitoring/data analysis sufficient to maintain compliance amid new regulatory and supervisory expectations.

In spite of the disruptions, or perhaps because of them, regulators are looking more closely at the effectiveness of compliance programs. In particular, they expect compliance programs to be evaluated on an ongoing basis, technology-enabled (using automated analytics/AI, digitized data and processes), linked to a firm’s enterprise risk management, and revised based on relevant operational data and information as well as “lessons learned.” Regulators also expect firms to further invest adequate resources into the compliance function to address evolving/enhanced skillsets, including staffing, training, structure, and stature.

Regulatory pressures

Similar to the regulatory focus for overall enterprise risk management, the compliance risk area will continue to be assessed to ensure the sound establishment, use, and effectiveness of the organization’s compliance management system.

Shifts in public policy due in part with an Administration change may significantly change prior regulatory accommodation, as well as regulatory expectations in both specific areas of risk and compliance (e.g., ESG/climate) and overall compliance management systems. Changes in agency leadership and direction will likely intensify regulatory supervision and enforcement.

The unique nature of the disruptions tied to the COVID-19 response will direct regulatory attention toward full and accurate implementation of policies and procedures designed to meet the applicable laws and regulations and consumer protections related to loan underwriting, new account opening, monitoring customer activity, processing transactions, modifying loans, servicing loans, and communicating with customers given the:

- Ongoing economic uncertainty and consumer financial insecurity tied to high unemployment, potential future shutdowns, and the unknown magnitude/composition of any possible stimulus package



Todd Semanco Partner, FS Regulatory & Compliance Risk

E: tsemanco@kpmg.com

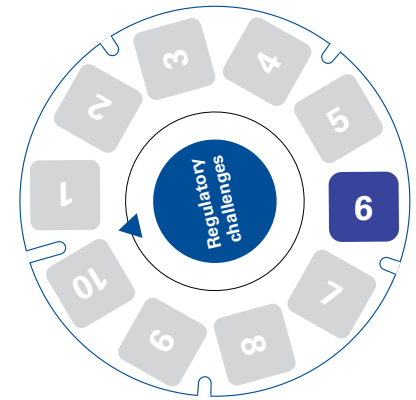
Todd is a Partner and National Lead for KPMG’s Banking Regulatory and Compliance Risk practice in the U.S. He has 23 years of experience helping all lines of management, and boards, to achieve strategic objectives while meeting regulatory expectations. As a RegTech leader, Todd designs and implements transformation initiatives embedding automation and analytics to optimize compliance.

Damian Plioplys Managing Director, FS Regulatory & Compliance Risk

E: dplioplys@kpmg.com

With more than 15 years of experience, Damian has a deep knowledge in the current and evolving financial services and consumer protection regulatory environment including with banks, and non-bank entities such as FinTechs, non-bank lenders, debt collection agencies, and non-bank finance companies.

- Risk of fraud associated with the urgent roll-out of stimulus fund programs and the rising number of investigations and charges being brought, especially in conjunction with the PPP
- Risk of disparate impact and disparate treatment associated with the urgent roll-out of stimulus fund programs and public attention drawn by the number of related consumer complaints and lawsuits
- Multiplicity of federal, state, and local assistance programs with varying applications, requirements, and timing in addition to actions taken by individual institutions
- Complicated and iterative changes to obligations under the assistance programs in addition to actions by individual institutions (e.g., extensions of temporary rules, relief)
- Rapid regulatory process changes required combined with high transaction volume
- Various workforce constraints, including remote locations, absenteeism, training, monitoring, and surveillance
- Customer interactions, including increased call center activity, error resolution related to new product/service implementation, requests for accommodations
- Deferred actions and other departures from standard processes due to the introduction of new priorities and redeployment of resources.



What's next?

In order to maintain stability and respond to regulatory pressures, financial services institutions should consider taking the following actions:

- Keep finger on the pulse of rapidly changing federal, state and local obligations related to foreclosures.
- Strengthen fraud and employee misconduct controls, including surveillance and fraud prevention programs that address ongoing remote working conditions and staff constraints.
- Increase the frequency at which you refresh risk assessments in order to account for the new environment.
- Increase the frequency at which you refresh and validate risk and compliance core data.
- Strengthen integration of compliance within the business, taking advantage of opportunities to embed compliance resources and new functionalities alongside large operational shifts.
- Know when to curtail accommodative strategies on loan modifications and loosened underwriting standards.
- Evolve consumer and investor standards and controls to heightened and changing regulatory risks and expectations (e.g., ADA, underbanked, protected classes, elderly protections, CRA, Best Interest).

Regulators also expect firms to further invest adequate resources into the compliance function to address evolving/enhanced skillsets, including staffing, training, structure, and stature.



Fraud and financial crime

Challenges

Financial institutions face challenges to enhance financial crimes prevention and detection capabilities while meeting their obligations to provide information to key regulators. Regulatory comments ask for better quality suspicious activity reporting versus a sheer volume of filings. In this environment, many firms struggle to augment legacy monitoring systems with artificial intelligence and other advanced detective approaches due to long implementation timelines.

Fraud concerns shifted due to COVID-19, and the operational flexibility to adjust detective and reporting processes to address emerging areas has required many institutions to shift more resources into fraud and financial crimes. PPP, unemployment, healthcare scams and other COVID-19-related schemes have emerged as key risk drivers, but significant uncertainty about the responsibilities of financial services companies remains.

While the respective regulatory pressures continue to mount, the mandate to meet those needs at a lower cost and with fewer resources is ever present – and growing with the emergence of FinTech competition with lower-cost business models.

Regulatory pressures

Alignment of risk with capabilities – Regulatory expectations continue to increase to match program design to real world risks presented by customers, products, and geographies. Consistent with the pressure for increased quality in reporting, regulators are demanding evidence of how KYC programs influence detective capabilities and risk assessments, and vice versa.

Deployment of advanced technology – Financial services companies continue to experiment with different levels of automation and artificial intelligence but legacy data and systems problems result in long and rigid implementation timelines. Many firms struggle to move these capabilities out of the lab and into production due to data, governance, validation, and reporting issues. Moreover, accelerated rollout of contemplated central bank digital currencies will require redesign of existing technology capabilities and operational processes.

Continued emphasis on sanctions – Economic sanctions continues to be a significant area of focus as the volume and complexity of sanctions programs grow globally. Many firms struggle to align sanctions detective and alert management capabilities to the need for faster or instantaneous payments and digital currencies. Legacy technology solutions result in high volumes of false positives and require significant manual intervention, thereby impacting processing times.

Exposure to COVID-19-related frauds – The regulatory expectations have increased for firms to detect and report suspicious activity related to COVID-19 relief program frauds and other emerging threats. Potential fraud and financial crime profiles have shifted due to COVID-19 with significant increase in medical scams, imposter scams, money mules, unemployment insurance, and cybercrime. Losses from these frauds are not strictly financial, with reputational damage and customer friction as significant concerns. Ongoing and after-the-fact reviews of COVID-19 relief programs for fraud are a significant, and emerging concern, especially in light of the sheer volume of the relief measures, and the speed at which they were necessarily rolled out.

John Caruso

Principal, Consulting, Financial Crimes & Analytics

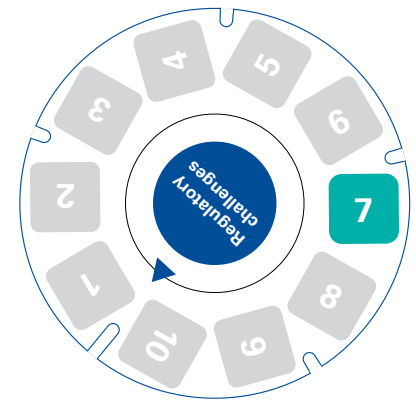
E: johncaruso@kpmg.com

John is a seasoned advisory professional with deep experience in Anti-Money Laundering and Financial Crimes Compliance. His experience includes advising clients on the design and operation of their full program, conducting audits and gap assessments of existing compliance programs, and assistance with regulatory and investigative matters across Financial Crimes. John has also developed an expansive practice advising clients in the cryptoassets industry.

Enterprise wide focus on fraud and financial crime – Regulators expect firms to measure and respond to fraud and financial crimes risks across business lines in a consistent and cohesive manner. Firms are challenged to work across functional silos in cyber/IT security, product-focused fraud, financial crimes teams, enterprise AML leadership, and regulatory reporting. Many firms may have to re-design their operational and reporting structures in areas that were traditionally separate functions.

Response to Cybercrime and Ransomware – Account take over, ID theft, bot attacks, and synthetic ID fraud continue to be major fraud risks arising from cybercrime and gaps in cybersecurity programs. Additionally, recent regulatory guidance, including red flag indicators, raised expectations that firms will file suspicious activity reports for cybercrime and ransomware payments using cryptoassets which may flow through the firm’s custodial or account operations.

Adapting to Cryptoassets – Competitive pressure from emerging FinTech companies and non-bank custodians is increasing the pressure for regulated firms to allow customers to hold cryptoassets in accounts. New charters for digital assets have been proposed at both the federal and state levels. However, most firms are not yet prepared to make the necessary changes to their financial crimes programs and technology in order to monitor and respond to the new fraud and financial crime risks presented by cryptoassets, both private (e.g., Bitcoin) and emerging government issued fiat digital currencies. At the same time, the emerging FinTech firms have been building more sophisticated compliance programs, including increasingly robust financial crimes compliance functions. DOJ recently released a report evaluating emerging threats posed by cryptoassets and the legal and regulatory tools available in the U.S. to confront those threats.



What's next?

- Align preventive, detective, and reactive capabilities with the risk profile of the company and its customers.
- Develop cohesive connections between fraud, cybersecurity, and financial crimes teams within all three lines of defense on a global scale.
- Design and build target operating models and responsibilities linking first and second line operations to remove internal friction and duplication of effort.
- Operationalize fraud processes and technology through integration of advanced technology tools, including enhanced analytics capabilities.
- Respond to rapid changes in threats with automation and new capabilities; integrate ethics and compliance efforts for scalability and continued sustainability.
- Develop financial crimes capabilities that are effective and suspicious activity reporting that provides adequate and meaningful information.
- Improve communication and collaboration across functional groups responsible for preventing, detecting, investigating and reporting potential fraud.
- Aggregate risks and losses across all business lines and develop appropriate metrics to monitor changes.
- Develop effective strategies for increased adoption of cryptoassets and the novel compliances challenges presented by existing and planned crypto and digital assets, particularly those with anonymous capabilities.

Average loss per ransomware attack reported on SARs increased from

\$417,000

in 2018 to

\$783,000

in 2020.

(FinCEN / FBI)

Consumer/investor protections

Challenges

Much like after the 2008 financial crisis, financial services companies should expect a high degree of scrutiny from regulators regarding their treatment of customers throughout 2020 and 2021. This scrutiny will be compounded by the attentions of customers themselves, both consumers and commercial businesses, who now have a heightened awareness of consumer protections, including fair access to financial products and services along with fair treatment.

Regulatory attention by the CFPB, SEC and other regulators, coupled with shifts in public policies resulting from an Administration change or agency leadership changes will likely increase regulatory supervision and enforcement overall. In addition, consumer protections may drive public policy and regulatory focus toward:

- Select consumer protections areas such as access to services, retail fees, fair lending, student loans, overdraft and UDAAP
- Best Interest (BI) and Know Your Customer (KYC) application to wealth management, inclusive of ESG and sustainable investments
- Housing finance reforms that address access and affordability
- Possible new financial services policies, such as postal service banking, banking access for cannabis businesses, the central banking approach to payments, and creation of a public credit reporting agency.

Regulatory pressures

Anti-Bias and Fairness. Financial institutions will need to demonstrate the upfront business justification and ongoing monitoring of consumer-impacting COVID-19-related activities (e.g., closing accounts, reducing credit lines, accommodations). The regulators will be focused on governance, controls, and testing for bias in models and AI, inclusive of on-premises builds and use, as well as appropriate third-party oversight.

Potential enhancements to the ECOA are under consideration, including:

- CFPB proposals to require data reporting on applications for credit by women-owned, minority-owned, and small businesses
- Efforts by State insurance regulators to prohibit certain factors, such as education, occupation, and credit scores, in underwriting algorithms
- Congressional efforts to expand prohibitions to a larger group of financial services companies and financial services products.

Investor protections. The SEC moved forward with the June 2020 compliance date for its Regulation Best Interest and Form CRS. Supervisory examinations, initially focused on assessing firms' good faith efforts to comply (policies, procedures, training), are expected to become more robust throughout 2021. FINRA has aligned its Reg BI compliance and examination expectations with SEC. DOL reinstated its five-part test for determining investment advice fiduciaries to ERISA plans and coincidentally proposed a new class exemption intended to align with Reg BI.

With the focus on ESG, SEC is expected to move toward standardized definitions/disclosures. Investment advisers and broker-dealers continue to work through the interplay between regulatory requirements for KYC, Suitability, and Reg BI (refer to the Climate and ESG section within this document). Adding some complication, a DOL rule requires ERISA plan advisers to execute their

Mike Lamberth Partner, FS Regulatory & Compliance Risk, Banking

E: mlamberth@kpmg.com

With more than 27 years of experience, Mike is a nationally recognized compliance leader focusing on compliance transformation services, supervisory and enforcement matters, enterprise-wide compliance and risk management programs, consumer protection, Fair and Responsible practices, and conduct risk governance. He works closely with leading banks and financial services companies, helping all lines of management, and boards, to achieve strategic objectives while meeting regulatory expectations.



fiduciary responsibilities based on financial factors rather than non-financial goals such as sustainability/ESG goals.

Know-your-customer. States are likely to focus on escheatment and associated practices; FINRA and other regulators are likely to take a renewed focus on deceased practices as part of investor protections.

Divergent regulations. A variety of laws and regulations put forth by federal and state authorities will influence the expectations of consumers and increase the challenges faced by financial services institutions:

- **Community Reinvestment Act:** The debate on revisions to the CRA regulations continues even as the federal banking agencies agree they would prefer a common set of requirements. OCC is the only agency yet to finalize a rule and differences in approach exist between OCC and FRB.
- **Data privacy:** California voted in a new law, the California Privacy Rights Act (CPRA), that will expand, beginning 2023, the consumer protections under the CCPA to more closely resemble the EU's GDPR. It will also establish a new regulatory agency dedicated to privacy protection. California's rules remain the most stringent data privacy rules in the U.S.; CFPB is expected to release an NPR on consumer data access, including consumer control and privacy, and data security and accuracy during 2021.
- **Anti-trust.** Regulatory (DOJ, FTC) and legislative focus on anti-trust compliance in the technology sector and digital markets is gaining momentum, especially with regard to the potential to derive market power through the data made available from large online platforms and user networks, and efforts to control innovation/competition through acquisitions of nascent companies or future competitors.
- **State "mini-CFPBs"** Like multiple other states, California established a regulatory body closely modeled after the CFPB; it has authority over all providers of financial products and services to California consumers, including nonbanks and FinTechs (though with notable exemptions.)



What's next?

- Assess the Reg BI Compliance program including a review of customer complaints and surveillance tools to ensure financial services representatives are acting in the best interest of consumers and focus on fair consumer outcomes; execute change management as needed.
- Implement and evaluate technology-enabled surveillance, monitoring, and testing controls to provide real-time feedback and timely notification to business management and risk officers.
- Perform Design and Operational effectiveness reviews to assess whether operational controls are functioning effectively, particularly for high-risk and emerging regulatory requirements, such as fair lending and CRA requirements.
- Review existing policies, standards, procedures, and management reporting protocols and update as needed to ensure they comprehensively cover all impacted business areas, are sufficiently detailed for first line employees to understand, and are appropriately revised to capture new and emerging regulatory requirements.
- Execute a gap assessment to evaluate whether all applicable new and revised COVID-19-related regulatory obligations were effectively identified and implemented across all impacted areas of an organization; focus on training, monitoring, testing, and reporting.
- Evaluate compliance with new and emerging data protection and consumer privacy rules, such as GDPR, CCPA, and HIPAA to evaluate readiness to meet requests from regulators and customers.

Much like after the 2008 financial crisis, financial services companies should expect a high degree of scrutiny from regulators regarding their treatment of customers throughout the full cycle of financial hardships created by COVID-19.

Payments

Challenges

The rapid pace of change in the payments industry, including innovative technology, entry of non-traditional payments providers into mainstream markets, and the rise of digital currencies has led to corresponding shifts in customer demand that have upended business organizations and delivery models. As financial institutions across the payments value chain seek to adapt to these changes, they find themselves in increasing competition, and in shifting partnerships with FinTechs, non-banks, and some of the country's largest retailers. Customers find themselves with more options than ever before and are consistently on the lookout for new services that enable them to make payments faster and at lower cost. In turn, regulators are continuing to focus on the need to protect consumers and are evaluating options to balance promotion of responsible innovation with enhanced oversight.

Regulatory pressures

Regulatory jurisdiction and supervision

The current regulatory regime has not yet adapted to the increase in both the number and type of firms providing payments services, resulting in inconsistent regulatory frameworks for some entities, and a dearth of regulation for others (*refer to Expanded Regulatory Authority section within this document*). Federal and State regulators are both seeking chartering authority on a number of fronts, and standardization of requirements across jurisdictions where feasible. However, each continues to expect firms to apply traditional expectations around anti-money laundering, consumer protection (*refer to Consumer Protection section within this document*), dispute resolution, privacy, and safety and soundness when offering innovative payments services.

Resiliency during COVID-19

The technological advances made in the payments industry prior to COVID-19 have kept payments services accessible during this time of unprecedented lockdown and financial upheaval. Digital banking, contactless card use, and mobile payments have all experienced significant growth; this shift in consumer behavior is expected to be prolonged and likely permanent. As firms continue to develop innovative payments offerings, regulators will have a renewed focus on the risks associated with the development and offering of new products, services, delivery and payment channels, and impact on related processes such as funds availability, fee disclosures, error resolution, and technology controls. Regulators will expect risk and regulatory compliance integration throughout the product development lifecycle, including through the transition to "business-as-usual" processes.

Inclusion and access

The shift to digital payments has in many ways made payments more accessible to populations that may have been excluded in the past due to lack of proximity to physical locations, mobility issues, or the high cost associated with traditional payments methods. However, many populations are still at risk of being left out, including those with no or inconsistent internet access, who are unfamiliar with how to use newer technology, and who have disabilities and need accommodations. Further, regulators continue to focus on the need to mitigate bias and disparate treatment when developing new products and services and the associated roll-out strategies.

Advancement of cryptoassets and digital assets

While the role of regulators, governments, and central banks in virtual currency remains uncertain and evolving, collectively they have expressed concern about the array of risks cryptoassets may pose to both consumers and financial

Chad Polen Managing Director, FS Regulatory and Compliance Risk

E: cpolen@kpmg.com

Chad has 17 years of professional financial services experience. He leads the delivery of testing services for the consumer protection agenda covering automation enabled compliance testing, large scale consumer harm remediation and regulatory response, new product and service testing, and compliance UAT testing for technology transformations. Chad also works with several leading peer-to-peer payment transfer companies, focusing on the identification of applicable regulatory requirements, control design and gap assessments, and compliance program transformation.



institutions. It will be imperative for firms to have a robust regulatory change management process in place to stay in tune with upcoming industry changes that are likely to yield new monetary policies and regulatory requirements aimed at protecting consumer information, advancing financial inclusion, and promoting financial stability both in the U.S. and globally.

Speed of compliance

The payments industry continues to drive towards providing faster, cheaper, and more transparent payment services. Compliance processes, particularly related to custody, know your customer, anti-money laundering, and fraud are often operating at a much slower pace, and are challenged by the volume and speed of the money movement (*refer to Compliance Risk and Fraud and Financial Crimes sections within this document*). Faster payments processes will also need to be balanced with careful management of the collection, use, and safeguarding of customer data to mitigate against improper disclosure and misappropriation. Firms will need to invest in the modernization of their compliance departments, including third party risk management, to meet these growing challenges, which may prove difficult for firms already investing heavily in service delivery.



What's next?

- Leverage regulatory sandboxes, no action letters, and other guidance to develop and pilot innovative payments solutions to assess feasibility of larger scale rollouts.
- Integrate compliance within digital payments strategy to facilitate upfront assessment of applicable regulatory requirements and testing of associated controls.
- Evaluate strategies and approach for financial inclusion to support identification of target customer audience and achievement of corporate growth goals.
- Assess the timing and cost of replacing outdated core banking systems, and consider the acceleration of other technology initiatives to contribute to a more flexible and resilient payments infrastructure.
- Automate compliance risk mitigation activities, particularly those impacted by a growing customer base and increased transaction volumes.
- Implement an enterprise-wide approach to third party due diligence that includes risk assessments and ongoing monitoring.
- Monitor regulatory and policy changes and current events to enable real-time responses.

Regulators are continuing to focus on the need to protect consumers and are evaluating options to balance promotion of responsible innovation with enhanced oversight.



Expanding regulatory authority

Challenges

The financial services landscape is fundamentally changing; technology is now integral to financial services delivery and much of the innovation is being developed through FinTech and nonbank financial services companies. Traditional banks are actively forging partnerships and alliances with one or more of these companies to quickly achieve scale, enter new markets, or acquire needed capabilities.

There is some tension between Federal and State regulators, which license/ charter most FinTech and nonbank financial services companies. States are working together to establish more uniform licensing and streamlined examinations recognizing companies increasingly hold a multiplicity of licenses. Efforts by the OCC to establish separate special purpose national bank charters are ongoing but have been opposed by the States; this debate will spill into 2021 and potentially beyond.

Throughout 2021, financial services companies may also be impacted, directly or indirectly, by:

- Some very large nonbanks seeking, and receiving, federal charters permitting deposit taking and potential access to the Federal payments system
- Heightened attention by DOJ and FTC to anti-trust and anti-competitive activity in financial services markets, including acquisitions of nascent companies
- State laws and regulations establishing new supervisory units or stringent regulations with broad application
- Expansion of regulators existing regulatory authority to new areas, such as artificial intelligence and ESG issues.

Regulatory pressures

Regulatory Acceptance of Emerging Areas – Expanding use of artificial intelligence, machine learning, and algorithms by bank and non-bank financial institutions to execute core activities will present novel challenges for both regulators and the institutions they supervise. Tighter integration of third-party technologies into core functions and customer facing applications will drive deeper scrutiny by regulators seeking to understand the risks posed to both safety and soundness and consumer protection. Regulators will press institutions to demonstrate and explain use cases for these new technologies as well as governance and oversight of the associated risks in a clear and concise manner.

Regulators are just beginning to understand ESG risks and are in the early stages of exploring how to monitor, measure, and report them. For 2021, the regulatory focus is clearly centered on climate change. Though even as regulators begin to set expectations, financial services companies should note the regulators currently have the jurisdictional authority needed to set forth supervisory expectations for addressing financial climate-related risks, and ESG risks more generally, without requirement for additional rulemaking.

Applications for Licensure – Technology companies and FinTechs seek licenses and charters to expand into adjacent businesses and to offer complimentary products on their digital platforms. Money Transmitter Licenses, Bank Charters, and SBA licenses will bring scrutiny to previously unregulated companies that will need to build teams, systems, and processes capable of responding to

Michael Scarpa Managing Director, FS Regulatory & Compliance Risk

E: mscarpa@kpmg.com

Michael has experience supporting traditional and non-traditional financial institutions regarding regulatory obligations and expectations and has developed dynamic action plans and responses to government regulators. He works on financial institution safety and soundness matters including but not limited to Federal Reserve regulations (most notably Regulation W), Qualified Financial Contract Recordkeeping, obligation drafting/policy mapping engagements, licensure and chartering, and fiduciary/ custody (including digital assets) regulatory compliance issues.

examinations. Bolstering compliance programs for new expectations will be slowed by hiring/staffing challenges during COVID-19. Industry opposition to the OCC's proposed special purpose charters questions whether supervisory oversight would mirror that for banks and their holding companies.

Federal and State Regulatory Divergence – Federal and State regulators are at odds over a variety of regulatory topics. DOJ and FTC are actively pursuing anti-trust compliance as it relates to customer data privacy, especially in the technology sector and digital markets. Some States have enacted laws and promulgated regulations that are setting expectations at the federal level, such as California's CCPA data privacy law, New York's cybersecurity regulation, and multiple States new "mini-CFPBs" (refer to *Consumer/Investor Protections section within this document*). Notably, the OCC and the NYDFS remain engaged in a legal dispute regarding chartering authorities. These divergences will create uncertainty for both regulators and the institutions they regulate. Simultaneous efforts by State supervisors to streamline licensing and examinations may drive more regulated financial activity to the States.

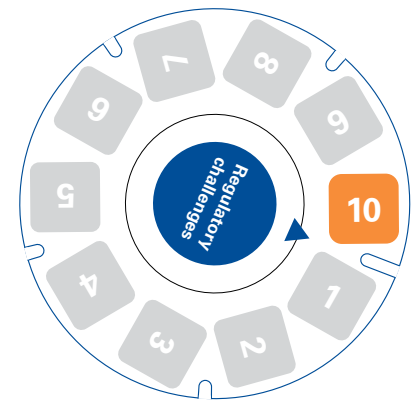
Regulatory Expansion Regarding Digital Assets and Cryptoassets – State frameworks for digital assets and cryptoassets (e.g. Wyoming and New York) will allow for new entrants to custody crypto assets alongside certain Federal banking entities. There is, however, little coordination in approach at the State level. Into 2021, regulatory guidance will remain sparse and evolving as the breadth of activities, scope of experience, and regulatory authorities expand. Supervision examinations are expected to cover areas such as BSA/AML/KYC/sanctions, custody and fiduciary activities, information technology, payment system risk and bank operations.

Mergers and Alliances – Continued consolidation amongst and across bank and nonbank financial services companies will expand the scope and scale of supervision that combined organizations will face.

Administration and Policy Changes – Shifts in public policies resulting from an Administration change or agency leadership changes may alter, or in some cases pull-back, efforts to redefine or expand regulatory chartering authorities at the Federal level. Other potential changes contemplated over a longer term portend competition from new government-run financial services providers, which could influence the viability of certain business relationships or M&A decisions.

What's next?

- Ensure that all leveraged technologies and their usage can be easily explained to regulators, including associated governance and risk management structures.
- Ensure that service continuity/resilience plans are established for any providers of key services (e.g. ML, AI, cloud), including contracted third parties and alliance partners.
- Evaluate innovation priorities and determine technology needs.
- Assess risk appetite and existing risk management frameworks for new technologies and products (e.g. cryptoassets).
- Develop a posture/strategy for M&A activity, giving consideration to transaction size and specific targets based on technology, markets, and/or geographies; maintain, monitor, and periodically reassess a list of potential targets in light of the strategic plan.
- Maintain a dialogue with regulatory authorities, as appropriate.
- Review pending or anticipated acquisitions and third-party relationships for anti-trust issues and risks as well as for how new products will be structured and operationalized.



Key considerations for bank charter applications:

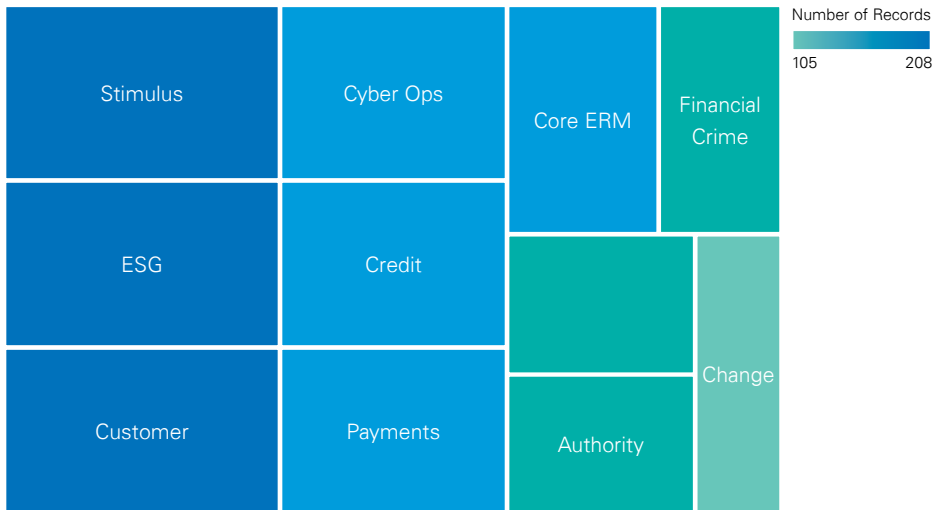
-  Organizers, management, directors
-  Business plan
-  Capital and liquidity
-  Consumer compliance
-  Financial inclusion
-  Contingency planning
-  Accounting and tax
-  Other regulators

Methodology

Historically, KPMG Regulatory Insights has prioritized the Ten Key Regulatory Challenges based on our assessment of policy announcements, regulatory activity, and client discussions. This year, we added a new dimension. KPMG Lighthouse Data and Analytics Center of Excellence utilized our 2019 and 2020 Washington Report 360 (WR360) newsletters (a curated weekly compilation of public policy, regulatory, and news articles impacting the financial services industry) to conduct Natural Language Processing (NLP) and text analytics to classify and thematically group the newsletter items, or records. The analysis included a technique called Guided Latent Dirichlet Allocation, which allows users to “seed” the algorithm with a series of words to guide their classification into predetermined topics – in this case the areas of regulatory challenge.

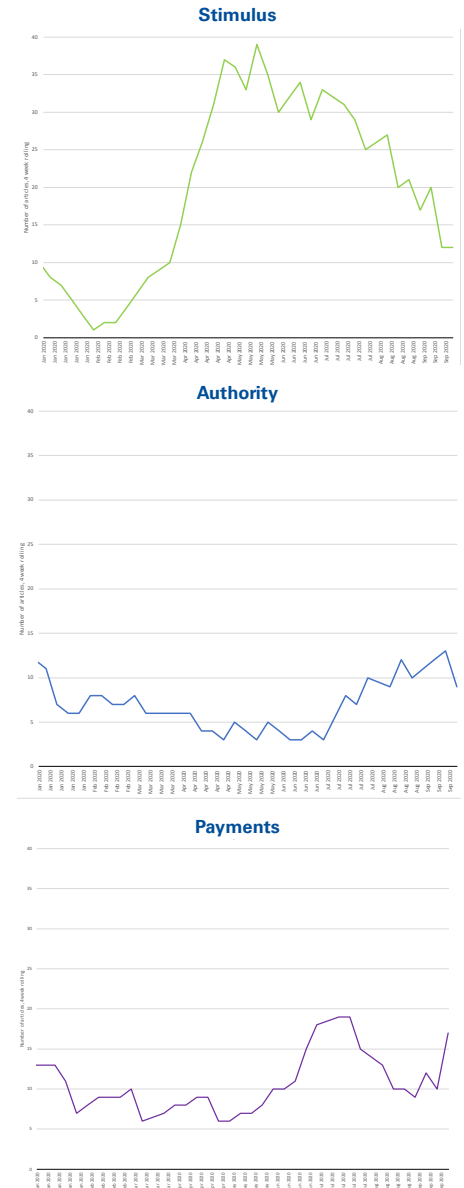
This graphic represents the number of records in each of the ten key challenge areas plus a “null” category for non-classified items. Note that some of the challenge areas we placed at the top for 2021 are those that may have had a lesser amount of news coverage but are anticipated to grow as well as those areas that tend to be thematic regulatory “standards”.

Washington Report 360: topics overall



Topic Short Name. Color shows sum of Number of Records. The marks are labeled by Topic Short Name.

Graphic representations of the number of WR360 articles, using a four-week rolling average, classified into individual challenge areas.



Timothy Cerino Managing Director, Data & Analytics

E: tcerino@kpmg.com

As a Managing Director in KPMG’s Lighthouse Data and Analytics COE, Tim leverages new big data architecture and statistical machine learning methods to provide advice and insights that complement traditional approaches and support Advisory engagements. Areas of opportunity include commercial banking, risk management, regulatory compliance, portfolio management, capital markets, corporate finance, and development of new, data-driven business solutions.

KPMG Regulatory Insights

We hope that you have enjoyed our insights in this publication and invite you to explore these and other timely regulatory topics as captured in our published thought leadership.

KPMG [Regulatory Insights](#) and our professionals regularly share ideas on financial services industry and technical issues with our clients and the marketplace through a range of publications, including analyses of emerging regulatory issues (Points of View), summaries of specific regulatory developments (Regulatory Alerts and Special Alerts), and a weekly newsletter covering legislative and policy actions (Washington Report 360).

Click below to access the libraries for our various thought leadership publications. If you are interested in subscribing to future issues, please [click here to subscribe](#).



Points of View

Insights and analyses of emerging regulatory issues impacting financial services firms.



Regulatory Alerts

Quick hitting summaries of specific regulatory developments and their impact on financial services firms.



Special Alerts

Short alerts summarizing high-profile regulatory developments with same-day release.
(same site as Regulatory Alerts)



Washington Report 360

A weekly newsletter covering legislative and regulatory developments affecting financial services firms—in 360 words or less.

Defined terms and abbreviations

ADA	American with Disabilities Act	FRB	Federal Reserve Board
ALLL	Allowance for Loan and Lease Losses	FSB	Financial Stability Board
AML	Anti-Money Laundering	FTC	Federal Trade Commission
ANPR	Advance Notice of Proposed Rulemaking	GDPR	EU General Data Protection Regulation
BAU	Business as Usual	HIPAA	Health Insurance Portability and Accountability Act
BCBS	Basel Committee on Banking Supervision	KPIs/KRIs	Key Performance Indicators/Key Risk Indicators
CARES Act	Coronavirus Aid, Relief, and Economic Security Act of 2020	KYC	Know-Your-Customer
CCAR	Comprehensive Capital Analysis and Review	LIBOR	London Inter-Bank Offered Rate
CCPA	California Consumer Privacy Act	M&A	Mergers & Acquisitions
CECL	Current Expected Credit Losses	ML	Machine Learning
CFPB	Consumer Financial Protection Bureau	NCUA	National Credit Union Administration
CFTC	Commodity Futures Trading Commission	NPR	Notice of Proposed Rulemaking
CPRA	California Privacy Rights Act	NYDFS	New York Department of Financial Services
CRA	Community Reinvestment Act	OCC	Office of the Comptroller of the Currency
CRE	Commercial Real Estate	OFAC	Office of Foreign Assets Control
DOJ	U.S. Department of Justice	PII	Personally Identifiable Information
DOL	U.S. Department of Labor	PPP	Paycheck Protection Program
ECOA	Equal Credit Opportunity Act	Reg BI	Regulation Best Interest
ERISA	Employee Retirement Income Security Act	RCSA	Risk Control Self-Assessment
ERM	Enterprise Risk Management	SAR	Suspicious Activity Report
ESG	Environmental, Social, and Governance	SASB	Sustainability Accounting Standards Board
EU	European Union	SBA	Small Business Administration
FAIR	Factor Analysis of Information Risk	SEC	Securities Exchange Commission
FBI	Federal Bureau of Investigation	SOFR	Secured Overnight Financing Rate
FCPA	Foreign Corrupt Practices Act	SOX	Sarbanes-Oxley Act
Federal Banking Agencies	FRB, OCC, and FDIC	TCFD	Task Force on Climate-related Financial Disclosure (FSB)
FDIC	Federal Deposit Insurance Corporation	TDR	Total Debt Restructuring
FinCEN	Financial Crimes Enforcement Network	TFCR	Task Force on Climate-related Financial Risks (BCBS)
FINRA	Financial Industry Regulatory Authority	UDAAP	Unfair, Deceptive, or Abusive Acts or Practices

Contributing authors:

Steven Arnold, Cameron Burke, John Caruso, Timothy Cerino, Anand Desai, Brian Hart, Michael Lamberth, Adam Levy, Chris Long, Amy Matsuo, Tim Phelps, Damian Plioplys, Chad Polen, Michael Scarpa, and Todd Semanco.

Acknowledgment:

We thank the following individuals for their assistance in drafting and producing this document: David Balbirnie, Sara Calenda, Dustin Crosby, Andrew Devlin, Brett Hayes, Amy Matsuo, Jonathan Meyer, Christopher Palumbo, Jean-Gabriel Prince, Michael Protevi, Sarah Silvis, Joe Slaninka, Karen Staines, and Stevi Winer.

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

kpmg.com/socialmedia

