Ten Key Regulatory Challenges of 2022

Preventing the domino effect

kpmg.com

Contents

Introduction

On behalf of KPMG Regulatory Insights, I am delighted to issue our Ten Key Regulatory Challenges for 2022. We anticipate that regulatory "perimeters" will continue to expand and expectations (without the need for new regulations, per se) will increase rapidly. All financial services companies should expect high levels of supervision and enforcement activity across each of these "Key Ten" challenge areas:

Rapid Change

- Fairness & Inclusion
- Climate & Sustainability
- Crypto & Digital Assets
- Platforms & Conduct

Maintain Focus

- Cyber & Data
- Fraud & Financial Crimes
- Valuation Vulnerabilities

Mitigate Risk

- Third Party & Cloud
- Tech & Resiliency
- Risk "Complacency"

We encourage you to reach out to us to learn more about the issues and actions highlighted in the following pages or to discuss your firm's unique challenges.

Sincerely,

Amy Matsuo
Principal and Leader,
ESG and Regulatory Insights

Fairness & Inclusion

Investor demand, public awareness, social unrest, and the priorities and directives of the Administration have focused regulatory attention on supervision and enforcement of consumer and investor protection on a broad scale and expanded the parameters of "fairness" to include all consumer touchpoints.

Prioritize and embed fairness across the customer journey from product/service design, marketing/advertising, disclosures, servicing, and customer interactions, including complaints management.
The perception of "fairness" has expanded beyond the parameters of fair lending and lending products specifically to include all access and touchpoints.

Execute centralized processes and quickly streamline and simplify all customer-focused communications.
Communications (in all formats and through all channels) are expected to be clear, accurate, and complete, providing disclosure sufficiently adequate for consumers to understand relevant information, alternatives, and/or conflicts of interest.

Enhance complaint management processes, technology, and data analytics; aggregate concerns, identify root causes, and deploy effective and streamlined responses.
Complaints management is fundamental to regulators' assessment of a company's compliance management system; it can serve as a guide to potentially emerging risks, management or structural deficiencies, third-party provider issues, recurring concerns, and necessary product or service improvements.

Set clear and measurable diversity, equity, and inclusion (DEI) goals; develop metrics to measure and monitor progress and factor into management accountability goals.
Calls to improve racial equity and inclusion within financial services have gained momentum consistent with investor demands, public awareness, social unrest, and the priorities and directives of the Administration. The pressure is only increasing.

Click the buttons to view more details on right

> Too many families were victimized… from the last crisis, and we must not allow robo-discrimination to proliferate in a new crisis.
>
> — **Rohit Chopra,** CFPB Director, October 2021

Todd Semanco
Partner, FS Regulatory & Compliance Risk
tsemanco@kpmg.com

Mike Sullivan
Principal, FS Regulatory & Compliance Risk
mmsullivan@kpmg.com

Mike Lamberth
Partner, FS Regulatory & Compliance Risk, Banking
mlamberth@kpmg.com

Climate & Sustainability

Pushed largely by significant and widespread investor demand and facilitated by myriad voluntary disclosure frameworks, financial services companies are working toward measuring, monitoring, and mitigating their climate-related financial risk. Regulatory expectations in this area have experienced sweeping changes that will continue, with rigor, into 2022 under existing and expanded jurisdictional authority. Federal financial agencies must develop, and execute on, a strategy to quantify, disclose, and mitigate the financial risk of climate change on both public and private assets. Public policy seeks to advance "consistent, clear, intelligible, comparable, and accurate disclosure of climate-related financial risk," and "to mitigate that risk and its drivers, while accounting for addressing disparate impacts on disadvantaged communities and communities of color."

Control production, consistency, and issuance of all climate and sustainability reporting (financial and non-financial), as well any disclosed metrics and measurements.
Without effective climate governance structures in place, a company may struggle to make climate-informed strategic decisions, manage climate-related risks, and establish and track climate-related metrics and targets. Climate risk is an issue that drives financial risk and opportunity; good governance should intrinsically include effective climate governance. For many companies, however, climate-related financial risk is a complex issue that entails grappling with scientific, macroeconomic, and policy uncertainties across broad time scales and beyond board terms.

Identify and develop qualitative and quantitative metrics and targets; hold business units, risk functions, and management responsible for integration and performance.
Climate-related financial reporting is rapidly evolving, pressured by demands from investors and other stakeholders, commitments by companies to achieve climate-related goals, calls for comparability and standardization, and efforts to increase the availability of data for metrics and disclosures. In the near term, multiple reporting frameworks (voluntary) are available to guide the development of metrics and targets though U.S. regulators are refining their expectations and beginning to detail more specific requirements.

Continue

Click the buttons to view more details on right

Reporting & Transparency

52% **of the U.S. CEOs said they are seeing significant demand for increased reporting and transparency on ESG issues today from stakeholders**

Source: *KPMG 2021 US CEO Outlook Survey*

Adam Levy
Principal, Modeling & Valuation
adamlevy@kpmg.com

Amy Matsuo
Principal and Leader, ESG and Regulatory Insights
amatsuo@kpmg.com

Climate & Sustainability

Develop initial assumptions and models for climate and sustainability inclusive of climate scenarios and/or stress tests (and in keeping with jurisdictional and global obligations).
Although there are not yet formal regulatory requirements in the US to conduct climate-related scenario analysis or stress testing, regulators do expect financial institutions to have systems in place to identify, measure, control, and monitor material risks, including climate risks. Globally, climate scenario analysis is emerging as a vital tool in assessing the impact of climate-related risks on financial institutions and financial stability more broadly.

Explore the potential for disproportionate climate risk-related impacts across customers/communities and/or geographies and industries; factor learnings into strategy, operations, and risk management.
Climate risk-related impacts and many of the efforts to control them (such as advancing net zero emissions goals and making climate resiliency investments) can exacerbate existing vulnerabilities. Physical risk events (e.g., floods, fires, storms, or rising sea levels) are geographically concentrated and can have spillover effects that place additional burden on vulnerable individuals, businesses, and municipalities such as spikes in insurance rates; impaired values, and potentially impaired usability, of properties and infrastructure; and investor abandonment. Transition risks (e.g., policy changes, consumer behavioral preferences) may initiate abrupt repricing events and result in stranded assets and impaired values.

Previous

Click the buttons to view more details on right

Crypto & Digital Assets

Regulatory activity around crypto and digital assets is intensifying as usage by investors, companies, and even some central banks, shows widespread interest and adoption at retail and institutional levels. The regulatory landscape in the U.S. is evolving alongside the market expansion with state and federal regulators and legislators all considering approaches to add clarity. Key issues include a focus on chartering, licensing, fraud and financial crimes risks, and consumer and investor protections.

Develop a corporate/product capability assessment and risk and compliance strategies for the appropriate licensing, issuance and/or use of digital assets
The current regulatory landscape for crypto and digital assets is fragmented and evolving quickly. Depending on the structure of the assets and the underlying facts and circumstances, multiple regulators at the federal and/or state level may have jurisdictional authority over a transaction. Gaps and overlaps are being created as the market develops; crypto technology firms are connecting to traditional financial systems and regulated banking entities are building out crypto infrastructure (e.g., custody services). Efforts to better define an appropriate regulatory regime, including licensing and chartering authorities, may require legislative change and could also change the relevant markets.

Establish/enhance internal risk policies, procedures, and controls with respect to digital assets and payments
Regulators are focused on consumer and investor protections across a broad array of risks such as fraud, cyber security, data privacy, misconduct, settlement, liquidity, market integrity, market volatility, transparency, and money laundering/terrorist financing. The enforcement environment is similarly complex, owing, in part, to the Administration's heightened focus on cybersecurity mitigation. Notably, DOJ has launched a National Cryptocurrency Enforcement Team to carry out investigations and enforcement of criminal misuse of cryptocurrencies; SEC and CFTC each continue to actively initiate enforcement actions within their respective jurisdictions.

Produce actionable and relevant digital asset information for board reporting
Regulators expect boards to set clear, aligned, and consistent direction regarding a firm's strategy and risk appetite based on information that is sufficient in scope, detail, and analysis to enable sound decision-making and consider potential risks.

Click the buttons to view more details on right

"The existing stablecoin market is worth nearly $130 billion, having grown 20-fold in the last 20 months."

— **Gary Gensler,**
SEC Chairman, Public Statement, November 2021

Damian Plioplys
Advisory Managing Director
FS Regulatory & Compliance Risk
dplioplys@kpmg.com

Chris Seigle
Director, FS Regulatory & Compliance Risk
cseigle@kpmg.com

Platforms & Conduct

Rapid developments in technology, increases in digital banking activity, growing sophistication of data collection, and the increasing influence of social media is reshaping the financial services landscape in ways never before seen or anticipated. These unprecedented times, underscored by ongoing social and economic changes associated with COVID-19, have fostered and accelerated unique advancements in the consumer experience—and given rise to new risks related to data security, fraud, and conflicts of interest.

Design compliant digital platforms with demonstrable and measurable customer experience, access, fairness, and inclusion principles and metrics
Digitalization has increased consumer expectations regarding the availability of, and access to, core financial services, including payments, savings, lending, and investing. In general, they are looking for powerful, intuitive, and personalized interfaces to conduct transactions through multiple and interconnected channels (e.g., online, mobile, phone, in person) on an anytime, anywhere basis. Social media is a benchmark, having set expectations for personalized experience that are now carried through to financial services by fintechs and Big Tech companies with access to vast stores of data.

Ensure data quality and integrity controls between the digital platform and the broader surveillance architecture at critical data handoffs in the workflow in order to maximize the integrity of the market conduct surveillances.

Assess, make needed changes, and actively surveil and mitigate conflicts of interest and market conduct risk.
Growing levels of scrutiny now surround long-standing—and some new—market practices that may present conflicts of interest for broker-dealers, exchanges, and wholesalers and could put fair market conduct at risk for investors.

Heighted regulatory focus on investor protections and conflicts of interest will assure continued attention on:

Click the buttons to view more details on right

Cyber & Data

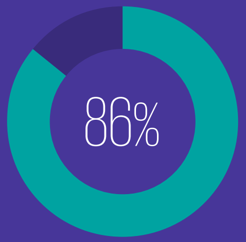
The financial services regulators have called cyber risk the foremost risk to financial stability—and the Administration has called it a persistent and increasingly sophisticated threat that weighs heavily on governments and financial services companies alike. Given the highly interconnected nature of the financial services sector and its dependencies on critical third-party service providers, all participants in the financial system must implement risk mitigation and resilience initiatives relative to both frequency and impact of cyber threats. Current or emerging threats include malware (e.g., ransomware), supply chain risk, and sophisticated DDOS.

Evolve your customer and enterprise identity and access management programs to ensure appropriate preventions against latest account takeover threats.
Increases in data transfer sophistication have widened the array of entry points to a financial services company's assets and consumer data, expanding the number of attack vectors for malicious actors. Weak access management and authentication controls provide opportunity for cyber attackers to leverage compromised credentials to access the same resources and data that legitimate users can.

Use orchestration and automation to augment limited cyber security resources and improve your speed to respond.
Increasing legal and regulatory compliance requirements are complicating compliance risks and serving as a key driver for enhancements to cyber security capabilities. Security orchestration, automation, and response (SOAR) tools combine to allow companies to collect data about security threats from multiple sources, initiate a response with limited human interaction, and coordinate post-incident reporting and information sharing. Benefits include faster detection and reaction, broader threat context, integrated data management safeguards, and lower costs—which should help companies weather the flurry of regulatory attention to cyber and data issues in 2022, including:

Identify, manage and protect the organization's information assets (throughout the data management lifecycle) by embedding "privacy by design" and automating data protection.
Businesses are collecting increasing amounts of customer data to feed predictive analytics, personalize marketing campaigns, and introduce/improve products and services. Consumers, for the most part, are increasingly concerned about how their information is being collected, used, and protected—focusing regulatory attention on customer data privacy and protection. "Privacy by design" principles set a baseline for robust data protection by embedding privacy into the design, operation, and management of new applications, including IT systems, AI platforms, and digital business practices, with the goal of preventing privacy vulnerabilities.

Click the buttons to view more details on right



of U.S. consumers say data privacy is a concern

don't trust companies to ethically use their data

Source: *Corporate data responsibility: Bridging the consumer trust gap*, KPMG, August 2021, KPMG

Matt Miller
Principal, Cyber Security Services
matthewpmiller@kpmg.com

Orson Lucas
Principal, Cyber Security Services
olucas@kpmg.com

Fraud & Financial Crimes

The adoption of innovative technologies to improve the effectiveness of fraud and financial crimes risks management is becoming an imperative as regulators emphasize innovative approaches (e.g., machine learning, enhanced data analytics) and the preponderance of threat risks, from cybersecurity to ransomware to cryptocurrency to identity theft, are technology-driven. The Administration has prioritized many of these concerns as issues of national security, embarking on a "whole-of-government" approach; new and emerging areas of focus are tied to transparency and ESG.

Reduce synthetic identity fraud by integrating automation and analytics into your client onboarding and maintenance processes.
Synthetic identity fraud (SIF) is among the fastest growing financial crimes in the United States. In contrast with traditional identity theft, SIF uses a combination of real and fabricated information to create a new identity and build a credit file over time—which makes it difficult to flag as suspicious using conventional fraud detection models. The FRB highlights ways to mitigate SIF risks.

Increase your defenses against account takeover and social engineering for real time payments through the eradication of out-of-date authentication technologies.
Real-time and faster payments shorten financial transaction clearing times, raising the potential for security and fraud risks and reinforcing the need for updated and agile security and fraud detection programs, including authentication and access protocols. Frauds to watch for might include online fraud (e.g., malware, phishing attempts), first-party fraud (e.g., SIFs), and false claims.

Establish a mature insider risk program, that includes behavioral models and scenario analysis, to reduce the likelihood of employee conduct and financial crime risk (including reputational harm, espionage, embezzlement, market and price manipulation).
Insider threats reflect a combination of technology and human risks. In the digital environment, insider attacks can result in financial and intellectual property theft, damaged or destroyed assets, and firm-wide disruption to internal systems and customer operations. Prevention and detection, however, can be difficult because of insiders' familiarity with, and trusted access to, firm systems; human input, analysis, and intelligence is needed to interpret technical data (e.g., from cybersecurity tools) and identify anomalous insider behavior. The scope of insiders will include directors, employees, contractors, and third parties.

Strengthen controls around evolving regulatory focal areas.
FinCEN released government-wide AML/CFT priorities in June 2021 and include corruption; cybercrime (including cybersecurity and virtual currency considerations); terrorist financing; fraud (including SIF); transnational criminal organization activity; drug trafficking; human trafficking; and proliferation financing.

Click the buttons to view more details on right

Ransomware SAR filings

458 first six months of 2021

487 total for 2020

Source: *Financial Trend Analysis*, Ransomware Trends, FinCEN, October 2021

Edwige Sacco
Principal, Forensic
esacco@kpmg.com

Todd Semanco
Partner, FS Regulatory & Compliance Risk
tsemanco@kpmg.com

Matt Miller
Principal, Cyber Security Services
matthewpmiller@kpmg.com

Valuation Vulnerabilities

There is a large amount of debt and leverage in some sectors of the financial system, coupled with historically elevated valuations for almost all asset classes (from corporate equities to real estate to cryptocurrencies). These areas may be susceptible to correction if rising inflation sends interest rates sharply higher; even relatively small pullbacks could have outsized impacts on asset values in market segments with concentrated or leveraged exposure. Regulatory focus on principles of fairness and competition could separately impose impacts on valuations.

Monitor valuation exposures and develop scenario and stress testing to gauge sensitivities.
As financial risks from the pandemic dissipate, regulators are looking to medium—and longer-term vulnerabilities, which can manifest through direct, indirect, concentrated, or leveraged exposures. Regulators are taking note of "exuberance" in asset classes such as residential real estate and financial markets (including corporate equities and "riskier assets" such as cryptocurrencies) as well as the potential for abrupt or steep valuation adjustments based on a variety of factors that may present individually or in concert.

Ensure effective LIBOR transition management processes and controls.
Federal and state financial regulators have cited the LIBOR transition as a key supervisory priority for 2022. To properly mitigate operational, compliance, legal, and reputational risks, as well as to prevent balance sheet destabilization and adverse financial impacts.

Evaluate synthesis and alignment in M&A considerations.
Digital adoption, technology modernization, competition from technology-driven services companies, reach for scale, market consolidation, and, most recently, ESG considerations are driving financial services companies to pursue a variety of M&A transactions as well as partnerships, and/or alliances.

Reinforce rigor of quantifiable and measurable credit standards across the credit lifecycle.
The quantification and measurement of credit risk across market sectors has posed challenges in the pandemic era due to the varying degree of government policies or programs supporting sector performance.

Click the buttons to view more details on right

> ...Cessation of LIBOR use...will be one of the highest priorities of...bank supervisors.
>
> — *"Goodbye to All That: The End of LIBOR,"* **Randall Quarles,** FRB, October 2021

Mark Nowakowski
Principal, Modeling & Valuation
mnowakowski@kpmg.com

Chris Long
Principal, Financial Services – Capital Markets
chrislong@kpmg.com

Third Party & Cloud

Driven to enhance competitiveness, expand operations, and accommodate customer needs, financial services companies are forming more numerous and complex relationships with third-party companies at significant speed and scale, including financial technology-focused entities such as cloud service providers. These relationships offer advantages but can also reduce management's direct control of activities, which may introduce new risks or elevate existing risks for companies and their customers.

Centralize and automate third party risk management (TPRM) processes while executing a resilient vendor strategy.

Execute dynamic TPRM risk assessments, with clarity on direct and indirect risk assessment, measurements and contingencies.
Risk assessments are foundational to a risk-based TPRM program and should be conducted over the TPRM life cycle. Deficiencies may expose an organization to strategic, reputation, credit, operational, compliance, liquidity, and/or concentration risks.

Ensure TPRM meets or exceed global and jurisdictional regulatory expectations.
The location of a third party (or fourth party) does not relieve the financial services company of its responsibility for compliance with all applicable laws and regulations, including ensuring that the third party also meets those obligations.

Use data sandboxes and parallel data proof of concept runs for changes to procurement and TPRM processes.

Build a "zero trust" security environment with modern security tools and continuous monitoring for IT/Cyber controls.

Click the buttons to view more details on right

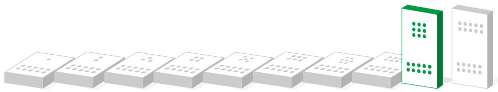
Six in 10 respondents (59%) warn that their technology still does not give them "**anywhere near the visibility they need**" to manage third-party risk across the supply chain.

Source: *KPMG TPRM Survey Outlook 2022* (to be released early 2022)

Greg Matthews
Partner, FS Regulatory & Compliance Risk
gmatthews1@kpmg.com

Sai Gadia
Partner, Cyber Security Services
sgadia@kpmg.com

Tech & Resiliency



Recent events, including technology-based failures, cyber incidents, pandemic outbreaks, and natural disasters, have made clear that significant disruptions are increasingly likely and can be interconnected (consider how a health crisis sparked a mobility crisis that spawned a financial crisis). Although advances in technology have improved firms' ability to identify and recover from such disruptions, the frequency of events and potential for interconnectedness and/or interdependencies to amplify risks nonetheless underscore the need for operational resilience and are prompting leading companies to adopt a more holistic, multi-function approach.

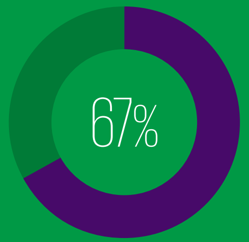
Set resilience standards and methodology for resilience criticality for services; map business assets to these services.
Sound practices prioritize the operational resilience of a firm's critical operations and core business lines; however, other operations, services, and functions for which a disruption could have a significant adverse impact on the firm or its customers also should be identified and addressed.

Measure asset financial and non-financial risk exposure, scoring and inputs for resiliency implications (e.g., vulnerability management, end of life, data classification).
Identification of financial and non-financial risk exposure is based on the multi-lines of impact within the firm. As risks are continuously evolving, controls processes and procedures should anticipate, test, and mitigate the impact of future threats and potential disruption.

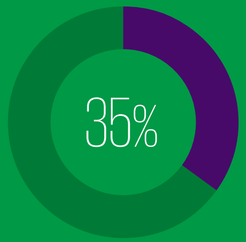
Provide transparency to boards and senior management with regular insights that clearly articulate minimum service levels, and degrees of resilience.
A company's board of directors and senior management must establish, oversee, and implement an effective operational resilience approach that enables them to respond and adapt to, and recover and learn from, disruptive events so that they can minimize the potential impact of disruptions and operate with confidence during a disruption.

Click the buttons to view more details on right

Top ethics and compliance activities to enhance



Use of automation and technology



Data analytics

Source: *KPMG CCO Survey 2021*, July 2021

Anand Desai
Principal, Technology Risk Management
ananddesai@kpmg.com

John Kemler
Managing Director, FS Regulatory & Compliance Risk
jkemler@kpmg.com

Risk 'Complacency'

Regulators view "risk complacency" by financial service companies as a potential threat to both stakeholder trust and safety and soundness. Companies must deliberately ensure that they are guarding against overconfidence—particularly during times of business, M&A, and innovative growth—by raising risk and compliance investment and voice.

Appropriately stature, recognize and size risk management.
Prudent risk and compliance management (commensurate with size, complexity, and risk profile) must accompany business change and growth, as well as anticipate and address expanded regulatory risk expectations.

Invest in data-driven risk automation, analytics and process efficiency.
Financial service companies must continuously determine how best to utilize data and technology to meet consumer and client demands—both from a business and a risk perspective. Regulators expect companies to take a data-driven approach to risk and compliance monitoring and assessment. Likewise, regulators increasingly utilize data-driven supervision and enforcement.

Anticipate and incorporate emerging risks, but don't lag in remediating known (or should have known) issues.
Financial service companies must incorporate emerging risks and regulatory expectations, but also continue to demonstrate timely identification and remediation of issues.

Champion risk-embedded business, operational and technology change.
Regulators will expect that risk and control functions are part of continued business, operational and technology change. The sense that "it cannot happen here", "the third party owns that risk", or "that's the way we have always done it" is unlikely to be a strong or sufficient risk stance and will be increasingly pressured by regulatory supervision and enforcement.

Click the buttons to view more details on right

"...Over-confidence leading to complacency is a risk—when prudent risk management is set aside in pursuit of profit."

— **Michael Hsu,**
Acting Comptroller of the Currency, August 2021

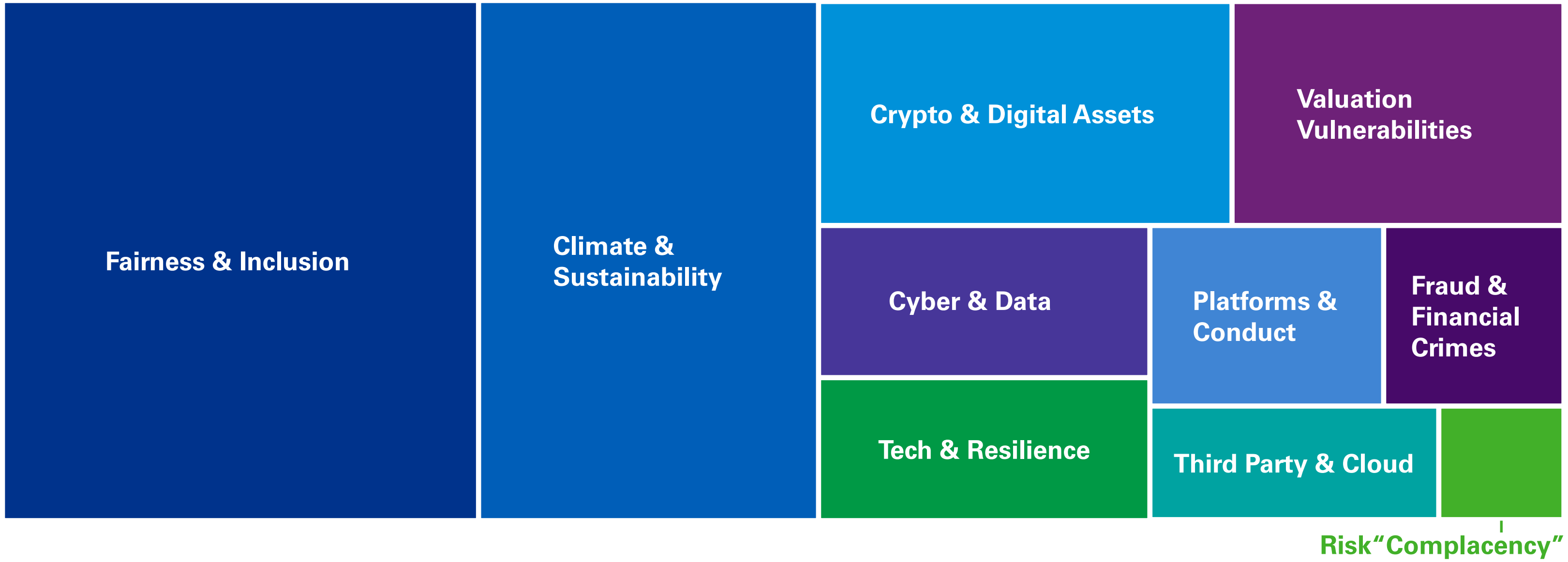
Amy Matsuo
Principal and Leader, ESG and Regulatory Insights
amatsuo@kpmg.com

Julie Gerlach
Partner, Internal Audit & Enterprise Risk
jgerlach@kpmg.com

Methodology

Historically, KPMG Regulatory Insights has prioritized the Ten Key Regulatory Challenges based on our assessment of policy announcements, regulatory activity, and client discussions. Last 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 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 year, with the impacts of COVID-19 and the change in Administrations and related regulatory priorities, we have limited our analysis to WR360 newsletters released in 2021. This graph visually represents the number of records in each of the ten key challenge areas.



Amy Matsuo
Principal and Leader, ESG and Regulatory Insights
amatsuo@kpmg.com

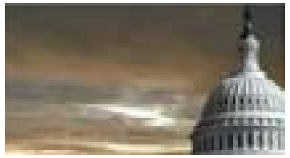
Timothy Cerino
Managing Director, Data & Analytics
tcerino@kpmg.com

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 is the thought leader hub for timely insight on risk and regulatory developments. Our perspectives enable our clients to help anticipate and manage regulatory change across the U.S. regulatory landscape. In collaboration with professionals across the firm's global regulatory practices, we provide perspectives on evolving supervisory, regulatory, and enforcement trends as they occur.

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.

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

Amy Matsuo
Principal and Leader, ESG and Regulatory Insights
amatsuo@kpmg.com

Defined Terms & Abbreviations

ADA	American with Disabilities Act
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Act of 2020
ANPR	Advance Notice of Proposed Rulemaking
BAU	Business as Usual
BCBS	Basel Committee on Banking Supervision
CARES Act	Coronavirus Aid, Relief, and Economic Security Act of 2020
CCAR	Comprehensive Capital Analysis and Review
CCPA	California Consumer Privacy Act
CECL	Current Expected Credit Losses
CFPB	Consumer Financial Protection Bureau
CFTC	Commodity Futures Trading Commission
CPRA	California Privacy Rights Act
CRA	Community Reinvestment Act
CSR/IR	Corporate Social Responsibility/Integrated Reporting
DDOS	Distributed Denial of Service
DEP	Digital Engagement Practices
DOJ	U.S. Department of Justice
ECOA	Equal Credit Opportunity Act
ERISA	Employee Retirement Income Security Act

ERM	Enterprise Risk Management
ESG	Environmental, Social, and Governance
EU	European Union
FCPA	Foreign Corrupt Practices Act
FDIC	Federal Deposit Insurance Corporation
FinCEN	Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority
FRB	Federal Reserve Board
FSB	Financial Stability Board
FTC	Federal Trade Commission
GDPR	EU General Data Protection Regulation
GRI	Global Reporting Initiative
HR	Human Resources
LMI	Low- and Moderate-Income
LOB	Line of Business
KYC	Know-Your-Customer
LIBOR	London Inter-bank Offered Rate
M&A	Mergers & Acquisitions
ML	Machine Learning
MSB/MTL	Money Services Business/Money Transmitter Licensee

NCUA	National Credit Union Administration
NYDFS	New York Department of Financial Services
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
PFOF	Payment for Order Flow
PII	Personal Identity Information
PPP	Paycheck Protection Program
Reg BI	Regulation Best Interest
SAR	Suspicious Activity Report
SASB	Sustainability Accounting Standards Board
SEC	Securities Exchange Commission
SOFR	Secured Overnight Financing Rate
TCFD	Task Force on Climate-related Financial Disclosure (FSB)
TFCR	Task Force on Climate-related Financial Risks (BCBS)
UDAAP	Unfair, Deceptive, or Abusive Acts or Practices
TDR	Total Debt Restructuring
TFCR	Task Force on Climate-related Financial Risks (BCBS)
UDAAP	Unfair, Deceptive, or Abusive Acts or Practices

Contact

Amy Matsuo
Principal and Leader, ESG and Regulatory Insights
amatsuo@kpmg.com

Acknowledgement

We thank the following individuals for their assistance in drafting and producing this document:
Amy Matsuo, Mark Dickemann, Steven Honeycutt, Amanda Kerr, Nisha Lane, Sam Mahler,
Daniel Marchesani, Milan Patel, Jean-Gabriel Prince, Joe Slaninka, Karen Staines, Royal Thankachan.