



Ten Key Regulatory Challenges of 2024

Strengthen the cards you hold



Introduction

I am delighted to present the KPMG Regulatory Insights' Ten Key Regulatory Challenges of 2024—our ninth annual edition!

Key takeaways

1. A return to heightened risk standards—Demonstrate sustainability
2. Prudential regulators “level-up” expectations—Show strength and resiliency
3. Data, models, and “model-like” risks gain focus—Drive security, privacy, and fairness
4. Strong supervisory and enforcement action—Prove accountability and stakeholder trust
5. “Old regulations” apply, even to new areas

We are experiencing a level of regulatory intensity rarely seen—not the simple effect of “net-new” regulations but the combination of a high-volume of regulatory issuances, the complexity and breadth of regulatory supervision, and the impact that these changes impose across the organization.

The “Key Ten” offers actions to consider and key “big rock” regulations to watch. Regulatory intensity will be felt across all areas of regulatory challenge—with our Regulatory Barometer, KPMG Regulatory Insights quantifies the regulatory intensity, giving a predictive indicator of the regulatory landscape.

Expect 2024 to be a year of continued economic fluctuations, election-year uncertainties, and legal actions giving fuel to already elevated levels of regulatory intensity.

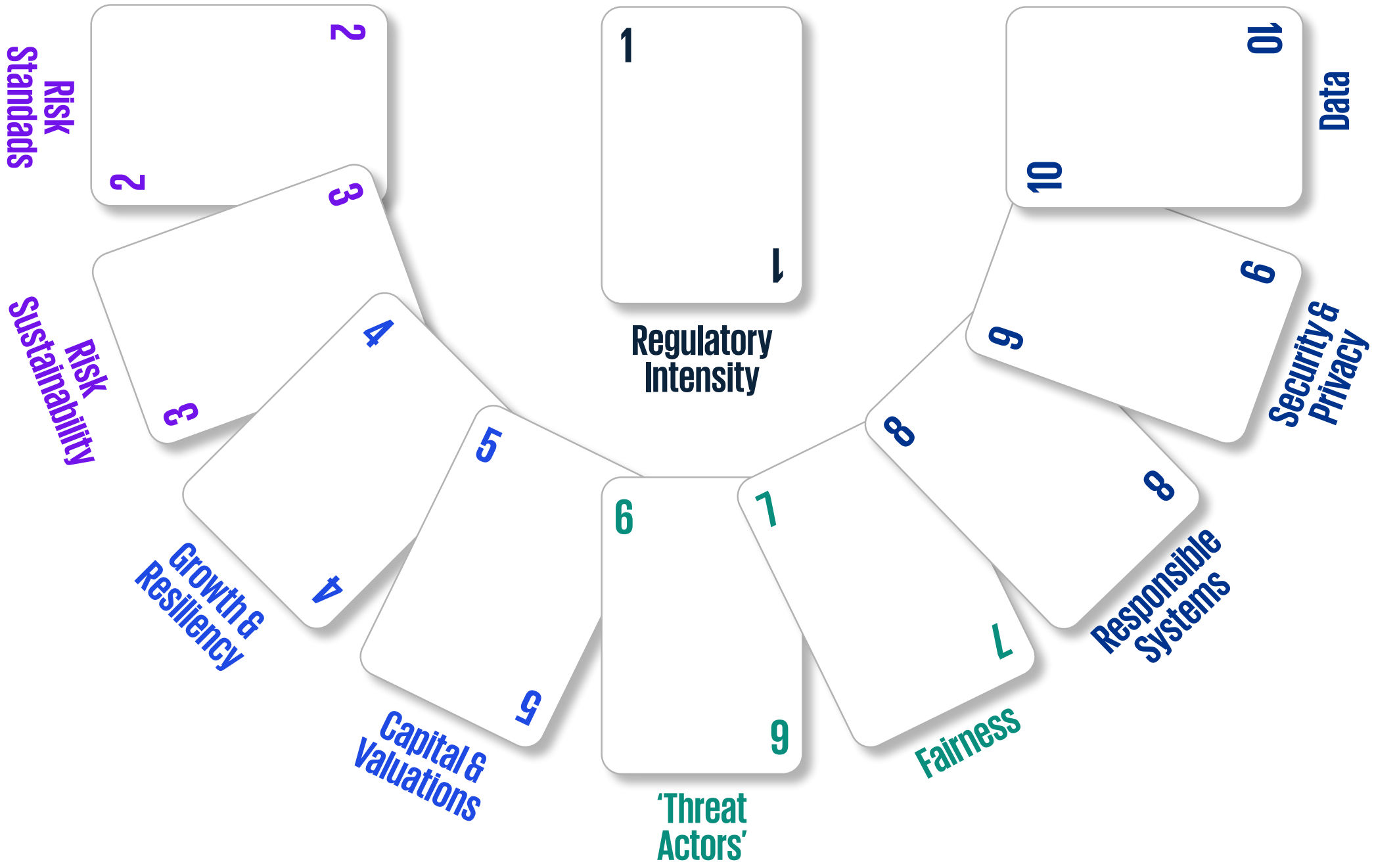
Strengthen the cards you hold!



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

Ten Key Regulatory Challenges of 2024

Strengthen the cards you hold



Source: KPMG Regulatory Insights

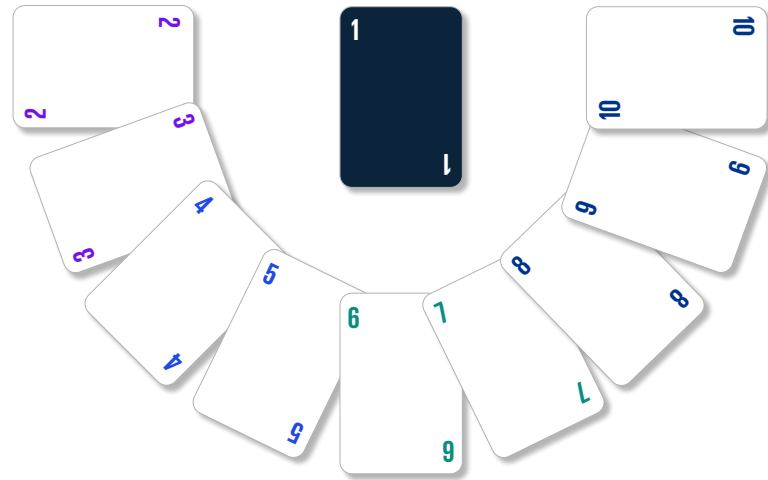

Risk Management
& Governance


Financial
Risk


Consumer/Investor
Protection

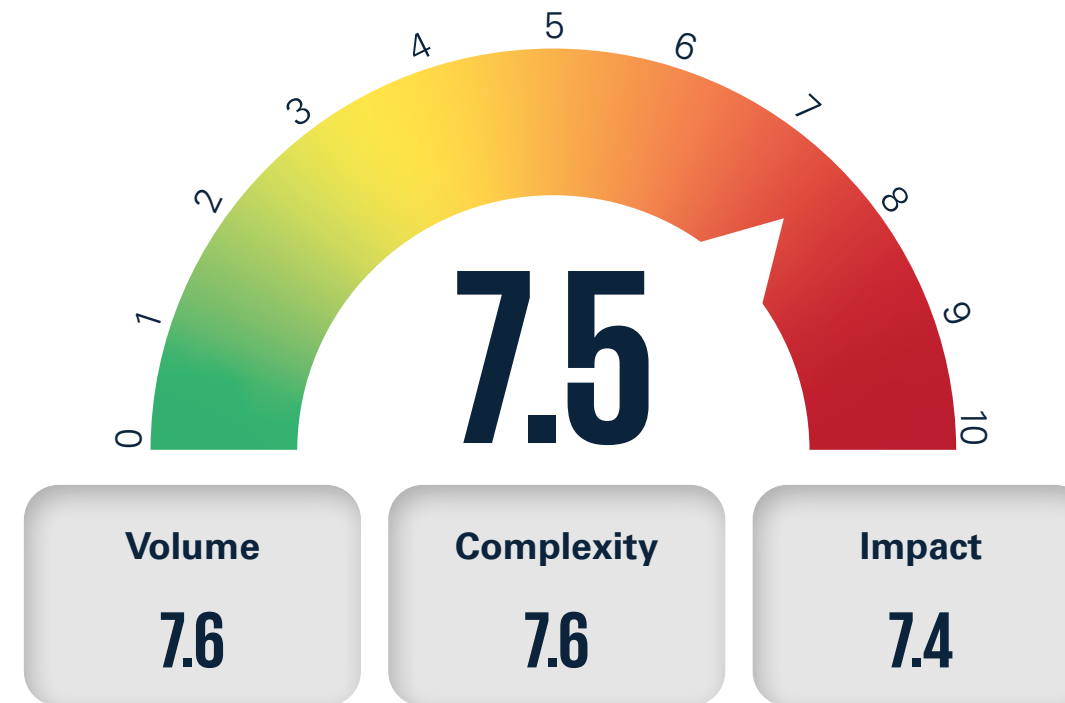

Technology
& Data Risk

Regulatory Intensity



Given continued economic fluctuations, election-year uncertainties, and legal actions, expect high regulatory intensity particularly in the areas of risk management/governance, financial risk, and data

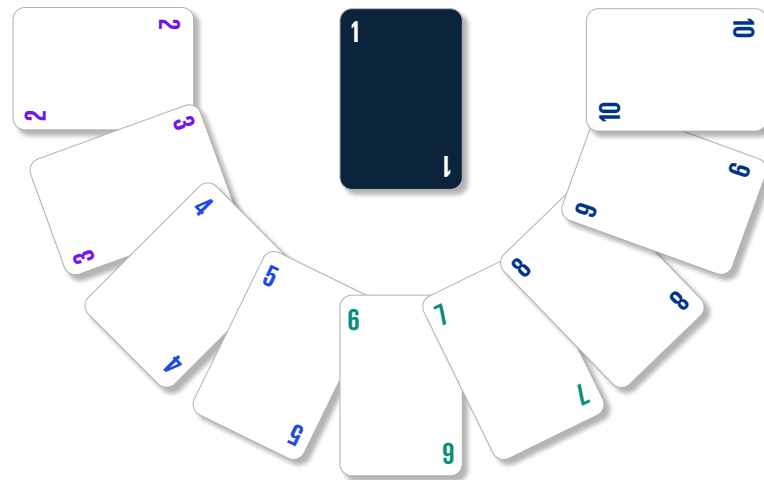
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: KPMG Regulatory Insights

Regulatory Intensity



Impact

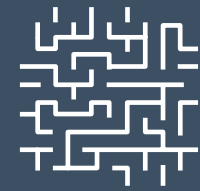
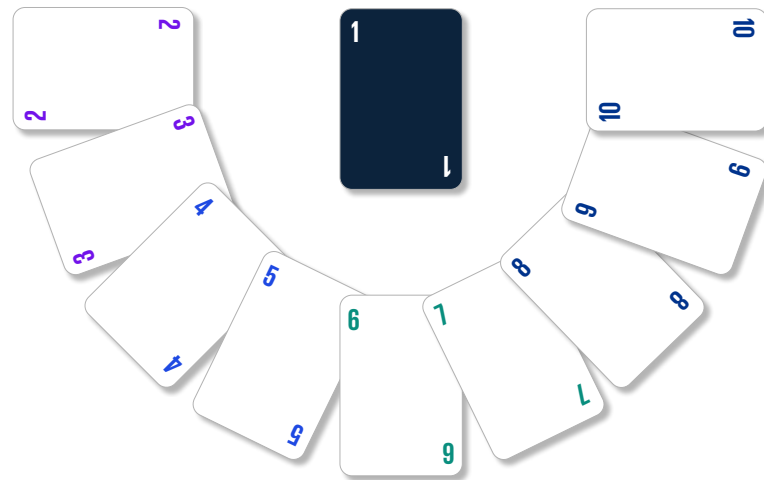
In 2024, the intensity of supervision and regulation will continue with marked changes to reviews and examinations (e.g., more frequent, faster response, issues escalation, more rapid remediation) and a focus on risk management and governance (e.g., liquidity, capital, interest rate, concentrations, operations). This intensity will require financial services providers to (re)assess the current and target states of their operations; risk management policies, governance, and controls; and data and systems infrastructure.

Firms should anticipate:

- **Immediate Action:** Growing scrutiny of “weaknesses” in risk management and compliance, especially with regard to correcting deficiencies, will drive regulators to more stringent evaluations, possible ratings downgrades, and/or supervisory and enforcement actions. Firms will need to show both immediate assessment and resources to address potential weaknesses, as well as sustained processes (and executive accountability) to mitigate and manage risks.
- **Commitment to Resolve:** Regulators will view inability to timely remediate supervisory concerns or identified “weaknesses,” or continuing, recurring, or increasing deficiencies, as cause to impose increasingly comprehensive and severe actions up to and including limitations on growth and required divestitures. Firms will need to demonstrate a commitment to resolving “weaknesses” such as through self-identification, proactive disclosure, completed root cause remediation, voluntary restitution, and executive accountability.
- **Intangible Risks:** Regulators will expect risk management and governance processes to be adequately resourced (e.g., skilled staff, technology investment); risk management and compliance deficiencies (and particularly during times of “cost take-out”) may be seen as indicators of insufficient investment and/or resourcing, increasing both operational and intangible risks. Regulators will identify firms as “persistently weak” or “repeat offenders” in public enforcement actions, which will subject those firms to heightened reputation risk and may also have implications to the examinations of other regulators. Similarly, requirements or restrictions imposed on firms (e.g., reduction in asset size, additions to capital or liquidity, divestiture of subsidiaries or business lines) may heighten risks related to legal and compliance as well as market share and competition.

Source: **KPMG Regulatory Insights**

Regulatory Intensity



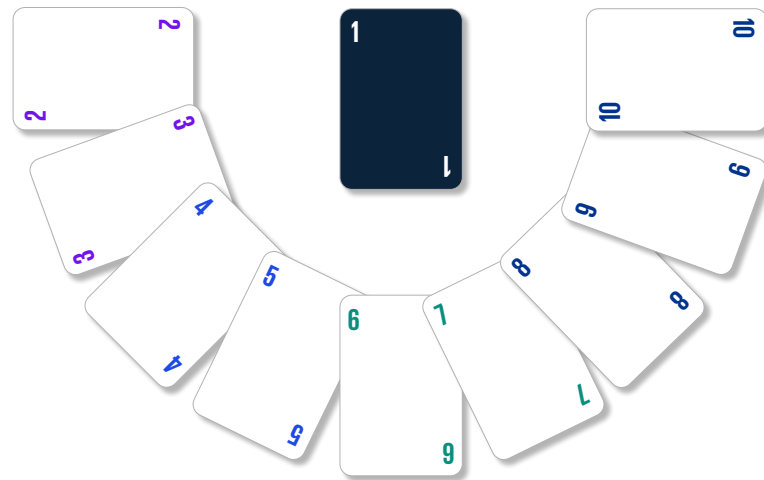
Complexity

Expanded regulatory “perimeters,” innovative technologies, rapidly evolving products and services, growing interconnectedness, and the global political environment are contributing to heightened supervision and examination by all regulators, acting independently and in coordination, at the state, federal, and international levels, significantly enhancing the complexity of regulatory compliance. In 2024, firms will see ongoing and potentially increasing:

- **Regulatory Discord:** International, federal, and state regulators will differ in public policies, areas of supervisory focus, and regulatory approaches even as they work on the same regulatory concerns, as exemplified by:
 - Efforts to promote international regulatory coordination and alignment (e.g., climate disclosure standards, capital and liquidity requirements) amidst U.S.-specific adaptation.
 - Multiagency approaches and coordination (i.e., federal “whole-of-government” approaches pursuant to the Administration’s Executive Orders) to address regulatory issues (e.g., cybersecurity, AI, consumer protection) amidst federal-to-state and state-to-state discord and divergence (and timing).
- **Legal Challenge:** Challenges to regulatory authorities, jurisdictions, and rulemakings (e.g., CFPB funding structure, SEC climate disclosures, charters for novel institutions, crypto/digital assets) are increasingly expected, raising the level of uncertainty and complexity in the regulatory landscape. Firms will see that to preempt such challenges, regulators now regularly stipulate the agency’s authority to issue regulations and/or take actions.
- **Implementation Challenge:** The regulatory discord and legal challenges will drive the need for firms to determine the level of direct investment (e.g., infrastructure and systems, people and resources, data) to prepare to comply with supervisory and regulatory expectations that may at present be uncertain or in flux.

Source: **KPMG Regulatory Insights**

Regulatory Intensity



Volume

The ambitious pace for new regulations set by regulators (led by the SEC) in recent years will likely slow in 2024, an election year, as regulators work to finalize existing proposals (some of which are already known to be the object of current and/or anticipated legal challenge). Additionally, 2024 “net-new” regulations may be thwarted amidst the “lookback” period by which Congress might review and disapprove final rules under provisions of the Congressional Review Act (summer 2024). Nevertheless, firms can expect regulatory activity throughout 2024 to encompass:

- **New “Big Rocks”**: Regulators will look to finalize “significant” new regulations (e.g., banking agency rules on Basel III capital standards, long-term debt requirements, SEC rules on climate disclosure, market structure).
- **Old is New**: Regulators will continue to vigorously apply existing rules, regulations, and guidance (e.g., heightened standards/ERM, financial stability, AML/BSA, UDAAP/UDAP, fair marketing, conflicts of interest, recordkeeping) to new and emerging areas (e.g., “automated systems,” predictive analytics, crypto and digital assets, digital devices) in supervision and enforcements.
- **Supervision and Enforcements Coming**: The uptick in supervision and enforcement activities will continue throughout 2024, including:
 - Continued/expanded prudential regulatory activity in areas of capital management, liquidity management, enhanced regulatory supervision, enterprise risk management, AML, and integrated data and reporting.
 - SEC/FINRA activity in areas of Best Interest, market structures (including Best Execution), cybersecurity risk management, investment adviser supervision, and conflicts of interest.

Regulators will also signal new areas of supervisory focus and emerging risk through risk alerts, speeches, blogs, and reports.

Source: **KPMG Regulatory Insights**

Regulatory Intensity



What to watch

Firms should look for the following items to set expectations about next years' regulatory intensity:

- **Regulatory Agendas:** Fall and Spring regulatory agendas released by each of the agencies outline rulemaking actions expected to be released in the next twelve months. Fall agendas are typically released in November; Spring agendas in June.
- **Supervision/Examination Reports:** The publication of regulators' supervisory and regulatory summary reports and priorities, including the FRB Supervision & Regulation Report (November/May) and Financial Stability Report (November/May); OCC Risk Perspectives Report (December/June); FDIC Risk Review (spring); CFPB Supervisory Highlights (biannual); SEC Examination Priorities (January/February); and FINRA Report on Examination and Risk Monitoring Programs (January/February).
- **Testimony/Speeches:** Congressional testimony related to oversight, pivotal speeches and/or statements indicating emerging risks and/or areas of rulemaking.
- **Enforcements/Legal Actions:** Public enforcement actions and/or legal actions that outline deficiencies related to compliance with specific laws and regulations as well as remedial actions to take.

Source: **KPMG Regulatory Insights**

KPMG Thought Leadership

Regulatory Insights Materials

[Regulatory Intensity: The standards go to new heights](#)

[The 'Empowerment' of State Law and Regulations](#)

For more information on ongoing Regulatory Insights materials, **Click Here**



Regulatory Intensity



Call to action...

- **Allocated sufficient resources:** Allocate sufficient investment, resourcing, and time to “regulatory intensity,” inclusive of, but not exclusively to, net-new regulations. This will often involve strong, centralized regulatory relations and regulatory remediation teams.
- **Implement “regulatory routines”:** Develop and execute on “regulatory routines,” inclusive of process automation and data analysis, for consistency and trends (including for regulatory requests and corporate responses).
- **Map regulations to risk assessments and controls:** Dynamically map regulations and regulatory expectations to risk assessments and risk controls, built on a robust regulatory change management inventory and process.
- **Integrate issues management into risk assessments:** Integrate regulatory issues management into dynamic risk assessments, with clearly defined ownership and accountability for resolution and critical challenge.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Banking and capital markets](#)

[Insurance](#)

[Asset Management](#)

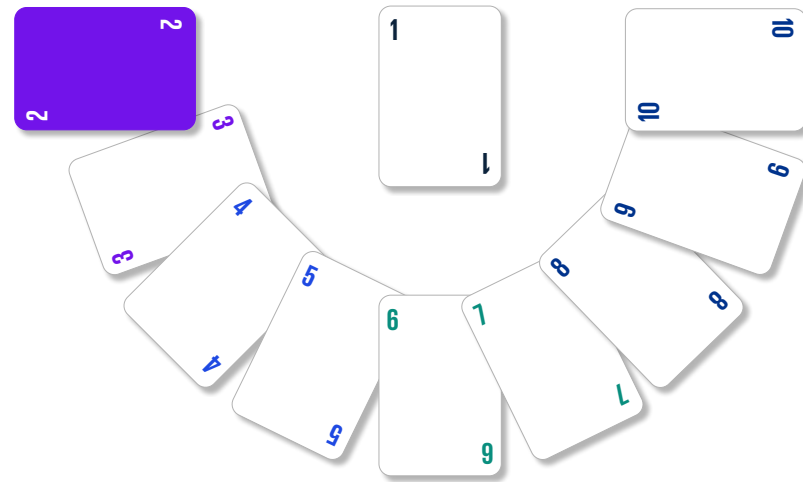
Contacts

Amy Matsuo

Principal

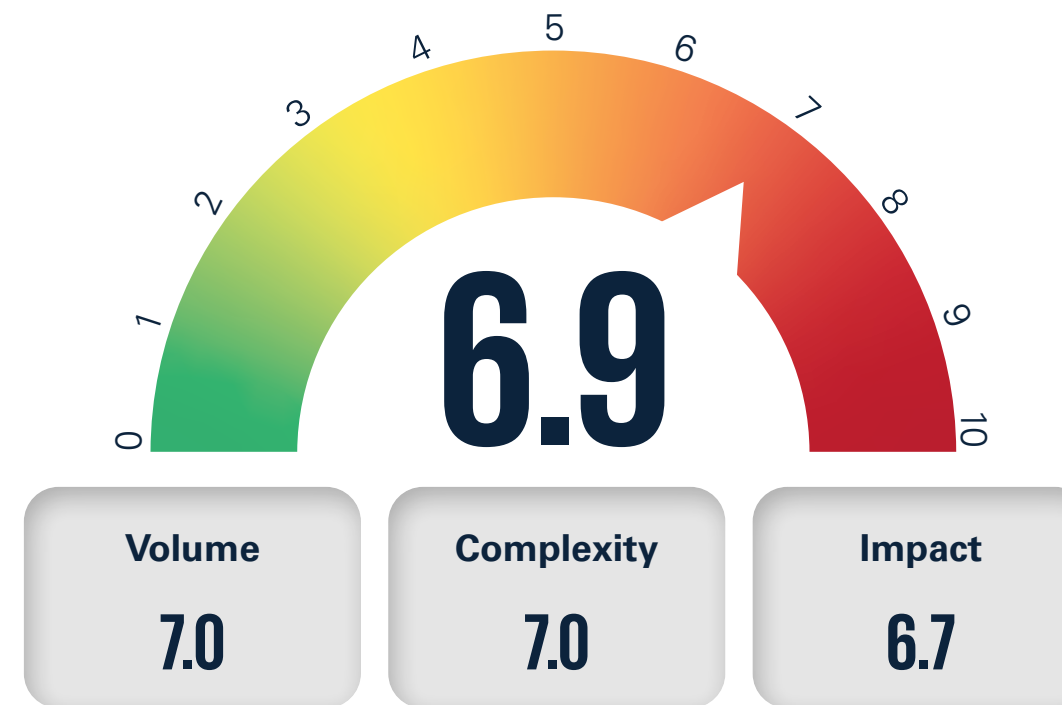
amatsuo@kpmg.com

Risk Standards



Supervisory intensity and enforcement, a focus on agility and mitigation of risk and compliance “shocks”, and expectations for robust (and demonstrable) risk accountability and governance combine to heighten risk standards.

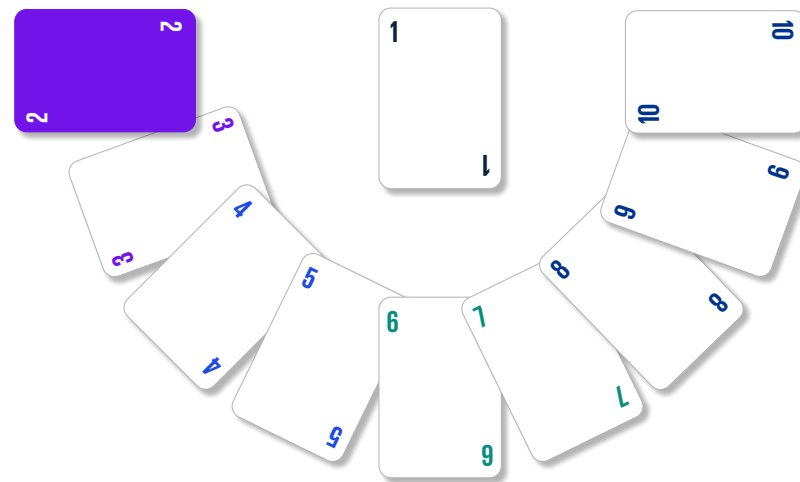
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: KPMG Regulatory Insights

Risk Standards



Heightened standards

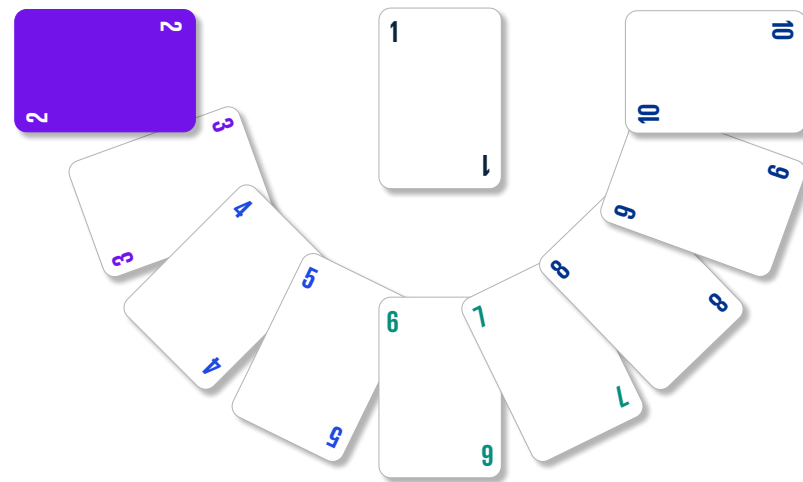
Reinforcing the importance of risk management, issues management, and governance, regulators have signaled expectations for heightened risk management standards, including an increased focus on “persistent weaknesses” (e.g., multiple enforcement actions executed over successive years, failure to adhere to corrective actions), “repeat offenses” (e.g., violations of terms or conditions in formal court or agency orders, “insufficient” progress toward correcting deficiencies or violations), and the belief select firms may be “too big to manage” (e.g., where size and complexity give way to persistent weaknesses and repeat offenses).

The expectations for meeting these heightened standards will be driven through regulatory:

- **Intensity:** Growing supervisory scrutiny of persistent weaknesses focusing on management’s ability to adequately identify and mitigate risks as well as timely remediate/correct supervisory concerns or identified deficiencies, including MRAs and enforcement actions. This will be reflected in:
 - Exam intensity (e.g., faster communication, issues escalation, expected remediation, new triggers).
 - Potential ratings impact and escalating enforcement activity (e.g., consent orders, MOUs, divestitures) based on severity of violations and compliance efforts (e.g., intent, history of violations, duration/ frequency, loss/ harm to consumers, actions taken by other regulators, self-identification, proactive disclosure) (e.g., CFTC Enforcement Advisory).
 - Multiagency focus on curbing “repeat offenders”/ holding firms (and boards and management) accountable for perceived ongoing risk and compliance weaknesses.
- **Scope:** Supervisory and enforcement levels have “shifted up.” Independent of firm size, should be able to demonstrate and sustain “heightened standards” in core safety and soundness principles across governance, risk management, internal controls, and Compliance including Treasury, liquidity, interest rate risks, risk assessments, model risk management, enterprise data management, digitalization, technology, and cybersecurity—and all three lines of defense (e.g., OCC Heightened Standards, FRB Enhanced Prudential Standards).

Source: **KPMG Regulatory Insights**

Risk Standards



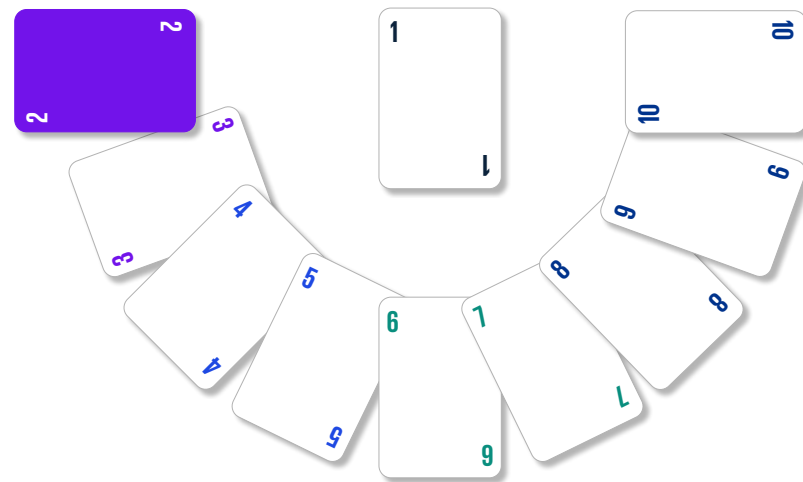
Financial and nonfinancial stability

Events in early 2023 demonstrated the importance of managing stability in the financial system, including mitigating contagion risk, improving resiliency, and preventing financial disruptions through supervision and regulation. Working together through the FSOC, financial services regulators will finalize an analytic framework designed to identify, assess, and mitigate stability risks (from activities, firms, or otherwise) with the goal of reducing the risk of adverse events, or “shocks”, to the financial system, inclusive of bank and nonbank financial companies (e.g., fintechs, insurers, funds).

- **‘Mitigating Shocks’:** Regulators, acting individually and collectively through the FSOC, will focus on mitigating the risk of shocks to the financial systems by:
 - Identifying risks, both financial and nonfinancial, through broad risk monitoring (including the increasing use of digital technology/automation, new or evolving products or practices, new or novel structures (e.g., partnerships, critical services), and developments that could impact resiliency such as cybersecurity).
 - Assessing vulnerabilities that contribute to risks (e.g., concentrations; interconnectedness; “inadequate” risk management (including appropriate resourcing and “voice” to Risk and Compliance); and operational risk and channels of “transmission” that can spread and amplify the negative effects of a financial stability risk to financial markets or market participants (e.g., exposures, critical function/service).
 - Evaluating identified areas of risk and compliance weakness and the sustainability of planned or completed tools/actions to address them.
 - Responding to potential stability risks through coordination, policy recommendations, new rulemakings, and ‘determinations’ or ‘designations’ of specific financial entities.

Source: **KPMG Regulatory Insights**

Risk Standards



Governance

As heightened attention is directed toward risk management standards, regulators will continue to look to demonstrable evidence of credible challenge and dynamic risk assessment and decisioning from both within and across the board and senior management. As part of these expectations (and as part of supervisory focus and evolving regulatory reporting), regulators will expect increased and formalized documentation, mapping, ownership, and ongoing testing and monitoring of controls. Looking toward 2024, regulators are beginning to include expectations/requirements for board and management governance responsibilities into new regulations, guidance, and enforcement actions:

- **New Regulations:** Provisions in new regulations and guidance that clarify the roles, responsibilities, and expectations for “ownership” of the board and management, including:
 - Oversight, documentation and reporting processes, escalation procedures, domain skills and experience/expertise (e.g., SEC Cyber Rule, SEC Climate Rule), and ongoing testing and monitoring of controls.
 - Incentive-based compensation arrangements to reward compliance commitment, as well as disincentives, such as “clawbacks” for employees engaged in misconduct (e.g., DOJ pilot program, Interagency rule).
 - Evaluating identified areas of risk and compliance weakness and the sustainability of planned or completed tools/actions to address them.
 - Responding to potential stability risks through coordination, policy recommendations, new rulemakings, and ‘determinations’ or ‘designations’ of specific financial entities.
- **Accountability:** Ongoing legislative and regulatory focus on holding board and management accountable.

Source: **KPMG Regulatory Insights**

Risk Standards



What to watch

Supervisory intensity and enforcement around heightened risk standards will center on firms' responsiveness to, and mitigation of, risk and compliance "shocks"; as well as risk accountability and governance. Key regulatory actions to watch will include:

- **Supervision of "Persistent Weaknesses" at Banks**

New OCC policies and procedures outlining supervisory or enforcement actions the agency may take against firms with "continuing, recurring, or increasing deficiencies over a prolonged period" and particularly when the firm has not made "sufficient progress" toward correcting deficiencies. Includes money penalties, remediation plans, and/or growth restrictions, or in certain cases, divestiture, and simplification.

- **Financial Services Supervisory and Regulatory Change**

The Administration and regulators continue to issue suggestions for potential changes to supervision and regulation (e.g., enhanced prudential standards (EPS) for banks, deposit insurance reforms, expectations for risk management and governance, and the intensity of supervisory reviews and exams).

- **Financial Stability and Nonbank Supervision**

A framework used by the FSOC and its member agencies to identify, assess, and respond to financial and nonfinancial stability risks posed by activities, firms, or otherwise, with the goal of reducing the risk of "shocks"; improving resilience, and mitigating vulnerabilities. hold individuals accountable, incentivize compliance, and penalize misconduct, including through compensation clawbacks and financial sanctions.

KPMG Thought Leadership

Regulatory Insights Materials



- [Bank Supervision: OCC "Persistent Weaknesses"](#)
- [Bank Supervision and Regulatory Change](#)
- [Financial Stability, Nonbank Supervision: FSOC Proposals](#)
- [DOJ Initiatives on Compensation, Voluntary Self-Disclosure](#)
- [Expanded Risk Governance and Management: FDIC Proposed Guidelines](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



Risk Standards



Call to action...

- **Demonstrate and sustain “Heightened Standards”:** Be able to both demonstrate and sustain the elements of “Heightened Standards”—regardless of size and complexity.
- **Strengthen risk assessment methodologies:** Strengthen the risk assessment and control methodology to ensure proactive identification of new and emerging risks, processes to capture risks within business lines, documentation of controls effectiveness throughout end-to-end business processes, first line ownership of risk assessment and controls process, the role of independent challenge/review, and remediation measures to address identified controls deficiencies in a sustainable manner.
- **Review control testing coverage:** Review supervision and control testing coverage with an eye to increasing coverage as needed. Invest in automation, analytics, and process improvements (including enhanced methodologies) to better identify potential risks.
- **Clarify the role of the board:** Clarify that it is the role of the board to ensure compliance with enforcement actions within required timeframes: hold management accountable; direct management to take corrective actions; approve necessary changes to policies, processes, procedures, and controls; establish processes to monitor and validate corrective actions.
- **Position, scale, and reward risk management:** Appropriately position, scale, and reward risk management and compliance; hold individuals accountable, incentivize compliance, and penalize misconduct, including through compensation clawbacks and financial sanctions.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Financial Services Risk, Regulatory, and Compliance](#)

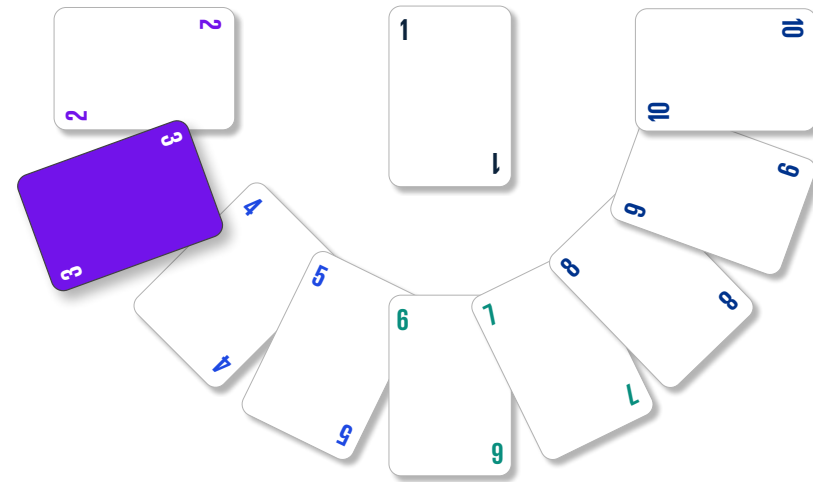
[Regulatory and compliance transformation](#)

Contacts

Todd Semanco
Partner
tsemanco@kpmg.com

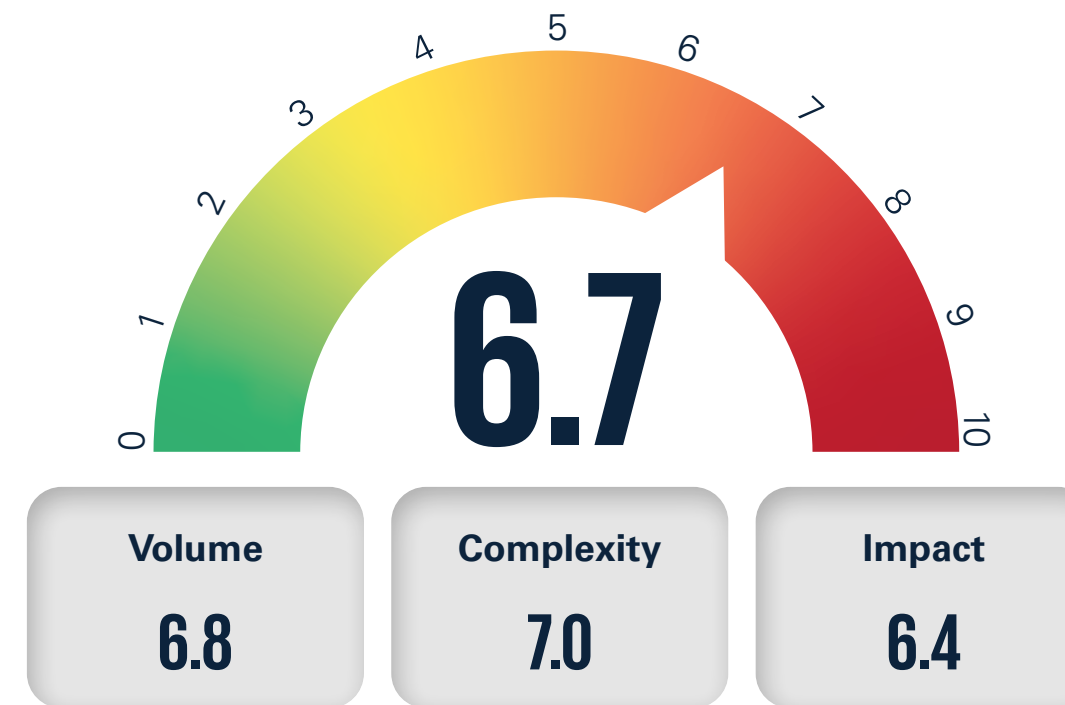
Laura Bray
Principal
laurabray@kpmg.com

Risk Sustainability



Demonstrating “sustainability” in Risk functions will transcend across regulatory areas, requiring it to be embedded across risk pillars and into financial analysis and business as usual.

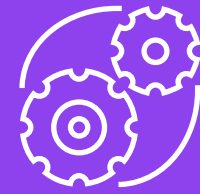
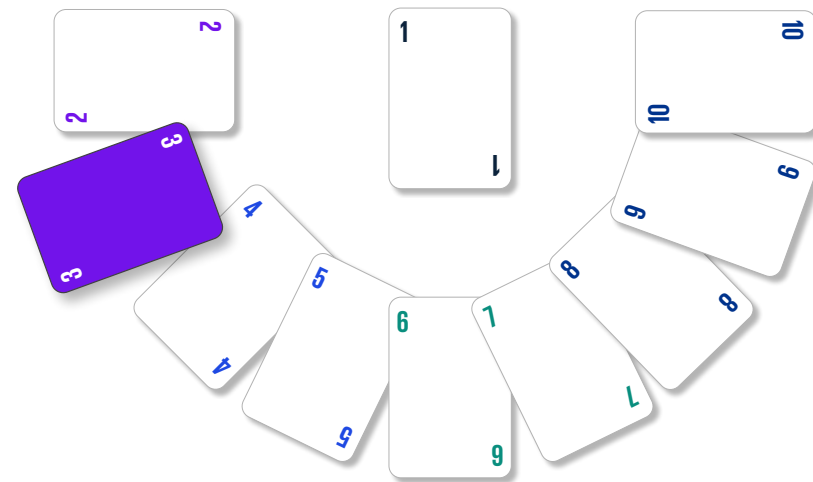
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: KPMG Regulatory Insights

Risk Sustainability



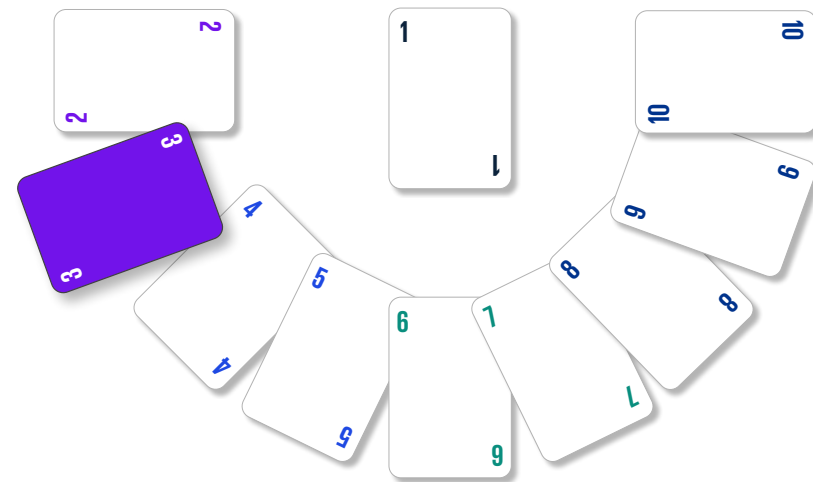
Proving sustainable processes

Regulators will expect evidence of the sustainability of risk management and governance processes, including the ability to address current and emerging risks, adequacy of resources (e.g., technology investment, skilled staffing), and a commitment to ethics and compliance. Firms will need to demonstrate:

- **Risk Culture:** Credible firm culture and values (e.g., rewards for compliant behaviors and accountability, deterrents for misconduct), as well as a sound approach to assessing and monitoring risk culture.
- **Risk Quantification and Integration:** Abilities to ‘quantify risks previously qualitative’, as well as link (in a dynamic/integrated way) to risk monitoring, “outside-in” analyses (e.g., industry enforcement, negative news), and issues management.
- **Business Changes:** Evidence of sustainable processes and effective risk coverage, including metric-driven capacity models to determine resource needs during times of cost containment, growth, or changes in business and parallel run exercises for new model/tech adoption.

Source: **KPMG Regulatory Insights**

Risk Sustainability



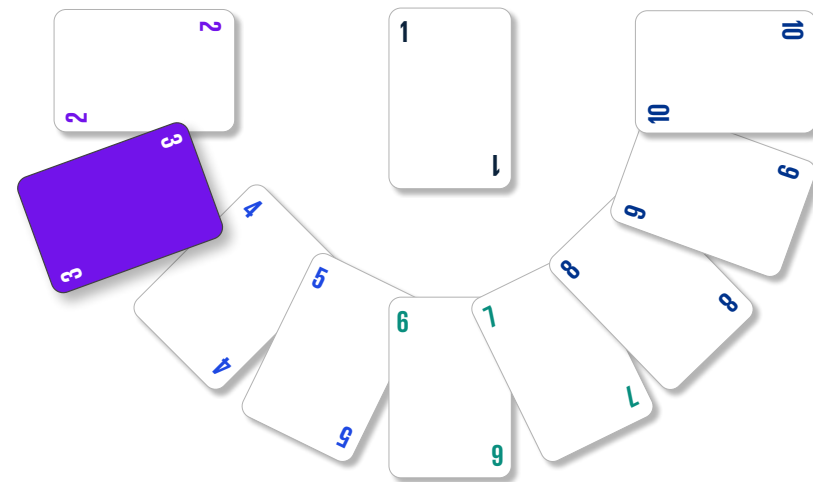
Issues and remediation

Regulators will continue to evaluate firms' management and remediation of issues, including their issues identification processes, adequacy and robustness of risk assessments, and associated actions, as well as effective challenge to issues management. In 2024, firms should expect regulators to focus on the following aspects of these areas:

- **Issues Management:** Scrutiny will focus on:
 - The degree of issues self-identified by the business line as well as by the 2nd and 3rd lines, including the associated timing to size, mitigate, and resolve the issues.
 - Deficiencies in data or reporting (e.g., data quality, timeliness, accuracy, board and management reporting) are quickly identified and appropriately remediated.
- **Risk Assessment:** Regulators will expect adequate and robust analysis of complaints, disputes, and claims information for systemic issues, as well as demonstration of actions taken based on the risk assessments (e.g., modification of products/services, enhancement of process controls, and clarifications to product terms or disclosures).
- **Effective Challenge:** Regulators will likewise look for:
 - A continuous "loop" from issues management to risk assessment (inherent and residual)
 - Quality assurance and review processes that demonstrate effective challenge of issues outcomes and remediation.

Source: **KPMG Regulatory Insights**

Risk Sustainability



Climate sustainability risk

At the federal, state, and global levels, regulators (banking, capital markets, and insurance) continue to push forward with supervision of climate-related financial risk management and to put forth new rules and guidance, increasing the risk of divergence (e.g., federal vs state, federal vs global, state vs state) and challenging firms as they look to set sustainability priorities and/or execute on their commitments and transition plans. As the regulatory landscape evolves, regulators will be assessing:

- **Risk Management and Governance:** Physical and transition risks will drive regulators to scrutinize:
 - Processes for assessing, identifying, and managing emerging and material climate-related risks.
 - Policies, procedures, and limits that reflect changing risk characteristics or firm activities.
 - Strategic planning, board oversight, and management’s effectiveness, including roles, responsibilities, and applicable acumen or experience/expertise.
 - Data, risk metrics, and modeling methodologies, including quantitative climate scenario analysis (such as outlined in the FRB Pilot Scenario Analysis) with clear objectives reflective of overall climate risk management strategy and adequate oversight, validation, and quality control standards.
- **Reporting:** Climate risk information should be integrated with internal reporting, monitoring, and escalation processes, as well as effective risk data aggregation and external and regulatory reporting capabilities. The scope of reporting and disclosures may include:
 - Strategy.
 - Risk management.
 - Governance.
 - Scenario analysis.
 - GHG emissions (Scopes 1, 2, 3).

Regulators will assess the accuracy and alignment of a firm’s reporting with its public statements, commitments, strategy, and products/services marketing (e.g., attention to risk of “greenwashing,” following through on commitments (including net zero), and tracking through transition plans).

Source: **KPMG Regulatory Insights**

Risk Sustainability



What to watch

Regulators are increasingly assessing the “sustainability” of firms’ internal culture and processes, issues management and remediation, and most visibly, climate-related sustainability risks. Key regulatory actions to watch will include:

- **Supervision of “Persistent Weaknesses” at Banks:** New OCC policies and procedures outlining supervisory or enforcement actions the agency may take against firms with “continuing, recurring, or increasing deficiencies over a prolonged period” and particularly when the firm has not made “sufficient progress” toward correcting deficiencies. Includes money penalties, remediation plans, and/or growth restrictions, or in certain cases, divestiture, and simplification.
- **Climate Risk Disclosures:** SEC climate risk disclosure rules for public companies, covering climate risk management, strategy, governance, and certain metrics related to financial statements and greenhouse gas (GHG) emissions. The rules are subject to wide-ranging debate and legal challenges are anticipated.
- **Climate Scenario Analysis and Risk Management:** A climate scenario analysis exercise, looking at multiple scenarios within physical and transition risk modules, conducted by the FRB throughout 2023 to help FRB “learn about large banking organizations’ climate risk management practices and challenges, and to enhance the ability of large banking organizations and supervisors to identify, measure, monitor, and manage these risks.”
- **Final Principles for Climate-Related Financial Risk Management:** Interagency guidance for large banks to identify, measure, monitor, and control climate-related financial risks. Identifies six principles and six specific risk areas.

KPMG Thought Leadership

Regulatory Insights Materials



- [Final Interagency Principles for Climate-Related Financial Risk Management](#)
- [Climate Risk: FRB’s Pilot Scenario Analysis and Risk Management Practices](#)
- [Climate Risk: SEC’s Mandatory Climate Disclosures Proposal](#)

[Implementing tech and data-driven compliance: Forward focus for ethics and compliance](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



Risk Sustainability



Call to action...

- **Establish accountability across lines of defense:** Hold each of the three lines of defense accountable for managing risk; investigate weaknesses in one line to possible weaknesses in the other two; voluntarily and timely self-disclose identified weaknesses and violations of laws and regulations; cooperate with investigations.
- **Ensure consistency in reporting and disclosures:** Adopt a uniform approach to both mandatory and voluntary reporting and disclosures; maintain transparency, accuracy, and consistency with actual strategies and activities across all reporting (financial and nonfinancial) and public-facing statements and/or disclosures.
- **Operationalize sustainability and climate:** Embed climate-related risks within the organization's broader risk governance and risk management frameworks. Develop and implement robust processes for identifying, assessing, managing, and monitoring climate-related risks across all business areas and risk pillars.
- **Reassess your risk culture:** Establish an effective compliance program and foster a culture that deters misconduct and promotes ethics and compliance. Incentivize responsible behavior and involve employees by holding them accountable for the proper use of risk policies and to take ownership of the organization's strategy. Enable employees to do what is required in terms of managing risks by clearly making the risk responses and the effects thereof visible within the organization.
- **Show critical challenge of sustained change:** Integrate critical challenge (e.g., escalation procedures, actions initiated, decisions made, and proof of altered/terminated paths based on risk determinations) into risk and governance frameworks; document root cause analysis and remediation; automate controls where possible; conduct ongoing monitoring and testing of sustained change.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Enterprise risk management](#)

[Regulatory and Compliance Transformation](#)

[Climate risk and resilience](#)

Contacts

Julie Gerlach

Partner

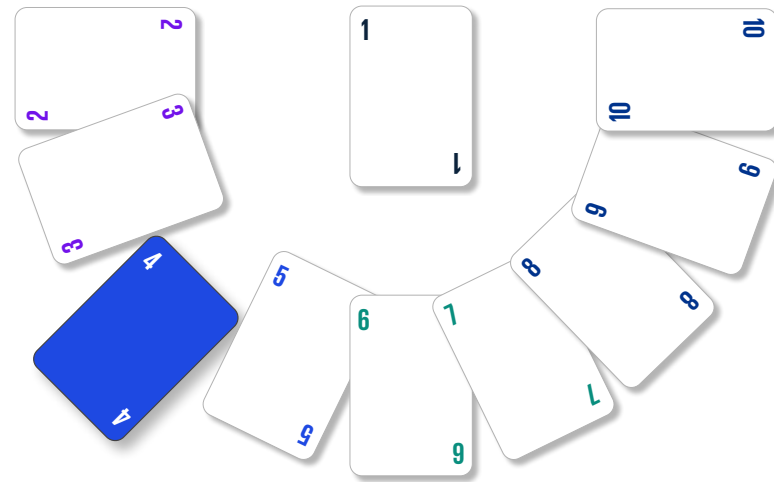
jgerlach@kpmg.com

Ben Harden

Managing Director

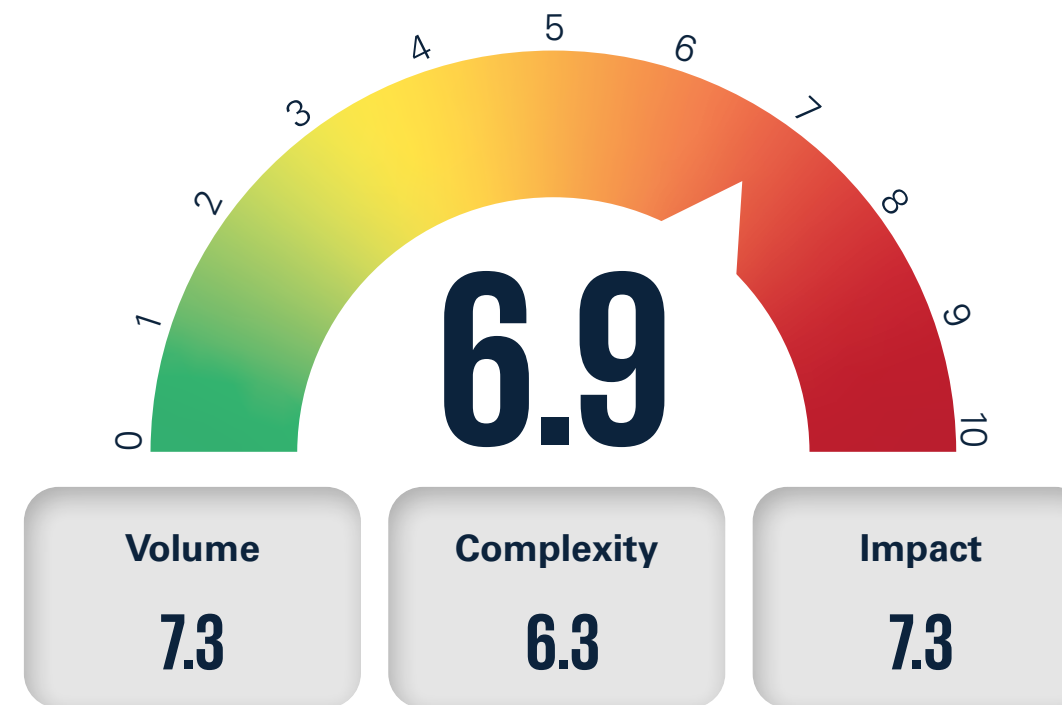
bharden@kpmg.com

Growth & Resiliency



Expanding regulatory scrutiny of “too big to manage” (TBTM), including firms’ ability for M&A activity or portfolio growth in the context of sound liquidity management, resolution planning, and demonstration of strong financial controls.

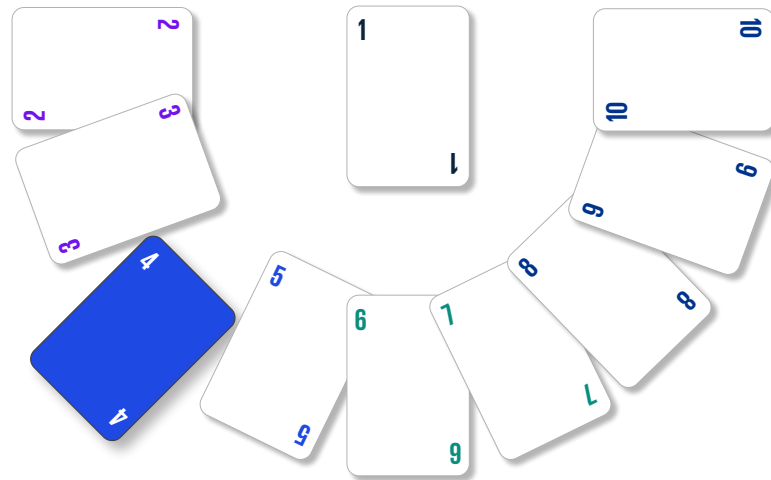
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: **KPMG Regulatory Insights**

Growth & Resiliency



Liquidity

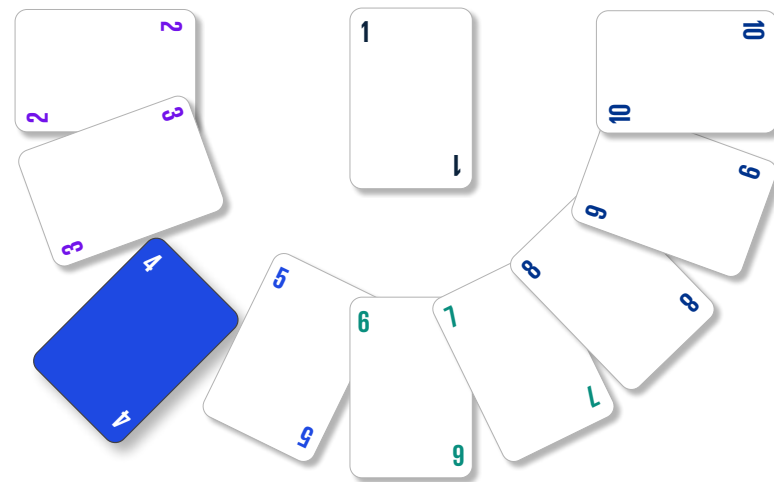
Regulators are responding to frequent changes in the interest rate environment combined with market turmoil in early 2023 by heightening the rigor of supervisory and regulatory reviews related to liquidity risks and effective liquidity risk management for firms in all sectors (banking, capital markets, insurance) and of all sizes.

In 2024, firms should anticipate increasing supervisory attention to:

- **Funding Plans:** Regulators will assess whether firms' contingency funding plans:
 - Are actionable over a range of possible stress scenarios.
 - Provide for stability and a range of funding sources that can be accessed in adverse circumstances.
 - Consider the FRB discount window as a funding source, and if so, whether operational readiness to borrow has been established and maintained.
- **Liquidity Risk Management:** Regulators will increase expectations around:
 - Models (e.g., strength, exposures), uninsured deposits, and held-to-maturity securities.
 - Liquidity management and reporting (e.g., shortened windows for daily and intraday capabilities, expanded information reporting).
 - Long-term debt requirements (including an interagency proposal to expand required holdings of long-term debt to certain banks and holding companies (e.g., \$100+ billion)).
 - Transactions with affiliates (and compliance with Regulation W) impacting capital and liquidity positions.
- **Interest Rate Risk Management:** Ongoing supervisory focus on interest rate risk management amid a changing interest rate environment, credit tightening, and quality and concentration risks, including stress testing and scenario analysis.

Source: **KPMG Regulatory Insights**

Growth & Resiliency



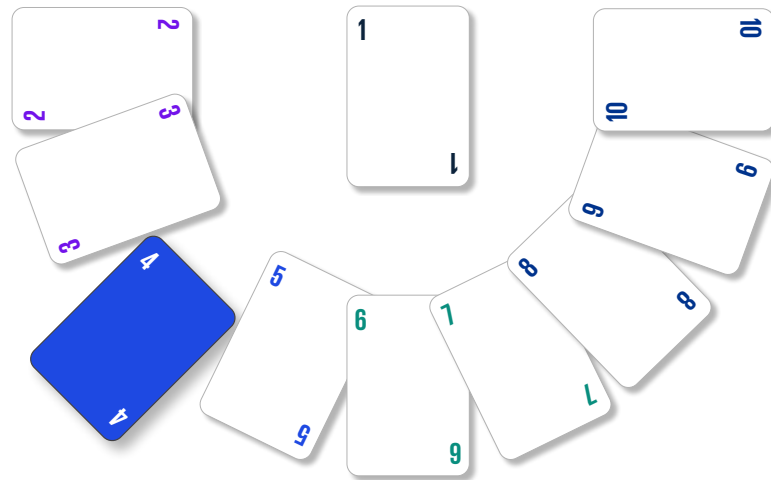
Resolutions

Along with heightened attention to liquidity risks, multiple regulators are revisiting/enhancing expectations for the preparation and submission of resolution plans, especially among larger firms, with an eye towards effecting more orderly resolutions. Supervisory and regulatory attention will continue to focus on:

- **Planning:** Multiple regulators will expand expectations to require more firms under their supervisory authority (e.g., \$50+ billion banks, Category II and III banking organizations, SEC-registered clearing agencies) to engage formal, detailed resolution planning and plan submissions (i.e., inclusive of the planning process, execution strategy, and consideration of areas of “potential vulnerability” to resolvability).
- **Bridging:** Banking regulators will focus on operational resiliency bridge planning, including the strategy for formation and stabilization of the bridge depository institution, as well as how operations could continue through resolution or separation from parent and/or affiliates and any associated activities.

Source: **KPMG Regulatory Insights**

Growth & Resiliency



Too Big to Manage

As large firms, especially banking organizations, continue to grow, both organically and through M&A activities, regulators are saying it is increasingly difficult to affect an orderly resolution owing in part to their large size as well as to complexities associated with their operations, assets, liabilities, and services which fall outside of the core business chain. Regulators also suggest that it is this size and complexity that can lead to “persistent weaknesses,” “repeat offenses,” and supervisory action (See 02—Risk Standards) as “effective management is not infinitely scalable.”

Firms should anticipate that regulators will be considering:

- **M&A:** Continuing scrutiny of anticompetitive M&A activity, as well as a potentially expanded scope of bank merger reviews (e.g., to include nonbank entities such as fintechs) and more timely reviews (e.g., shortened timeframes). Deal activity in 2024 will be dictated largely by macroeconomic conditions, including interest rates and inflation and tight lending standards, in both banking and capital markets.
- **Tech and Operational Resiliency:** Evolving and growing focus on elements of tech and operational resiliency, including deployment of new technologies (e.g., automated systems, predictive analytics, cloud); data governance (e.g., privacy, use, sharing); identification of critical operations/core business lines/material entities and business continuity planning; threat detection/risk monitoring including third party relationships; concentrations and interdependencies; accountability (e.g., roles, responsibilities, escalation protocols).
- **Examination Scrutiny:** Deficiencies identified by regulators, coupled with perceived repeat offenses or failures to remediate them, will drive close examination of the size and complexity of firms and evaluation of whether management has reached its “limits.”
- **Remediation:** Consideration and prescription of escalating options for “remediation” of supervisory concerns and identified deficiencies (e.g., enforcement actions, changing management, implementing action plans, imposing fines, capping growth, divesting business lines/activities) with the intent of simplifying and “meaningfully changing business incentives.”

Source: **KPMG Regulatory Insights**

Growth & Resiliency



What to watch

Regulatory actions to watch in 2024 will include:

- **Long-Term Debt Requirements:** Interagency (FRB, FDIC, OCC) proposal to impose long-term debt requirements on certain large banks and holding companies with assets of \$100+ billion; perceived benefits include improved resolvability, reduced costs to the Deposit Insurance Fund, and mitigated financial stability and contagion risks.
- **Resolutions and Living Wills:** FDIC rule proposal requiring banks with assets of \$50+ billion to periodically submit resolution plans, and joint FDIC/FRB guidance proposal on the development of resolution plans for Category II and III banking organizations (\$250+ billion).
- **Merger Review:** Ongoing developments to DOJ/FTC Merger Guidelines and bank regulator consideration of updates to the Bank Merger Policy.
- **Resilience:** Evolving regulatory expectations for third parties providing “critical activities” to financial services firms (e.g., cloud services, IT support), including evolving focus on resilience risk standards and testing tools (e.g., resilience, scenario, cyber).

KPMG Thought Leadership

Regulatory Insights Materials



- [Clearing Agency Risk Management and “Living Wills”](#)
- [Financial Stability, Nonbank Supervision: FSOC Proposals](#)
- [FDIC Deposit Insurance Reform Options](#)
- [Bank Supervision and Regulatory Change](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



Growth & Resiliency



Call to action...

- **Strengthen risk management and governance:**

- Review and optimize capital requirements, including consideration of unrealized gains and losses on available for sale securities.
- Review and update resolution and recovery plans, including consideration of personnel and retention plans, critical third-party and shared services, payments and trading activities, and communications systems; franchise components for separation or sale.
- Improve governance processes, such as board and senior management reporting, skill sets, incentive compensation, and responsiveness to supervisory direction.

- **Prepare for increased supervisory reviews and examinations:** Anticipate and adapt to increased regulatory reporting frequency and level of detail. Address identified issues and monitor progress against plans proactively and efficiently. Evaluate potential impacts of alternative deposit insurance options (limited coverage, unlimited coverage, and targeted coverage) on the company's risk profile and operations.

- **Evaluate and adjust to financial stability risks:** Analyze the impact of potential financial and nonfinancial risks and vulnerabilities that may contribute to these risks. Implement changes as necessary to stay ahead of potential policy approaches or regulatory actions.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Market, Credit, and Liquidity Risk](#)

[Transactions](#)

Contacts

Tim Johnson

Partner

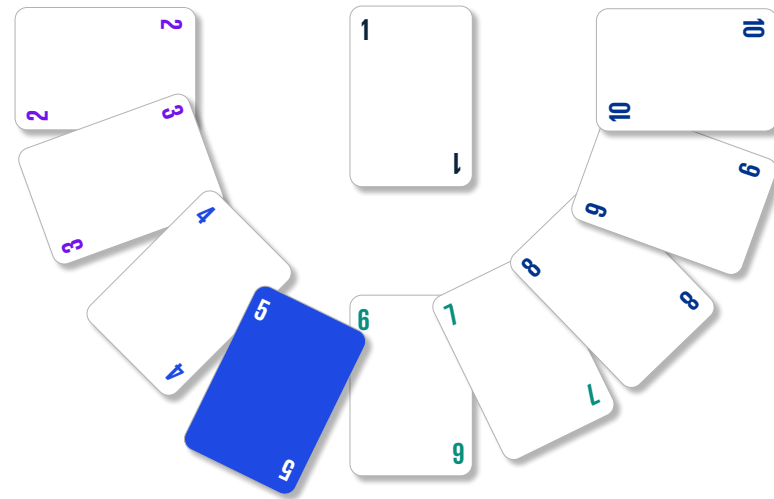
tejohnson@kpmg.com

KB Babar

Managing Director

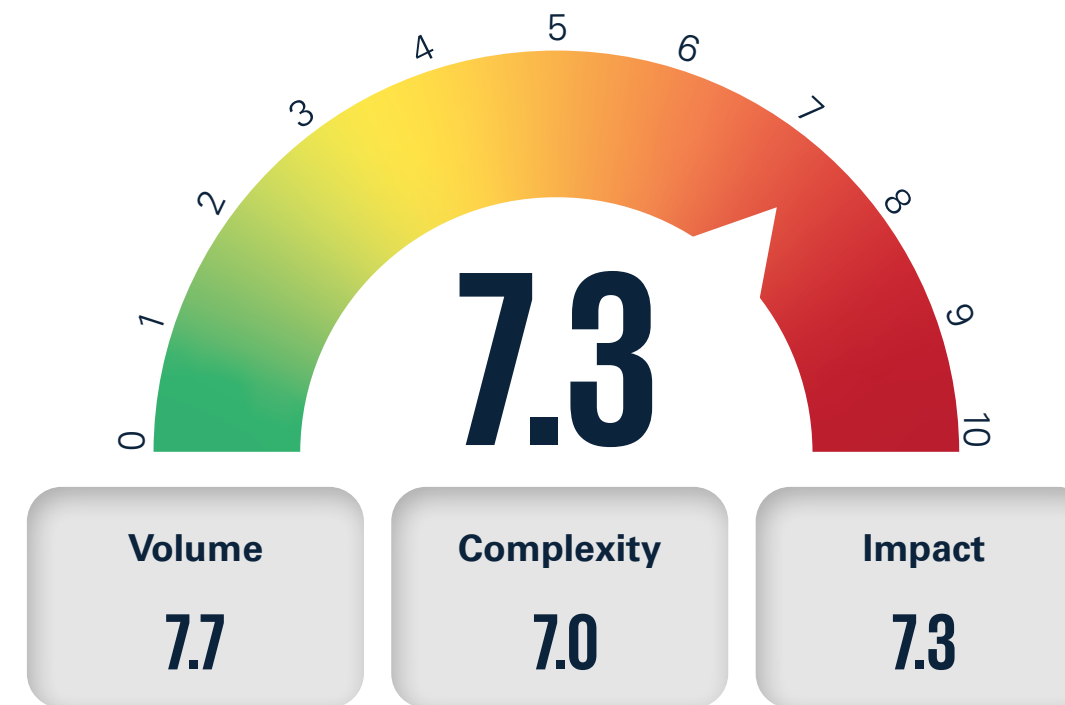
kbabar@kpmg.com

Capital & Valuations



Escalating regulatory attention on risk calculations, stress testing, capital planning, and broad risk management—across financial risks as well as operational risks

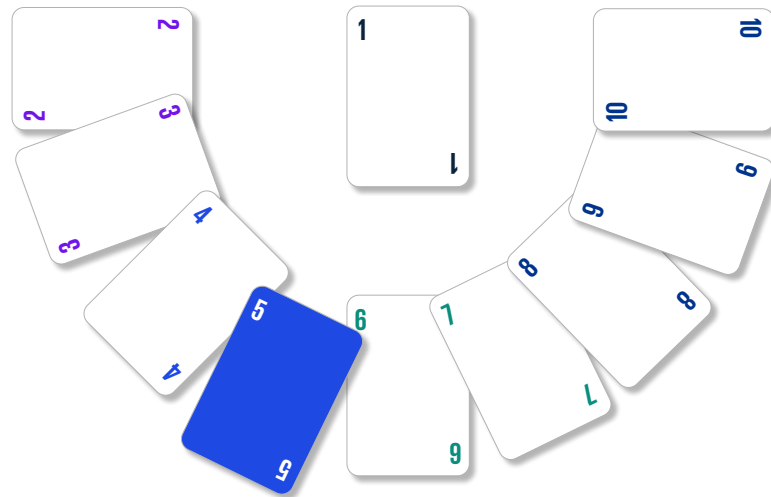
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: KPMG Regulatory Insights

Capital & Valuations



Calculation

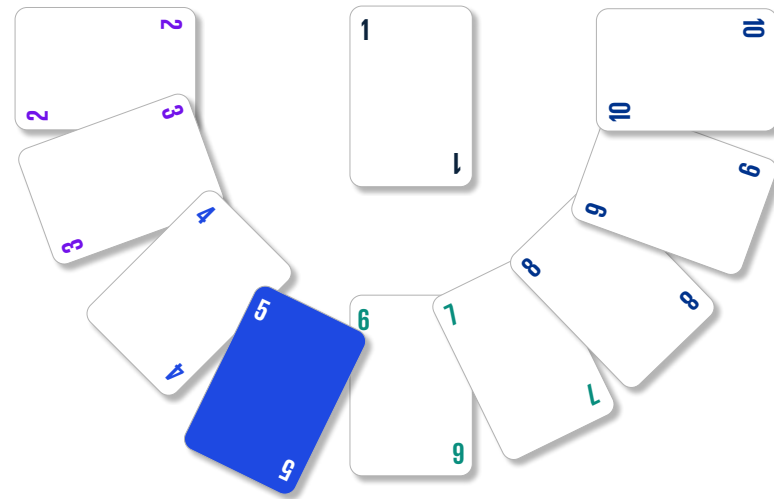
The federal banking regulators (FRB, FDIC, OCC) will jointly seek to increase the strength and resilience of the banking system through changes to the large bank capital requirements (all Category I to IV banking organizations with assets of \$100+ billion), including applying a broader set of capital requirements to more large banks and standardizing certain aspects of the capital framework. The effect of the changes, which would implement the final components of the international capital standards (e.g., the Basel III agreement) in the US as well as markedly change the U.S. “tailoring rules” (e.g., impose more requirements on all Category II, III, and IV banking organizations), is expected to vary for each bank based on its activities and risk profile.

The regulators intend for changes to introduce more transparency, consistency, and risk sensitivity to the measurement of risk-weighted assets. Firms should anticipate regulatory focus across core risk areas (e.g., operational risk, credit risk, market risk) as well as business lines and corporate functions.

- **Risk-Weightings:** Adjustments to risk-weighted capital calculations include:
 - Operational Risk: Standardized approach would use a function of firms’ “business indicator components” and “internal loss multipliers”.
 - Credit Risk: Expanded risk-based approach with increased “risk sensitivity” from additional criteria and metrics for differentiation of credit risk within exposure categories and a broader range of risk weights for various asset classes (e.g., exposures to depository institutions, foreign banks, and credit unions; subordinated debt; real estate, retail, and corporate exposures).
 - Market Risk: Standardized and internal model approaches for calculating risk-weighted assets for market risk; introduces the concept of a trading desk and restricts application of the models-based approach to the trading desk level.
 - Credit Valuation Adjustment Risk: New, standardized approach allows recognizing hedges for expected exposure component of CVA risk.
 - Securitization Exposures and Equity Exposures.
- **Whole of Business:** For all impacted institutions, changes to capital requirements will drive extensive changes in governance processes, data, models, system infrastructure, internal controls, and regulatory reporting, which will span both business lines and corporate functions over a multiyear timeframe. Further, firms (regardless of size) should anticipate that regulators may request information on practices and data that seem to be a “tier up” from current category levels.

Source: **KPMG Regulatory Insights**

Capital & Valuations



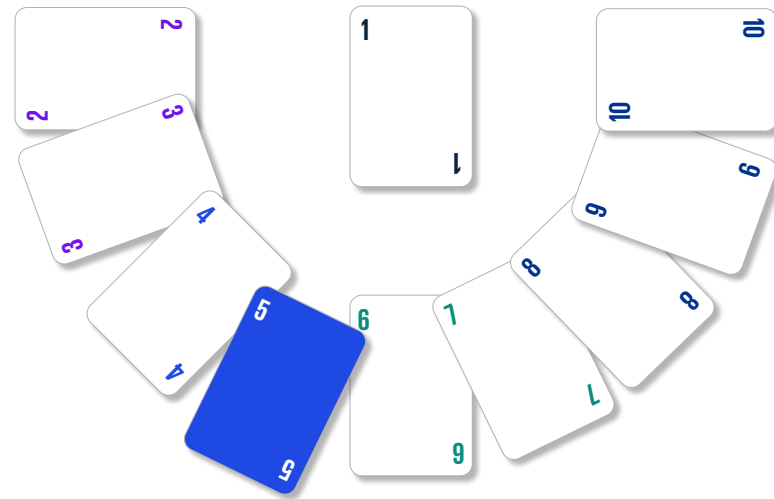
Framework

Changes to the capital requirements will also impact:

- **Stress Testing:** Revised calculations under the proposed “dual-requirement capital structure with output floors” (i.e., a requirement that risk-based capital ratios be calculated under both the “expanded risk-based approach” and the “standardized approach” and the lower of the two be used for each risk-based capital ratio) will drive (re)assessment and (re)alignment of existing stress testing frameworks with the need for additional scenarios, including scenarios that consider the impact of rising rates on asset values, deposit stability, liquidity, and earnings.
- **Capital Planning and Balance Sheet Management:** Capital planning and balance sheet management strategies will evolve based on the new approaches/requirements; expect heightened data requirements, supervisory scrutiny of models, and more granular reporting.
- **Accounting and tax:** Changing capital plans, balance sheet management strategies, and corresponding adjustments will potentially result in changes to accounting and tax calculations (e.g., AOCI, DTA).

Source: **KPMG Regulatory Insights**

Capital & Valuations



Risk management

In combination with economic uncertainties and interest rate pressures, changes to the capital requirements will focus supervisory attention to:

- **Impacts and Metrics:** Evaluation of the impact changed capital requirements would have on portfolios and products, as well as reassessment of risk management metrics and thresholds to align with evolving capital requirements.
- **Unrealized Losses:** Impact of potential new requirements to recognize unrealized losses on available-for-sale securities in regulatory capital and related changes to capital and liquidity risk management programs (see 04 Growth & Resiliency).
- **Credit Vulnerabilities:** Increasing risks (e.g., repricing, default) amidst rising interest rates, tightening of credit terms (e.g., loan size, maturities, collateralization, interest rate floors), and weaknesses in select sectors (e.g., urban commercial real estate—offices, hotels); regulators will look to stress testing and scenario analysis as ways to identify and measure the impact of credit vulnerabilities (e.g., concentrations, highly leveraged borrowers, lower-rated borrowers).
- **Long-Term Debt:** For large banks and BHCs (e.g., \$100+ billion), plans to issue and maintain minimum levels of eligible long-term debt sufficient to absorb losses or to provide capital in a resolution (i.e., as required through an interagency rulemaking).

Source: **KPMG Regulatory Insights**

Capital & Valuations



What to watch

Regulatory attention, based on the proposed capital requirements, will focus on the impacts and implications to firms' business processes, capital and risk calculations, and capital planning and investment strategies.

- **Capital Requirements: Proposed "Basel III Endgame":** Interagency (FRB, FDIC, OCC) proposal to substantially change regulatory capital requirements impacting large banks with \$100+ billion in total assets; the changes would implement final components of the Basel III agreement in the US as well as make changes to the US "tailoring rules."
- **Long-Term Debt Requirements:** Interagency (FRB, FDIC, OCC) proposal to impose long-term debt requirements for certain large banks and holding companies with assets of \$100+ billion.

KPMG Thought Leadership

Regulatory Insights Materials



[Capital Requirements: Proposed "Basel III Endgame" & GSIB Capital Surcharges](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



Capital & Valuations



Call to action...

- **Conduct current-state assessment:** Evaluate the existing governance, data, data quality, models, system infrastructure, internal controls, regulatory reporting, and capital strategies to identify areas where remediation is needed considering the new capital requirements. Assess changes to regulatory reporting and build needed capabilities to include process, system, and technology changes. Start collecting data and perform pro forma RWA impact analyses on banks' portfolios. Identify potential data gaps to support the proposed rules.
- **Establish centralized coordination:** Implement a coordinated approach to drive the various transition efforts across business lines and corporate functions, streamlining the process and ensuring compliance with the proposed rules.
- **Optimize business and investment strategies:** Banks should reconsider their strategies to comply with the new capital requirements—particularly in light of the impacts to various components including credit and operational risks (especially for larger, complex institutions)—paying particular attention to risk-sensitive areas such as high-leverage/private equity exposures, resecuritization, and large trading activities.
- **Prepare implementation and compliance timeline:** Develop a comprehensive multiyear, firmwide plan to achieve compliance with the proposed rules, considering the transition period and the proposed compliance dates. Understand capacity planning to execute changes, specifically for data, analytics and modeling teams, which will be constrained as credit conditions continue to be volatile into 2024.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Market, Credit, and Liquidity Risk](#)

[Risk, Regulatory, and Compliance](#)

Contacts

Adam Levy

Principal

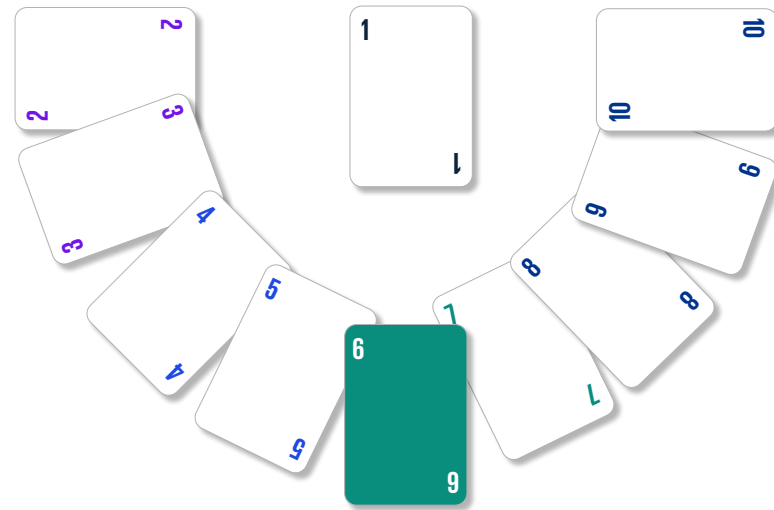
adamlevy@kpmg.com

Jeff Dykstra

Principal

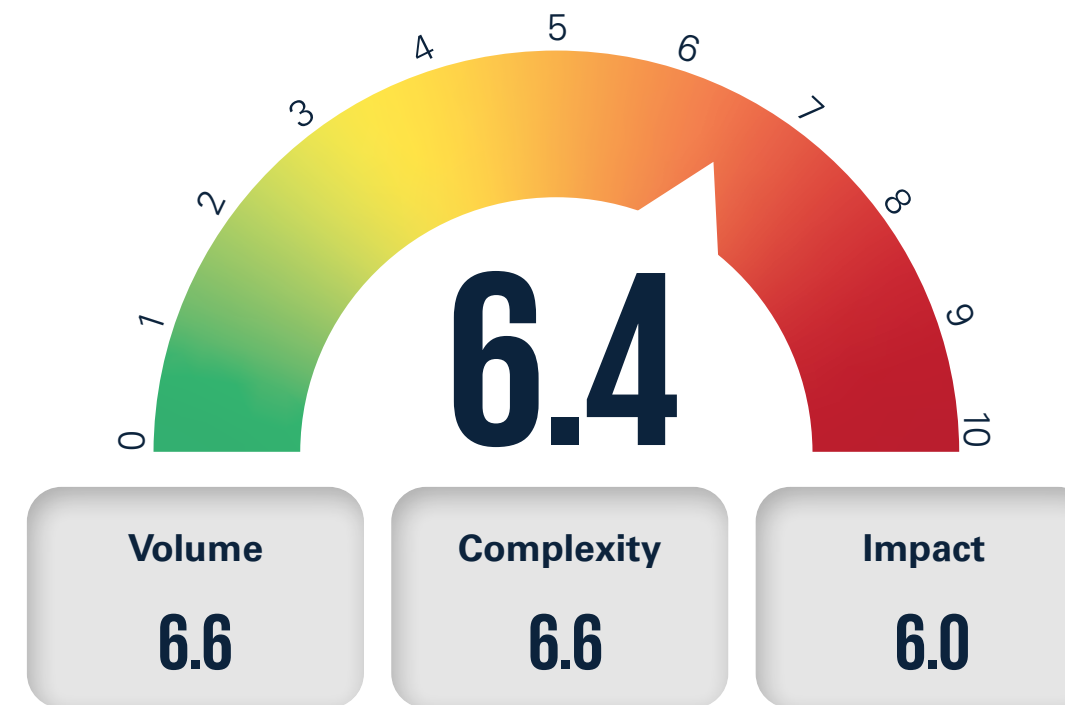
jdykstra@kpmg.com

'Threat Actors'



Expanding regulatory expectations around the detection, mitigation, tracking and remediation of “threat actors”—perpetrators of financial crime, fraud, and misconduct—all while maintaining consumer protections

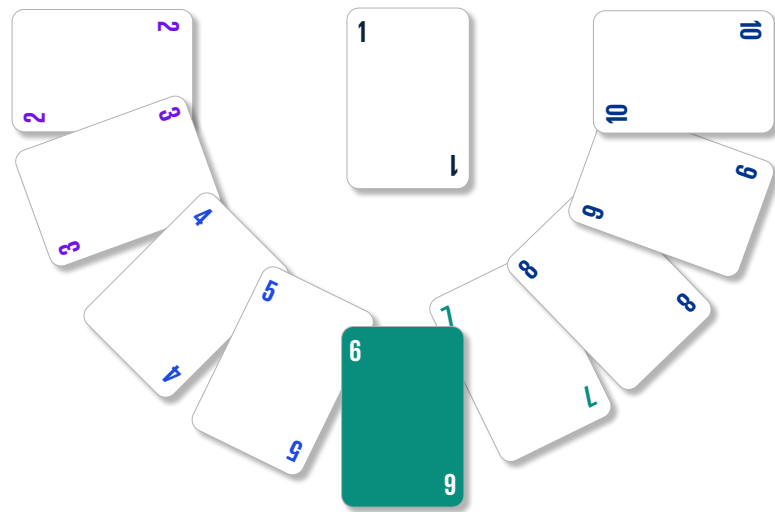
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: KPMG Regulatory Insights

'Threat Actors'



Financial crime

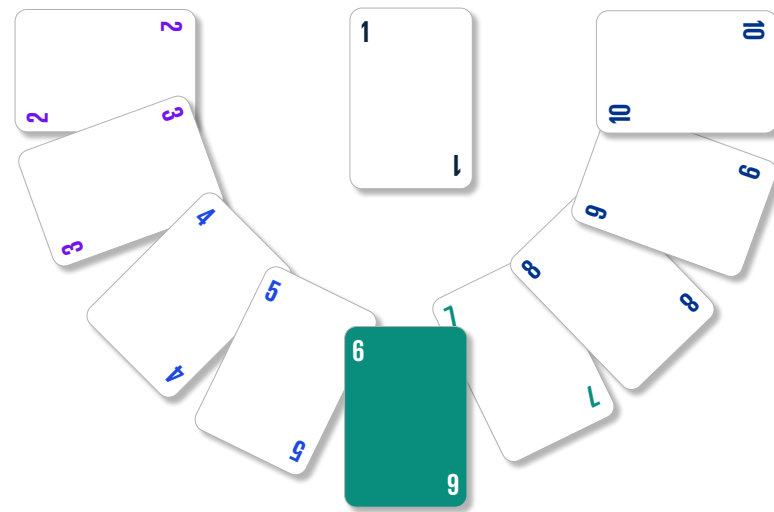
Technological developments, geopolitical events, and evolving interconnections and interdependencies in financial networks can increase financial crime risks, exposures, and complexities. Regulators will continue to be vigilant in supervising and examining firms' defenses against financial crimes, such as terrorist financing, money laundering, beneficial ownership, sanctions or tax evasion, trafficking (e.g., drug, human), cybercrime, and potential compliance violations.

As part of these efforts in 2024, regulators will scrutinize:

- **Data Traceability:** Abilities to demonstrate, and report on, the traceability of data at both the customer and transaction level, as well as across business processes, systems of record, and systems of origin.
- **Transaction Monitoring:** The quality of transaction monitoring and surveillance systems, processes, and controls, with expectations for increased accuracy and consistency, as well as better and more efficient outcomes via automation. Regulatory focus in areas such as BSA/AML/CFT, trading activity, and KYC/CDD and beneficial ownership monitoring will continue along with attention to preparations for implementing risk-based compliance programs in these priority areas.
- **Expanded Threats:** The adequacy and continual improvement of threat detection, monitoring, and response capabilities, including the reliability of processes (e.g., due diligence, access, safeguards) and coverage of novel and emerging threats and vulnerabilities (e.g., virtual currencies, sanctions evasion, malware/ransomware, human rights/forced labor, organized crime).

Source: **KPMG Regulatory Insights**

'Threat Actors'



Fraud

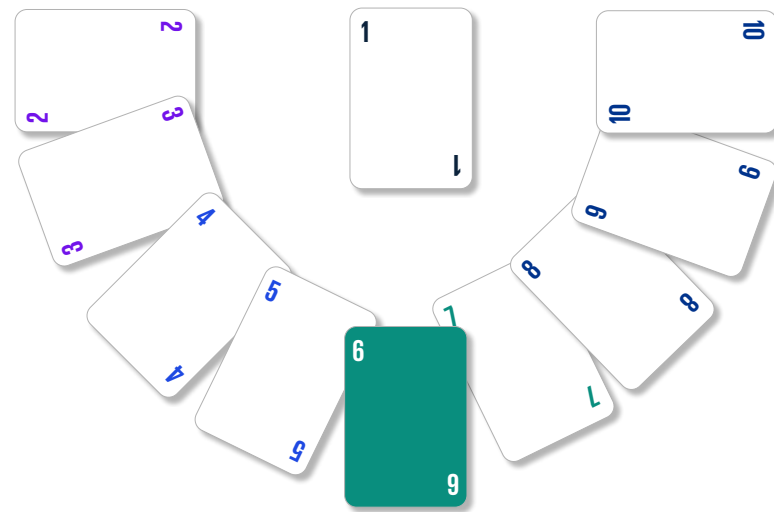
Regulators report that the costs to consumers and firms from fraud, identity theft, and other “scams” are increasing. Similar to financial crime, technological advancements (e.g., automated systems, crypto and digital assets, digitalization) and developing interconnections and interdependencies will drive regulators to continue to evaluate safeguards against fraud and other scams and consumer protections.

Expect regulators to focus on:

- **Safeguards:** Risk and fraud model management and controls related to existing and new products, services, customers, and geographic operations, including consumer protections from fraud, identity theft, and other scams.
- **Consumer Treatment:** Fair processing and treatment of consumer complaints, claims, and disputes within the fraud and investigation processes, as well as the clarity of consumer communications. Areas of focus will include data sharing (e.g., large data models, data sharing with third parties and affiliates, customer permissioned sharing), payments authentication procedures (e.g., P2P), model development and validation, account holds and freezes, and ongoing oversight and monitoring of synthetic identity fraud.
- **Crypto & Digital Assets:** Continued investigations and enforcement of non-compliance with existing regulations (e.g., unregistered offerings or sales of crypto asset securities or derivatives products, false statements, market manipulation, red flag indicators).

Source: **KPMG Regulatory Insights**

'Threat Actors'



Misconduct

Regulators are similarly giving heightened attention to conduct risk and ethical business practices; regulators view conduct risk as connected to risk culture and to the integrity and reliability of reporting, marketing/advertising, and customer interactions, which are essential to building trust.

As part of their role to safeguard public trust and confidence in the financial services industry, expect regulators to focus on:

- **Threat Detection and Monitoring:** The presence of:
 - Continual process improvement to identify, adapt, monitor, and respond to changing tactics from threat actors, as well as to timely remediate issues, as necessary.
 - Mature insider risk programs, inclusive of behavioral models and scenario analysis, to reduce the likelihood of insider corruption and financial crime risk (e.g., authentication/access management, synthetic identity fraud).
 - Surveillance programs to monitor use of digital devices, third-party messaging platforms, and e-communication social tools.
- **Compliance Culture:** A culture of compliance and “individual accountability,” including incentives for ethical behavior and culture commitment (e.g., cooperation with supervisors, proactive identification of misconduct, self-disclosure, timely remediation), disincentives for misconduct (e.g., compensation “clawbacks”), and business practices that place the interest of customers first (e.g., avoidance/disclosure of conflicts of interest).

Source: **KPMG Regulatory Insights**

'Threat Actors'



What to watch

Key regulatory actions to watch related to fraud, financial crime, and misconduct, include:

- **AML Supervision and Enforcement:** Regulators identify BSA/AML/CFT compliance, CDD, and beneficial ownership as key areas of examination focus; the importance of AML program examinations is elevated due to the geopolitical environment and sanctions activity. Intensifying supervision and enforcement may include data traceability, transaction monitoring, suspicious activity reporting, independent reviews, and employee training.
- **FinCEN Supervision and Examination Priorities:** Forthcoming FinCEN rules requiring financial institutions to carry out risk-based programs for government-wide AML and CFT priorities. Pending Corporate Transparency Act regulations (including the beneficial ownership information reporting rule, related safeguards and access rule, and anticipated revisions to CDD Rule requirements).
- **"Covered Technologies" and Conflicts of Interest:** SEC proposal "to eliminate conflicts of interest associated with interactions with investors [e.g., correspondence, online, advertising] through the use of technologies [e.g., predictive analytics, AI, ML] that optimize for, predict, guide, forecast, or direct, investment-related behaviors or outcomes."
- **Regulatory "Trust":** Growing expectation for ongoing collaboration, adaptability, and communication among financial industry participants and regulators to strengthen public "trust" in the financial services industry.

KPMG Thought Leadership

Regulatory Insights Materials



- [AML Enforcement: SEC Risk Alert & FFIEC Exam Manual Updates](#)
- [2023 Regulatory Agendas: Federal Banking Regulators](#)
- [Fraud, Identity Theft, and Other Scams](#)
- [SEC Beneficial Ownership Reporting Amendments](#)
- [DOJ Initiatives on Compensation, Voluntary Self-Disclosure](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



'Threat Actors'



Call to action...

- **Enhance technology and analytics:** Assess/pilot/adopt innovative approaches (e.g., AI/GenAI, enhanced data analytics) to enhance fraud and financial crime risk management and augment or potentially replace legacy systems. Establish associated parallel testing processes and robust governance structures.
- **Strengthen client onboarding:** Implement analytics and automation in client onboarding processes and strengthen processes to gather, store, report, and monitor KYC information, including beneficial ownership, as appropriate.
- **Develop a mature insider risk program:** Promote a culture of compliance through ongoing communication, consistent enforcement of consequences for violations, and clear behavioral expectations. Implement tailored training and awareness programs for all personnel. Leverage technical tools and advanced analytics to monitor behavior and human input to identify anomalous insider behavior.
- **Mitigate synthetic identity fraud (SIF):** Deploy a multilayered approach, including manual and technological data analysis, for SIF risk assessment. Utilize additional data sources beyond basic personally identifiable information (PII). Implement robust link analysis processes to monitor transactions, entities.
- **Strengthen security:** Establish robust authentication and access protocols for real-time and faster payments to minimize account takeover and social engineering risks. Enhance controls around regulatory focus areas, such as malware, phishing, credential stuffing, and identify theft.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Financial crimes](#)

[Forensic](#)

[Financial Services Risk, Regulatory, and Compliance](#)

Contacts

Chad Polen

Partner

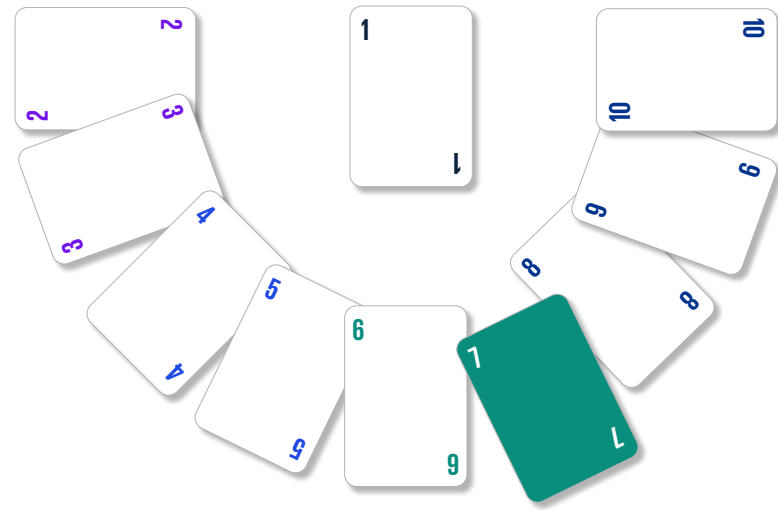
cpolen@kpmg.com

John Caruso

Principal

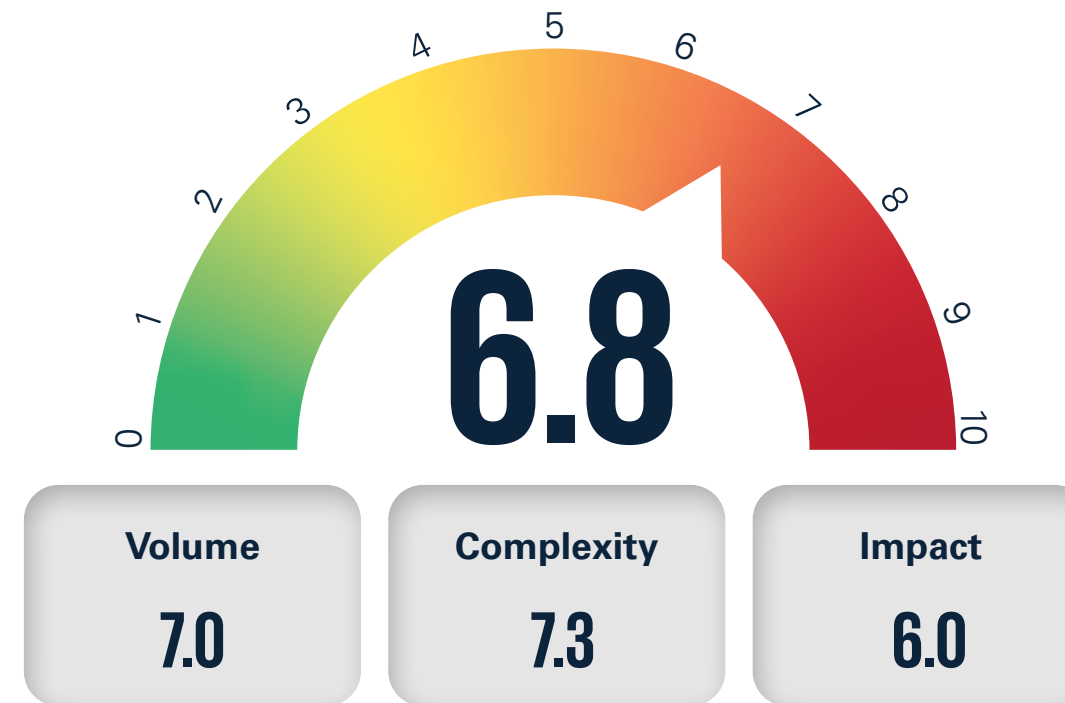
johncaruso@kpmg.com

Fairness



Multiagency focus on fairness principles, including access, treatment, and product risks—“Say what you do, do what you say.”

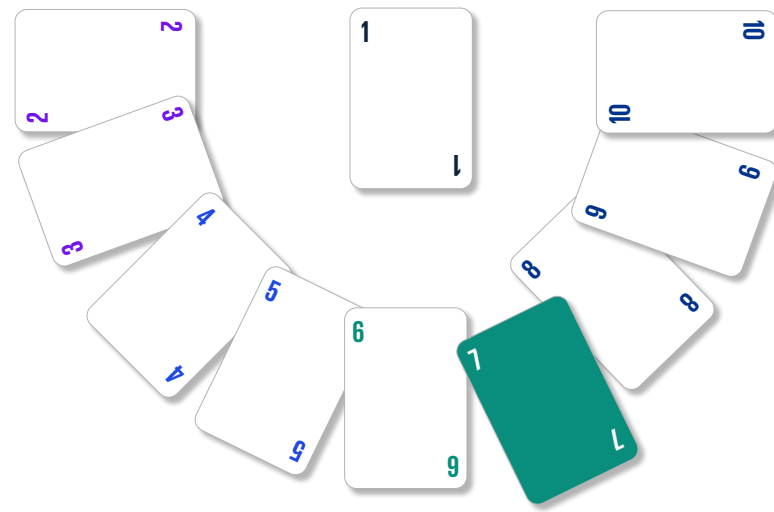
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: KPMG Regulatory Insights

Fairness



Fairness

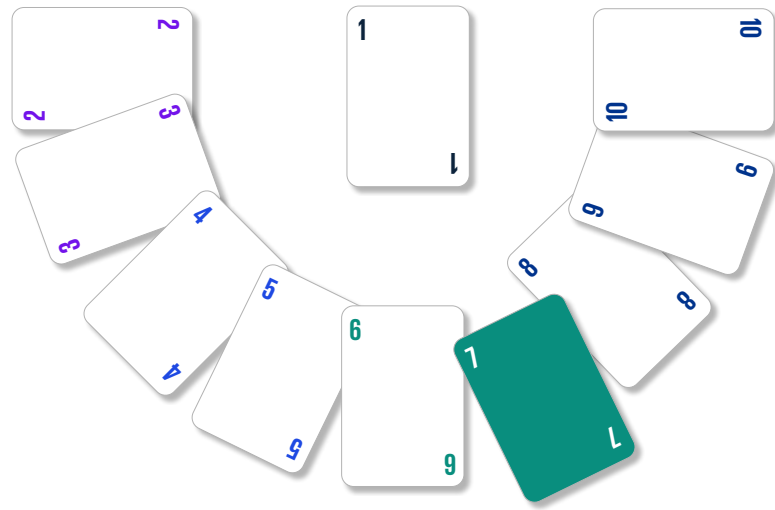
Banking, capital markets, and insurance regulators will continue to assess the fairness of financial market products and services over the “customer journey,” including development, marketing, sales, servicing, and complaints/claims management. Consumer and investor protections will look to “unfairness” and marketing claims to fulfillment, under both new and existing regulations. Supervisory intensity will be applied to increases in model usage (including data permissibility) and bias outcomes.

Fairness and potential breaches to customer trust will be driven through:

- **Supervision and Enforcement:** Fairness will continue to be examined throughout the customer journey and across products and services (e.g., auto loans, servicing, payments, deposits, advertising, sales, and data and privacy practices), as well as underlying decision-making processes, including the use of “automated systems” (e.g., models, algorithms, programs, AI/ML) and related marketing/advertising. Fairness should also be factored into a firm’s operations through dynamic and ongoing risk assessment processes, monitoring, testing and data analyses.
- **Regulatory Expansion:** Despite potential court challenges on regulatory authority, regulators will continue to apply an expanded lens of fairness to existing regulations (e.g., UDAAP/UDAP). Expect revisions to existing regulations and guidance (e.g., CRA, merger and antitrust reviews, and conflicts of interest) and new regulations to include fairness considerations. And while legal challenges could potentially extend implementation timelines for certain new rules and proposals (e.g., CFPB’s 1071 small business lending rule), regulators will expect the industry to continue preparedness and implementation planning.

Source: **KPMG Regulatory Insights**

Fairness



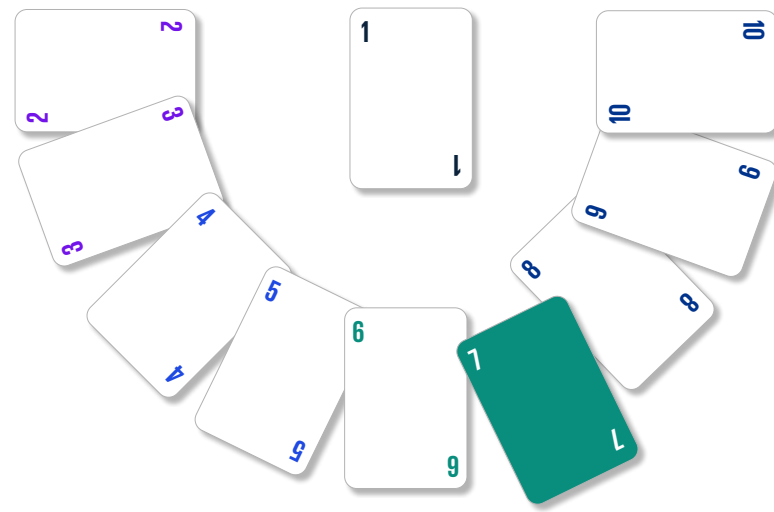
Access/Treatment

Through rulemakings, regulators will look to improve transparency, access, and treatment for consumers and investors. Example areas of regulatory focus will include:

- **Market Structure Changes:** Anticipated changes to the retail trading market structure aim to reduce “inefficiencies” that may disproportionately impact retail investors. The changes promote transparency and market competition through new Best Execution standards, expanded order execution disclosure, “improvements” to certain pricing and fees, and increased order competition.
- **Fair Treatment:** Regulatory focus on complaints, claims, and fraud management, with particular focus around timeliness, substance, and completeness of responses will be ongoing. Regulators will look for consistency between consumer groups and responsive/fair remediation of disputes.

Source: **KPMG Regulatory Insights**

Fairness



Product Risk

Regulators are expanding oversight from product risk to include execution risk, reinforcing the expectation that firms will be held to the standard of “say what you do, do what you say.” Regulators will assess whether products and services are fulfilled fairly, consistently with the terms and statements provided customers, and that representations are not misleading to a “reasonable” consumer. These efforts will be seen in 2024 around:

- **Clarity:** Continued regulatory focus on the clarity, completeness, accuracy, and consistency of statements and claims made regarding products and services in related marketing, advertising, and disclosures.
- **Supervision:** Continued scrutiny to evaluate whether:
 - Products and services are offered on substantially the same terms to all consumers/investors and are not designed to favor one group over another.
 - Analyses are conducted to identify potential discriminatory outcomes and/or conflicts of interest related to a product or service (including those offered through third or fourth parties, and especially where automated systems are being used,) and steps are taken to mitigate that risk.
 - The “reasonableness” of certain fees or material statements of fact can be substantiated (e.g., “tangible benefit” to the consumer or investor).
 - Investigations of complaints are “reasonable” and pursue timely resolutions.
- **Fraud:** Continued regulatory focus on fraud, identity theft, and other scams (e.g., crypto- or payment-related scams) as costs to consumers and consumer complaints increase. Areas of regulatory focus will include:
 - Fraud models, operations/errors, and investigations processes.
 - Insider misconduct and corruption.
 - Consumer protection laws and regulations; consumer complaints, claims, disputes, and account/transaction freezes.
 - Cybersecurity risk management (including synthetic identity fraud).

Source: **KPMG Regulatory Insights**

Fairness



What to watch

Key fairness regulatory actions to watch (including potential associated legal challenges):

- **Community Reinvestment Act (CRA):** Interagency (FRB, OCC, and FDIC) rules updating the CRA, including “standardized” metrics and expansion of qualified activities.
- **SEC Market Structure:** SEC rules and amendments around market structure, including best execution, disclosure of order execution information, minimum pricing, fees, and pricing transparency, and order competition.
- **CFPB 1033 Consumer Financial Data Rights (Open Banking):** CFPB proposed rule on consumers rights to access their own financial data.
- **CFPB 1071 Small Business Lending Data Rule:** Finalized in 2023, CFPB 1071 requires the collection and reporting of small business credit data. A district court ordered the CFPB not to implement or enforce its 1071 rule against the plaintiffs; additional litigation is ongoing.

KPMG Thought Leadership

Regulatory Insights Materials



- [“Covered Technologies” and Conflicts of Interest: SEC Proposal](#)
- [SEC Examinations Risk Alert: Marketing Rule](#)
- [CFPB Small Business Lending Data \(Section 1071\)](#)
- [SEC Examinations Risk Alert: Regulation Best Interest](#)
- [Fraud, Identity Theft, and Other Scams](#)
- [Biometric Information: Federal Trade Commission UDAP](#)
- [Market structure: SEC proposals addressing transparency, competition, and investor protections](#)
- [SEC final rule for T+1 settlement cycle](#)
- [Enforcement/Supervision to “Automated Systems”](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



Fairness



Call to action...

- **Embed fairness controls:** Embed fairness controls across consumer and retail products and services.
- **Prioritize fairness:** Prioritize and embed fairness across the full customer journey.
- **Centralize processes:** Execute centralized processes; streamline and simplify customer-focused communications.
- **Enhance equitable treatment:** Enhance complaint, claims, and dispute management processes, technology, and data analytics.
- **Evolve compliance management:** Evolve the CMS (across lines) by revisiting the inputs and weights into risk assessments and new product and service reviews and approvals—all to consider inclusion, access, tangible benefit, and consistent and equitable outcomes.

Source: KPMG Regulatory Insights

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Financial Services Risk, Regulatory, and Compliance](#)

[Banking and Consumer Compliance](#)



[Capital markets and investment management](#)

Contacts

Mike Lamberth

Partner

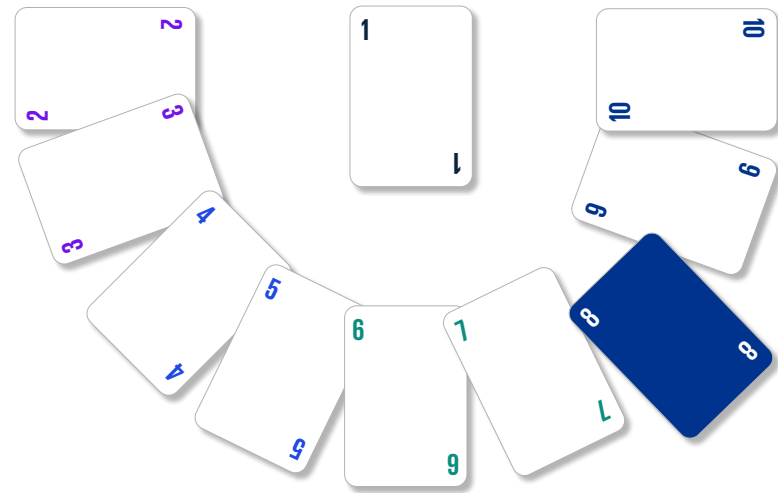
mlamberth@kpmg.com

Mike Sullivan

Principal

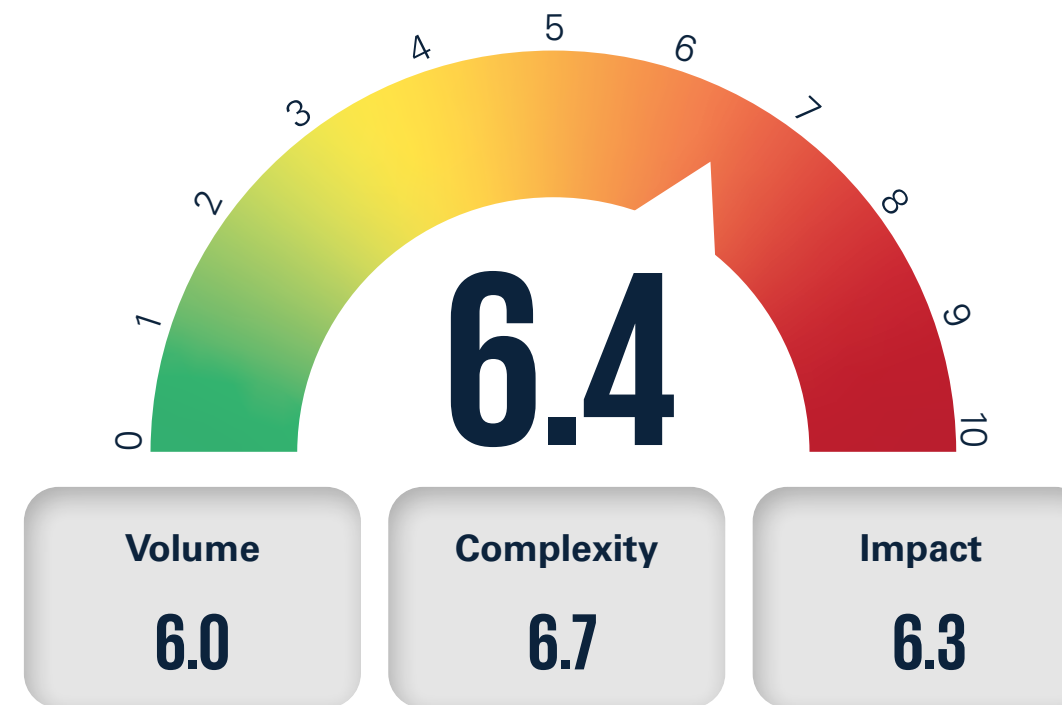
mmsullivan@kpmg.com

Responsible Systems



Regulators are applying existing rules to AI/GenAI, “automated systems,” “predictive analytics,” and other “innovative new technologies,” across a wide array of risks and across the entirety of the firm. As the rules and technologies evolve, risk management will be critical to innovating while maintaining trust.

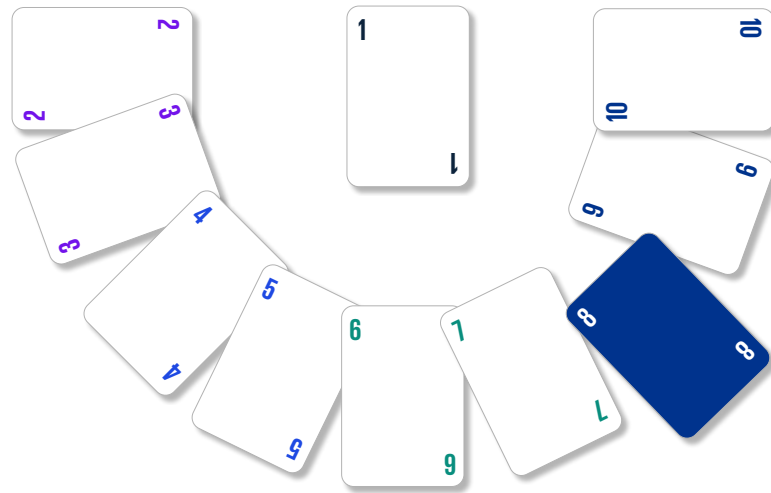
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: **KPMG Regulatory Insights**

Responsible Systems



Current and evolving regulations

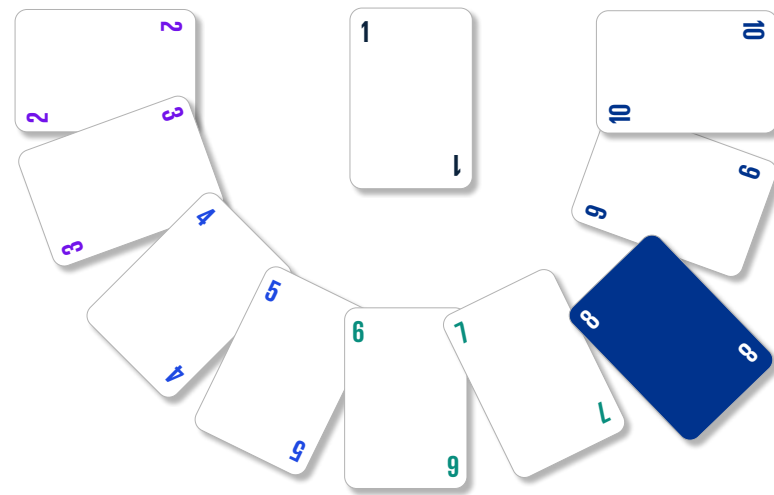
Amid heightened public policy and legislative interest in AI and ML, regulators will apply existing regulations to AI/GenAI, “automated systems” and “innovative new technologies” (e.g., software; models; predictive analytics; and algorithmic processes, such as AI, ML, NLP, and LLMs) across the full lifecycle of design, development, deployment, and continuous monitoring. Regulators across financial services (banking, capital markets, insurance) will focus on whether the technologies (algorithms, tools, and products) can be trusted, work as claimed, and do so without causing harm (financial or otherwise) to users.

Firms should anticipate regulatory attentions in 2024 to focus on:

- **Risk Management:** Regulators will examine risk management and governance of the design, development, deployment, and ongoing monitoring of “automated systems” from the perspective of:
 - Safety and effectiveness (e.g., protections against unintended or inappropriate access or use).
 - Anti-bias and anti-discrimination (i.e., protections against, and ongoing testing).
 - Data governance and data privacy.
 - Transparency (e.g., what/how information is used; potential impacts to businesses/consumers).
 - Accountability and oversight.
- **Fairness/Consumer Protection:** Following the direction of the Administration, regulators will take a “whole of government” approach to supervision and enforcement of fairness and consumer protections in applications of “automated systems” under existing (and evolving) laws and regulations. Key areas of concern include data and data sets, model opacity and access, and design and use—which drive the decision-making enabled by the automated system or related tools. Regardless of the technology used, supervisors will evaluate:
 - Fairness (e.g., UDAAP/UDAP, fair lending, “fair and balanced” marketing, conflicts of interest).
 - Consumer and other legal protections (e.g., civil rights, nondiscrimination, equal employment opportunity).
- **Purpose Limitation and Data Minimization:** With the proliferation of consumer data collection alongside the increasing application of automated systems, regulatory scrutiny and enforcement will focus on:
 - Limitations around collection, access, use, retention, and disposal of consumer data for specific and/or explicit purposes, subject to permission, consent, opt in/out, and authorization, as appropriate (e.g., only what is needed).
 - Limitations on data retention (e.g., only for the stated purpose).
 - Safeguards on access and use.

Source: **KPMG Regulatory Insights**

Responsible Systems



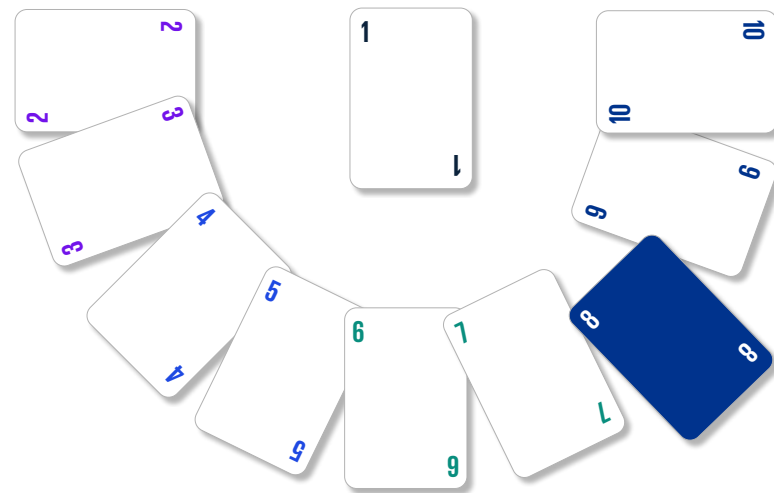
Regulatory complexity

Expect regulatory approaches and areas of supervisory focus on automated systems and new technologies will evolve and may diverge across state, federal, and global jurisdictions, increasing the complexity of compliance. Similarly, regulatory expectations in other evolving areas that touch on system inputs and outputs, or customer impacts (e.g., fairness, privacy, security), may overlap with expectations for automated systems and new technologies, heightening scrutiny and additional complexity.

- **Regulatory Divergence:** Diverging regulatory approaches or areas of supervisory focus on automated systems would greatly expand the complexity of both risks and compliance and necessitate reassessment of current and target state compliance functions and approaches to compliance risk assessments. Impact assessments, jurisdictional risks, regulatory awareness, and timing would also need to be considered.
- **Jurisdictional Challenge:** Legal challenges to regulatory approaches, such as application of existing consumer protection regulations to examine firms' systems, technologies, data, and algorithms, could similarly present added complexity if uncertainties around regulatory jurisdiction and authorities persist.

Source: **KPMG Regulatory Insights**

Responsible Systems



Spanning risks

The benefits and risks of automated systems will touch areas across firms, including aspects of operations, products and services, and customer interactions. Areas to watch for upcoming regulatory developments include:

- **“Trustworthiness”:** Focus on the trustworthiness of automated systems and new technologies, particularly around safety, efficacy, fairness, privacy, “explainability,” and accountability. This will necessitate a holistic reassessment of the purpose and application of automated systems throughout the firm, including data collection, inputs and outputs, use, privacy, and security.
- **Model Risk Management:** Expectation that the design, development, deployment, and monitoring of automated systems will be incorporated into the firms’ MRM framework (and legacy risk frameworks will be adapted, as appropriate), including:
 - Areas such as approved use, ongoing monitoring, and risk ratings.
 - Protocols for modeling usage that align to the MRM standards.
 - Monitoring of legislative/regulatory actions necessitating potential changes to practices or business models.
- **Misuse or Inaccuracy:** Risks associated with misuse or inaccuracy will be assessed through the AI risk management framework; regulators will look for:
 - Robust development, implementation, and use (e.g., clear statement of purpose, sound design, theory, or logic).
 - Effective validation conducted independently of design and development.
 - Sound governance, policies, and controls (e.g., access controls, training).

Source: **KPMG Regulatory Insights**

Responsible Systems



What to watch

Key regulatory actions to watch concerning the design, development, deployment, and ongoing monitoring of responsible applications of automated systems and new innovative technologies will include:

- **Executive Order on Safe, Secure and Trustworthy AI**: White House Executive Order calling for AI risk management actions/standards for privacy, security, consumer/investor protections, and innovation.
- **Enforcement/Supervision to “Automated Systems”**: Interagency Statement (CFPB, DOJ, EEOC, and FTC) on supervision and enforcement (under existing authorities, e.g., civil rights, nondiscrimination, fair competition, consumer protection) of automated systems and new technologies.
- **Automated Valuation Models**: Interagency (FRB, OCC, FDIC, CFPB, NCUA, and FHFA) proposal on quality control standards for automated valuation models (AVMs), including compliance with applicable nondiscrimination laws.
- **“Covered Technologies” and Conflicts of Interest**: SEC proposal “to eliminate conflicts of interest associated with interactions with investors [e.g., correspondence, online, advertising] through the use of technologies [e.g., predictive analytics, AI, ML] that optimize for, predict, guide, forecast, or direct, investment-related behaviors or outcomes.”
- **Ensuring Trust in AI: Commerce Department Request for Comment**: A request for information on AI accountability measures and policies with a focus on how to provide “reliable evidence to external stakeholders—that is to provide assurance—that AI systems are legal, effective, ethical, safe, and otherwise trustworthy.”

KPMG Thought Leadership

Regulatory Insights Materials



- [Executive Order on Safe, Secure, and Trustworthy AI](#)
- [“Covered Technologies” and Conflicts of Interest: SEC Proposal](#)
- [Enforcement/Supervision to “Automated Systems”](#)
- [Interagency Proposals: Automated Valuation Models: Reconsideration of Value](#)
- [Ensuring Trust in AI: Commerce Department Request for Comment](#)
- [Focus on Tech: Cloud, AI, Personal Data](#)

- [Where will AI/GenAI regulations go?: Demonstrating ‘trusted AI systems’](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



Responsible Systems



Call to action...

- **Establish and maintain a governance framework:** Implement and maintain a governance framework that guides the design, use, and deployment of automated systems ensuring adherence to ethical standards, regulatory requirements, and best practices.
- **Conduct predeployment testing and ongoing monitoring:** Perform thorough predeployment testing, risk identification, and mitigation for automated systems to ensure their safety and effectiveness. Conduct runs in parallel with existing processes and have demonstrable uplift from a regulatory perspective (e.g., decrease in false positives) before full deployment. Stay up to date on regulatory developments; implement continuous monitoring and evaluation practices to identify potential issues, biases, and undesirable outcomes in a system's performance; and adjust accordingly.
- **Promote transparency and accountability:** Foster a culture of transparency and accountability within the organization, clearly communicating the goals, functionality, and potential impacts of automated systems to both internal and external stakeholders.
- **Implement effective MRM:** Adopt a robust MRM framework to ensure models are reliable, accurate, and unbiased. Conduct regular validation, testing, and monitoring of the models, and timely address any identified issues to minimize adverse impact on investors and comply with regulations. Provide transparency regarding model performance and risk exposure to the board and management.
- **Provide human alternatives and remediation:** Offer human alternatives and fallback options for customers who wish to opt out from using automated systems, where appropriate. Establish mechanisms for customers to report errors, contest unfavorable decisions, and request remediation, demonstrating the organization's commitment to fairness and responsible use of technology.
- **Understand system strategy and roadmap:** Align the organization's vision, strategy, and operating model for system solutions with their broader goals. Assess the board-level oversight and maintain an inventory of the system landscape within your organization. Monitor third-party risks associated with data protection, storage, and access to confidential data, and evaluate software tools acquired to maintain data security and privacy.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Drive innovation](#)

[AI security framework design](#)

[Intelligent automation](#)

Contacts

Emily Frolick

Partner

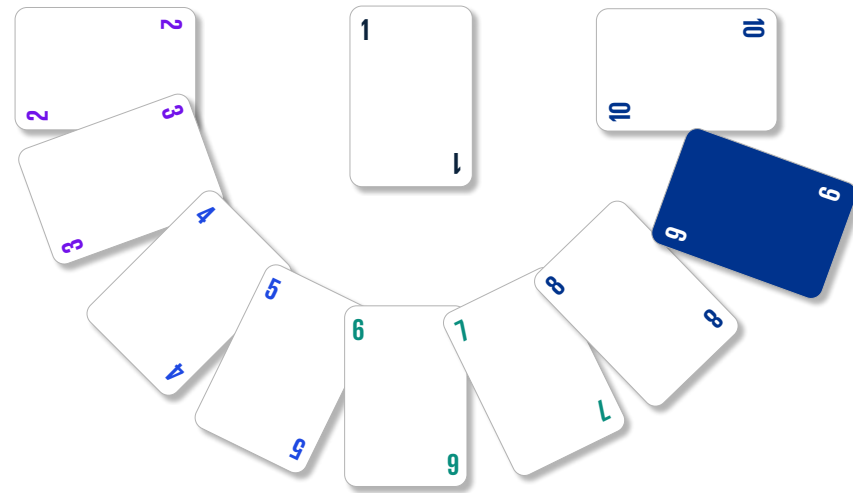
efrolick@kpmg.com

Anand Desai

Principal

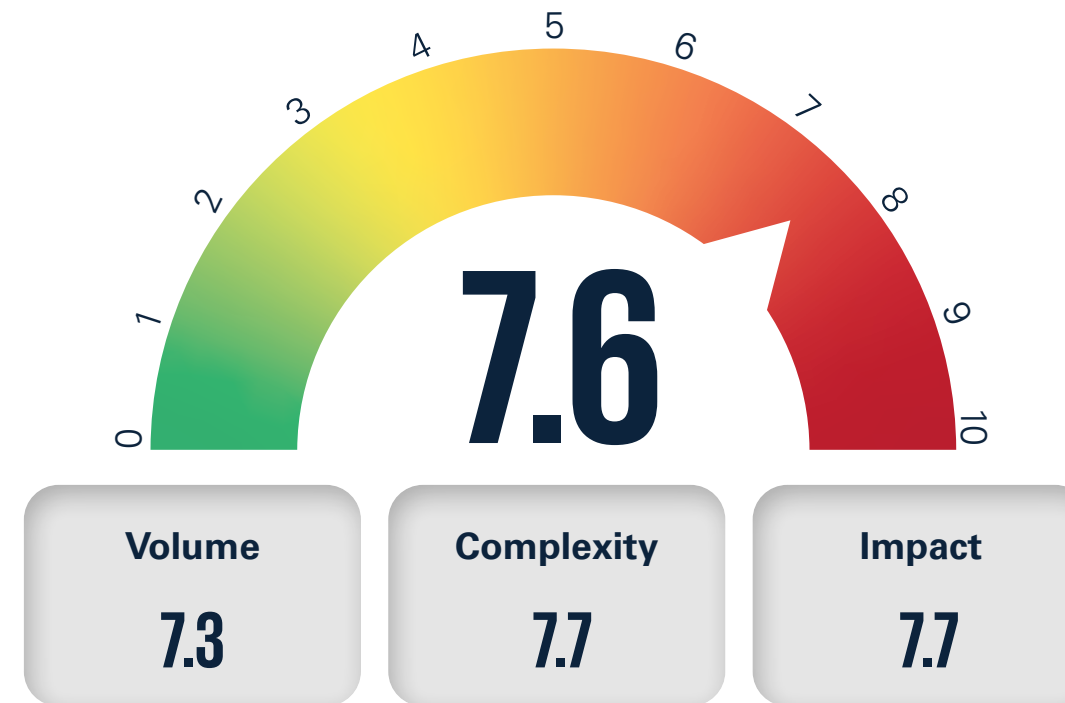
ananddesai@kpmg.com

Security & Privacy



In tandem with all things “data,” broad regulatory concerns around data security, management, and privacy will include, but expand beyond, cybersecurity and IT risk to all facets of regulatory coverage.

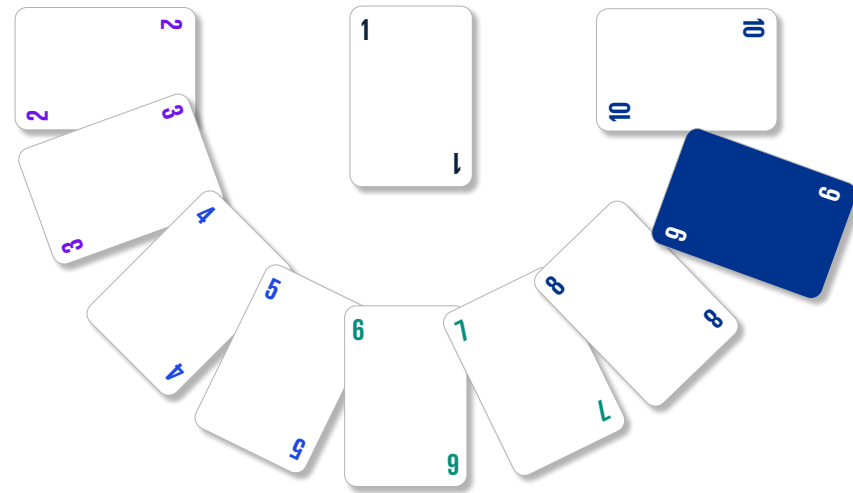
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: **KPMG Regulatory Insights**

Security & Privacy



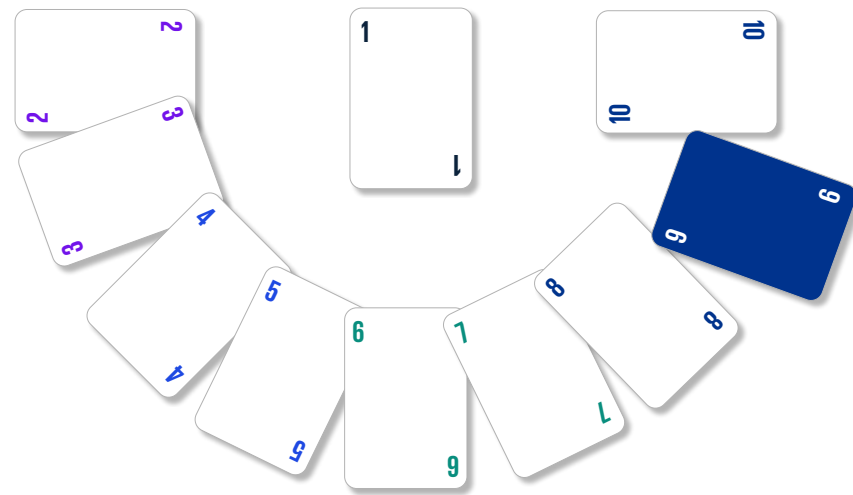
Security

Regulators will continue to focus on strengthening risk management and governance around the security of data, IT systems, and networks as well as promote resiliency and incident response. Regulators will be reviewing:

- **Cybersecurity Threats:** Increasing cybersecurity risks (e.g., adversarial attacks, data poisoning, insider threats, and model reverse engineering) will drive regulatory scrutiny to:
 - Processes for assessing, identifying, and managing risks from potential cybersecurity threats and potential threat actors.
 - Board oversight and management effectiveness, including roles, responsibilities, and applicable experience.
 - Timely reporting and disclosure of material cybersecurity incidents.
 - Speed of incident remediation.
- **Threat Detection and Monitoring:** Expanding expectations around the adequacy of threat detection and monitoring processes will include:
 - Maturity of endpoint detection and monitoring solutions.
 - Coverage of threat intelligence (both on premises and cloud environments).
 - Maturation of third-party risk programs, inclusive of ongoing management of supply chain risks.
- **Technology/Operational Resiliency:** The small number of cloud service providers is driving renewed regulatory focus on the wide range of service uses (e.g., IT and cybersecurity management, data storage, and computing facilities need for AI/ML applications). Areas of interest will include:
 - Resiliency (e.g., cyber incidents, technical vulnerabilities, physical events) and business continuity planning.
 - Transparency from cloud service providers (e.g., information on risks related to incidents and outages needed to build technology architecture with consumer protections).
 - Market concentration, interconnectedness of providers, and concentration of “critical uses” of cloud services and similar third-party services.
 - Clarity and thoroughness of company and cloud provider responsibilities documented in contracts; third party risk management.

Source: **KPMG Regulatory Insights**

Security & Privacy



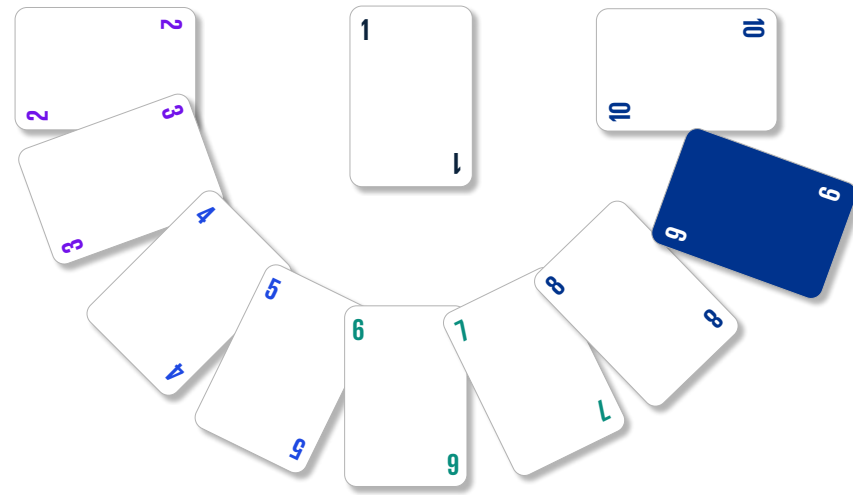
Data management

Regulators emphasize the importance of data management and controls across all systems and applications, whether internal, or through affiliates and/or third or fourth parties, and across the data lifecycle. Areas of regulatory focus will include:

- **Access:** Attention to access management programs and controls (e.g., multifactor authentication (MFA), least privilege, recertification), authentication credentials (e.g., encryption), and data practices (e.g., purpose, collection and handling, use, safeguarding, retention, and disposal).
- **Third/Fourth Parties:** Evaluation of third- and fourth-party risk management and governance processes throughout the relationship lifecycle, including whether “higher-risk” activities and complex relationships are subject to more comprehensive and rigorous oversight.
- **“Automated Systems”:** Application of existing authorities and regulations to supervise and enforce the design, development, and deployment of “automated systems” (e.g., algorithms, predictive analytics, AI, ML, quantum computing and other innovative technologies). Key risk areas will include data integrity, statistical validity, model accuracy, transparency, fairness, resiliency/reliability, and protections against data manipulation. Firms are expected to consider during the design stage and thereafter ways that a system could potentially be misused for fraud or cause other harms, and to take reasonable steps to mitigate such risks through “durable, built-in features.”

Source: **KPMG Regulatory Insights**

Security & Privacy



Privacy

Regulators will continue to assess consumer financial data privacy protections across collection, use, safeguarding, retention, and disposal, including increasing attention to purpose limitation, data minimization, and consumer rights. Expect examinations to cover:

- **Evolving Processes:** Is data privacy considered in the design, operation, and management of new applications, including technology systems, automated systems, and digital business practices, with the goal of preventing vulnerabilities (e.g., malware, fraud, identity theft, insider risk, reputation risk)?
- **Lifecycle Operations:** Are regulatory requirements related to consumer data integrated throughout the data lifecycle, including consumer notices, disclosures, opt outs, and other rights enumerated under applicable privacy laws and regulations (e.g., UDAP, GLBA, GDPR, CPRA)?
- **Data Brokering:** Are data aggregation practices or those of third parties, including monetization and use by data brokers and their customers, designed to ensure transparent practices and consumer privacy protections (e.g., clarity of communications, consumer choice)?

Source: **KPMG Regulatory Insights**

Security & Privacy



What to watch

As data collection and use proliferates, so will security and privacy threats. Key regulatory actions to watch will include:

- **SEC Cybersecurity Disclosures:** Finalized in 2023, the rule requires public companies to disclose information about cybersecurity risk management, strategy, governance, and material incidents. Additional rule proposals for investment funds and advisers and market entities similarly address “cyber hygiene,” incident notification, and data privacy protection.
- **SEC Amendments to Regulation S-P:** A proposal to amend on consumer financial data privacy protections-rules by imposing requirements regarding notification of data breach, monitoring and detection of unauthorized access to or use of sensitive data, and proper disposal.
- **Third-Party Risk Management (TPRM):** Final Interagency Guidance: Finalized in 2023, the Interagency (FRB, FDIC, OCC) guidance establishes expectations for “sound” TPRM over the relationship lifecycle, varying with the degree of risk and complexity of each relationship.

KPMG Thought Leadership

Regulatory Insights Materials



- [Public Company Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure](#)
- [“Covered Technologies” and Conflicts of Interest: SEC Proposal](#)
- [Third-Party Risk Management \(TPRM\): Final Interagency Guidance](#)
- [Third party risk management: SEC Investment Adviser Proposal](#)
- [Enforcement/Supervision to “Automated Systems”](#)
- [Ensuring Trust in AI: Commerce Department Request for Comment](#)
- [SEC Proposals on Cyber Risk Management for Market Entities](#)
- [White House Announces National Cybersecurity Strategy](#)
- [Focus on Tech: Cloud, AI, Personal Data](#)
- [Where will AI/GenAI regulations go?: Demonstrating ‘trusted AI systems’](#)
- [Regulatory Scrutiny of Technology and Data](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



Security & Privacy



Call to action...

- **Enhance board and executive oversight:** Strengthen the oversight of security risk management, strategy, and governance at the board and executive level. Conduct regular communication and reporting between executives, management, and the board to foster a proactive approach to identifying, monitoring, and mitigating potential security threats as well as timely incident response.
- **Maintain transparent and timely reporting:** Implement a system for transparent and timely reporting of security threat incidents, as required by regulatory authorities. All incident-related information should be accurate, up to date, and communicated to the appropriate stakeholders, including regulatory agencies and customers, as appropriate.
- **Effectively govern data management:** Establish formal and effective governance around the management of data assets, including:
 - Governance around data definitions, standards, artifacts, and key data management processes; and
 - Well-defined roles and responsibilities pertaining to the management and ownership of data assets.
- **Prevent privacy vulnerabilities:** Design, operate, and manage new applications, including technology systems, AI, and digital business practices, with the goal of preventing privacy vulnerabilities (e.g., malware, fraud, identity theft, insider risk, reputation risk).
- **Invest in expertise and talent:** Cultivate a skilled workforce that is well-equipped to manage data and security risks in areas, such as systems access/authorization; development of “automated systems”; arrangements with 3rd/4th parties; consumer protections; and data retention, storage, use, and disposal. Encourage ongoing training and continued development at all levels of the organization.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Data privacy](#)

[Cyber Security Services](#)

Contacts

Matt Miller

Principal

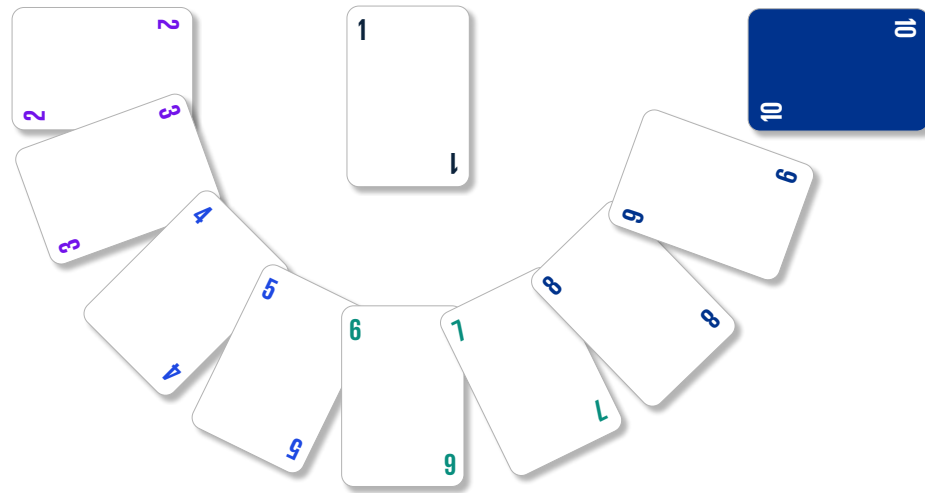
matthewpmiller@kpmg.com

Steve Stein

Principal

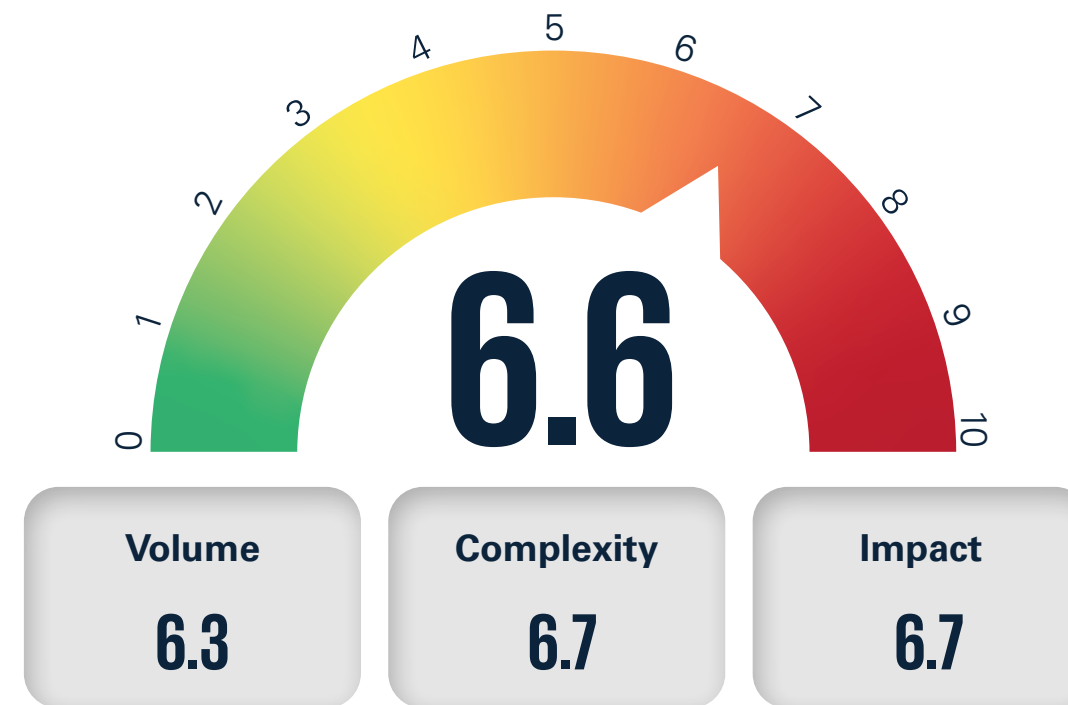
ssstein@kpmg.com

Data



Regulators see data as the potential “soft underbelly” for heightened risk and compliance standards, particularly around quality data governance, data risk and controls, and data lifecycle management.

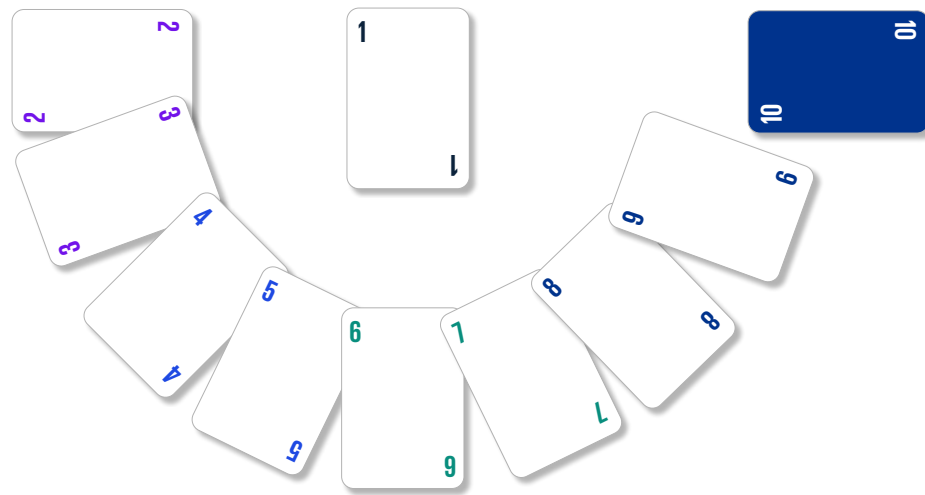
KPMG Regulatory Barometer*



*See KPMG Regulatory Barometer Methodology.

Source: KPMG Regulatory Insights

Data



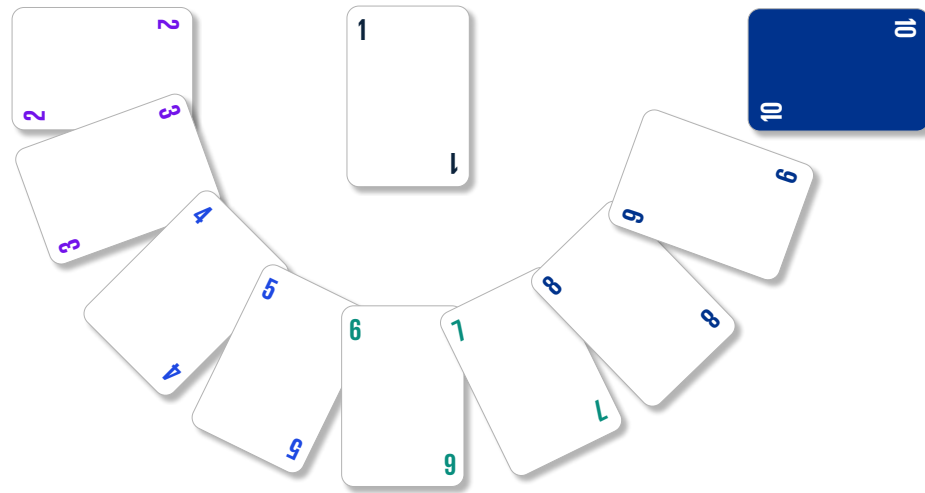
Data governance

Regulators are continuing to look broadly at the strength of firms' data risk management and governance, including policies, procedures, and accountability, data outputs (e.g., reporting, models, metrics), and third-party risks. Scrutiny will focus on firms' understanding and identification of risks around the ways data is collected, used, shared, and/or monetized, as well as how it is protected from misuse. Anticipate data governance supervisory themes to include:

- **Scope:** An expanded scope of regulatory scrutiny will include reporting and other key data outputs (e.g., models, risk metrics, and compliance reports pertaining to fair lending, consumer protection, and financial crimes).
- **Traceability:** Demonstrable ability to trace and report on the relationship between data outputs and business processes, systems of record, and systems of origin.
- **Heightened Standards:** Increasing scrutiny of effective data risk management and compliance program standards across business lines and key functions, and with clear roles, responsibilities, and accountabilities for board, management and across 1st, 2nd, and 3rd lines.
- **Classification:** Data classifications, tiering, and risk ratings based on the level of sensitivity, integrity, and availability, as well as the value and criticality of the data to the firm.
- **Third-Party Data:** Understanding of data sourced from, or shared with, third parties, as well as data risk management and governance requirements embedded into third-party service agreements.

Source: **KPMG Regulatory Insights**

Data



Data risk and controls

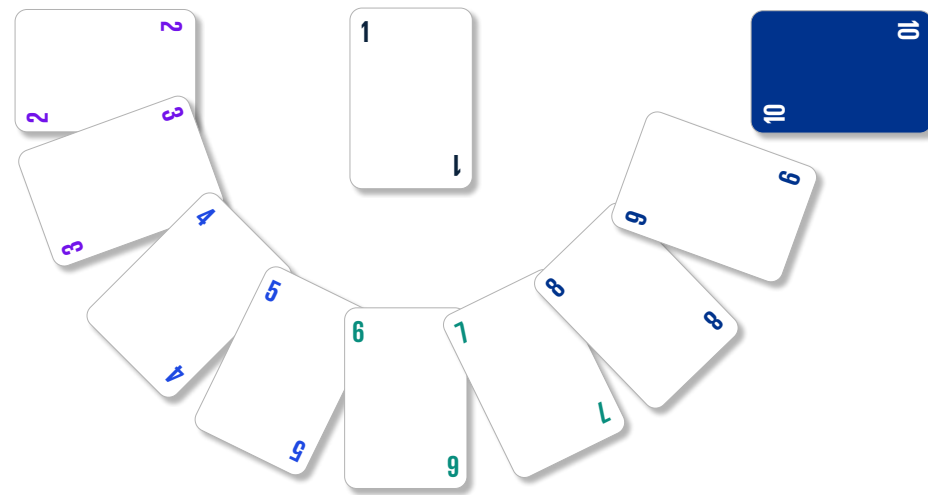
Regulators will assess firms' processes to define, identify, measure, monitor, manage and report on data risks, including those posed by third parties, at all levels of the enterprise.

In 2024 firms should look for continuing regulatory focus on the following capabilities:

- **Data Risk:** Data risk defined through the risk taxonomy (e.g., data protection, data integrity, and data resiliency) and metrics and processes to identify, measure, manage, and monitor risk established at both the line-of-business and enterprise levels.
- **Data Controls:** Standardized data controls established around access and authorization, use, privacy and security, and sharing with third-parties or other data aggregators. These controls should align to the data risk taxonomy and show sustainability through a regular and robust control testing function.
- **Reporting:** Holistic reporting on data risk and controls at the line-of-business, regional/ country, and enterprise levels.

Source: **KPMG Regulatory Insights**

Data



Data lifecycle management

Through guidance, policy statements, supervision, and enforcement actions, regulators have expressed expectations for firms to demonstrate cohesive and comprehensive strategies for managing and overseeing systems, data, and controls throughout the data lifecycle, including procedures for every step of the data lifecycle—from collection or acquisition, processing, and safeguarding to retention, possible migration, and end-of-life processes or disposal.

Expect regulatory examinations to consider:

- **Data collection:** Prioritization of effective risk management and oversight of information systems, data, controls, and procedures, including when data is:
 - Initially captured and processed, especially if the data is sensitive consumer information (e.g., biometric, genetics or health, demographic) or manipulated or altered (e.g., conversion from structured to unstructured forms).
 - Acquired from, shared with, or sold to new data sources, including external third-parties or data aggregators.
 - Migrated to new internal systems from old systems (e.g., legacy or decommissioned) or to external (third-party) systems (e.g., cloud, part of an M&A transaction).
- **Data Retention and Disposal:** Scrutiny of data retention and recordkeeping, including collection, storage, retention, and disposal practices under existing data retention, privacy, and risk management regulations and guidance. Continuing supervision and enforcement focus on data associated with decommissioned systems/IT assets (e.g., end-of-life practices) and recordkeeping associated with unauthorized channels or devices (e.g., SEC Regulation S-P) will continue.

Source: **KPMG Regulatory Insights**

Data



What to watch

Amongst all things 'data', key regulatory actions to watch will include:

- **Data Safeguarding, Retention, & Disposal:** Examination and enforcement around practices for safeguarding and securing data, as well as retaining and disposing of it under existing regulations (e.g., SEC Regulation S-P).
- **Data Risk Management:** Intensifying scrutiny of data risk management processes across business lines and functions, including data classification and traceability, internal governance processes, and external, third-party oversight (e.g., Interagency TPRM Guidance)
- **Data Reporting Requirements:** Increasing expectations around data reporting capabilities, particularly around newly proposed/finalized rules (e.g., SEC cybersecurity and incident disclosures, Basel III capital requirements, CFPB 1071 small business lending data).

KPMG Thought Leadership

Regulatory Insights Materials



- [Public Company Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure](#)
- [Data Retention and Deletion: Increasing Regulatory Expectations](#)
- [Focus on Tech: Cloud, AI, Personal Data](#)
- [Biometric Information: Federal Trade Commission UDAP](#)
- [FTC Recent Focus on Tech: Digital Advertising, Cloud](#)

For more information on ongoing Regulatory Insights materials, [Click Here](#)



Data



Call to action...

- **Clearly define data scope expectations:** Clearly define the scope covered by data governance and ensure that it is expanding beyond the traditional scope of prudential regulatory reports.
- **Adjust risk taxonomy to consolidate data risks:** Ensure the data risk taxonomy addresses data protection, data integrity, and data resiliency and that data owners understand the expectation to own and mitigate those risks.
- **Be explicit on standardized data controls:** Ensure that there are standardized data controls aligned to the data risks and there is clear guidance for the lines of businesses and functions on what minimum control requirements apply to what scope and how to operationalize the controls.
- **Continuous monitoring and improvement:** Drive ongoing monitoring and assessment of your organization's holistic data risk to ensure effectiveness of the controls and to address potential risks.

Source: **KPMG Regulatory Insights**

How KPMG can help

Click below on the picture or the hyperlinks to learn more about related KPMG services

[Financial Services](#)

[Financial Services Risk, Regulatory, and Compliance](#)

Contacts

Brian Radakovich

Partner

bradakovich@kpmg.com

Robert Westbrook

Principal

rwestbrook@kpmg.com

Definition of terms

- AI: Artificial Intelligence
- AML: Anti-Money Laundering
- AOCI: Accumulated Other Comprehensive Income
- Automated systems: As defined by CFPB, DOJ, DOC, and EEOC, software and algorithmic processes, including AI
- AVM: Automated Valuation Model
- Basel, Basel III, or Basel III Endgame: Proposed Basel III capital requirements as issued by the Basel Committee on Banking Supervision
- BHC: Bank Holding Company
- BSA: Bank Secrecy Act
- CDD: Customer Due Diligence
- CFPB: Consumer Financial Protection Bureau
- CFT: Countering the Financing of Terrorism
- CMS: Compliance Management System
- CPRA: California Privacy Rights Act
- CRA: Community Reinvestment Act
- CTA: Corporate Transparency Act
- CVA: Credit Valuation Adjustment
- DOJ: Department of Justice
- DTA: Deferred Tax Assets
- EEOC: Equal Employment Opportunity Commission
- EPS: Enhanced Prudential Standards
- ERM: Enterprise Risk Management
- FDIC: Federal Deposit Insurance Corporation
- FINRA: Financial Industry Regulatory Authority
- FRB: Federal Reserve Board
- FSOC: Financial Stability Oversight Council
- FTC: Federal Trade Commission
- GDPR: General Data Protection Regulation
- GenAI: Generative Artificial Intelligence
- GHG: Greenhouse Gas
- GLBA: Gramm-Leach-Bliley Act
- IT: Information Technology
- KYC: "Know Your Customer"
- LLM: Large Language Model
- M&A: Mergers and Acquisitions
- MFA: Multifactor Authentication
- ML: Machine Learning
- MOU: Memorandum of Understanding
- MRA: Matter Requiring Attention
- MRM: Model Risk Management
- NCUA: National Credit Union Administration
- NLP: Natural Language Processing
- OCC: Office of the Comptroller of the Currency
- P2P: Peer-to-Peer
- PII: Personally Identifiable Information
- SEC: Securities and Exchange Commission
- SIF: Synthetic Identity Fraud
- TBTM: "Too big to manage"
- TPRM: Third-Party Risk Management
- UDAAP: Unfair, Deceptive, or Abusive Acts or Practices
- UDAP: Unfair or Deceptive Acts or Practices

Regulatory Barometer Methodology

The KPMG Regulatory Insights Barometer assesses areas of upcoming regulatory pressure and direction of change.* The Barometer:

- Is based on a 10-point scale of regulatory intensity that ranges from “minimally increasing” (1.0) to “significantly increasing” (10.0)
- Assesses three attributes for each challenge area:
 - Volume (V)—based on a combination of anticipated rulemakings (proposed/final/guidance), coverage in communications (reports/speeches/hearings), and oversight activities (supervision, enforcement)
 - Complexity (C)—based on factors such as the intricacies of future requirements versus existing ones, consistency of expectations across jurisdictions, and interactions with other regulations or standards
 - Impact (I)—based on factors such as the urgency of action required, potential implementation costs, resourcing challenges, and business risk
- Combines the individual factors for each attribute (V, C, I) to arrive at a single weighted average indicator of regulatory intensity for each challenge area.

* The KPMG Regulatory Insights Barometer is based on KPMG understanding of industry practices and regulatory expectations; KPMG cannot guarantee that regulatory authorities would agree with our analysis and understanding or that our perspectives would foreclose or limit any potential regulatory action or criticism. Further, our views herein may not identify all issues that may exist or that may become apparent in the future and may be subject to change.



Contact us



Amy Matsuo
Principal and Leader
Regulatory Insights
E: amatsuo@kpmg.com

Acknowledgements

We thank the following individuals for the help in drafting and producing this document: Amy Matsuo, Mark Dickemann, Joe Slaninka, Karen Staines, Janna Magnusson and Scott Tevington.

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

