Ten Key Regulatory Challenges of 2025

Rolling through the Shift

Subtitle goes here

Date

Table of Contents

Ten Key Regulatory Challenges of 2025

On behalf of KPMG Regulatory Insights, I am delighted to issue the tenth edition of our annual Key Ten Regulatory Challenges.

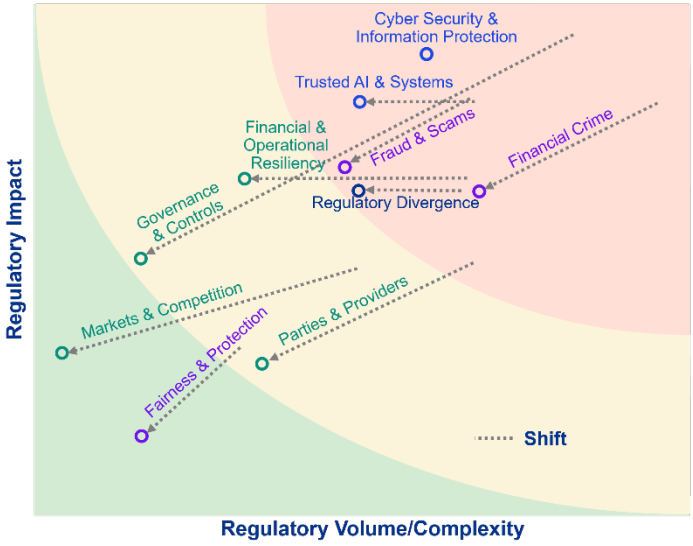
This 2025 edition anticipates the regulatory volume, complexity, and impact due to the new Administration's priorities and changes to agency leadership along with such factors as technology advances, disruptive events, and regulatory divergence.

We anticipate 2025 to be the Year of Regulatory Shift—across areas of technology and data risks, consumer/investor protections, and risk management and governance.

In the following pages we anticipate how this Regulatory Shift will alter regulatory actions and how companies will need to 'roll-forward' to mitigate and respond to these emerging risks.

We, of course, welcome the opportunity to assist you in these and related areas to meet the challenges ahead.

The Year of Regulatory Shift



"2025 will be the Year of Regulatory Shift fueled by a new Administration, agency leadership changes, and expanded regulatory divergence. Companies will look to "roll through the shift" but must remain vigilant to potential new, emerging, and downstream risks—even amidst an agenda to reduce regulatory burden."

Amy Matsuo
Principal & National Leader
Regulatory Insights
amatsuo@kpmg.com

Regulatory Divergence

1 2 3 4 5 6 7 8 9 10

Regulatory Shift

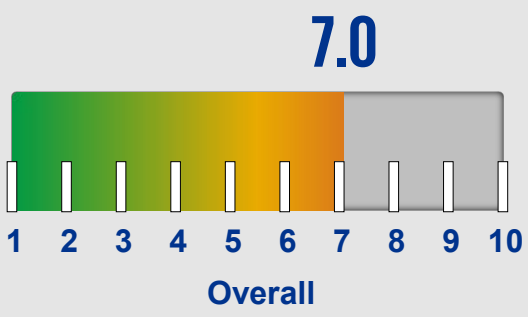
Legal Impacts

Diverging Regulations Across Other Jurisdictions

Actions

Regulatory divergence and legal challenge will continue, drive high operational, risk and compliance challenges/ impacts and potential compliance and reputational risks. Companies will need to remain vigilant and adaptable, balancing the diverse regulations and stakeholder interests to mitigate potential risks and align with emerging and evolving regulatory expectations. Regulatory focus and actions will be impacted by agency leadership mission changes amid the Administration's "day one" priorities. Expect varying associated intensity/lessening of intensity to supervision and enforcement and growing global regulatory.

Regulatory Barometer



6.9	7.0	7.0
Volume	Complexity	Impact

-1.8	↑	↑
Shift	Legal	State

Regulatory Shift

Although the regulatory landscape is expected to evolve in 2025, reflecting changes related to increasing digitalization, technology innovation, and pressure from legislative/ regulatory activity at the federal/state/global levels and associated legal challenge, regulators will continue their focus on resiliency and risk management across industries.

Key areas will include:

Resiliency

Regulators are emphasizing the importance of resiliency in both financial risk (e.g., capital, liquidity, credit) and non-financial risk (e.g., cybersecurity, third party, operational) and companies' abilities to anticipate and manage change, growth, and disruption to processes, systems, platforms, and markets, through effective and sound risk management controls.

Technology Risk

With the increasing adoption of innovative technologies such as AI/GenAI and predictive analytics, there are increasing expectations for risk and compliance in areas of technology risk including:

- Cybersecurity /information protection (e.g., incident reporting, skilled resources, business continuity planning).
- AI/GenAI (e.g., governance, testing and validation, transparency).
- Third/"nth" party providers and arrangements for "higher risk" and "critical activities" (e.g., cloud services, payments processing)
- Data and models (e.g., inputs, outcomes, bias, privacy).

Financial Crime

To keep pace with increasingly sophisticated financial crime threats (including risks to critical systems, services and infrastructure), expect attention in regulatory areas such as cybercrime, ransomware, sanctions, know-your-customer, AML/CFT, and beneficial ownership.

Fraud

Risks related to fraud, scams, and misrepresentations are increasing alongside advancements in technology, with increasing and significant cost to consumers and companies. Closely tied to cybersecurity and data privacy risks, regulators will focus on areas of expanding threat and vulnerability in 2025, including:

- Consumer/investor protections against fraud, identity theft, and imposter and other scams (e.g., payments, deepfakes).
- Complaints management (e.g., fair treatment, resolution/remediation).
- Analysis of loss exposures associated with existing and new products and services and associated model risk management.
- Data quality, lineage, sharing, and access (within and across the company and its parties/providers).

Rulemaking

Regulators will continue to utilize and apply existing rules, regulations, and guidance (e.g., heightened standards/ERM, financial stability, AML/BSA, UDAAP/UDAP, fair marketing, conflicts of interest, recordkeeping) to the supervision and enforcement of new and emerging areas (e.g., "automated systems," predictive analytics, crypto and digital assets, digital devices), as appropriate.

Legal Impacts

Regulatory Shift

Legal Impacts

Diverging Regulations Across Other Jurisdictions

Actions

Legal challenges and impacts from prior legal cases will continue to stymie rulemaking resulting in:

Increased Guidance vs. New Regulations

A noticeable rise in legal challenges to federal and state level regulations will prompt a shift towards more guidance and frameworks rather than the introduction of new regulations.

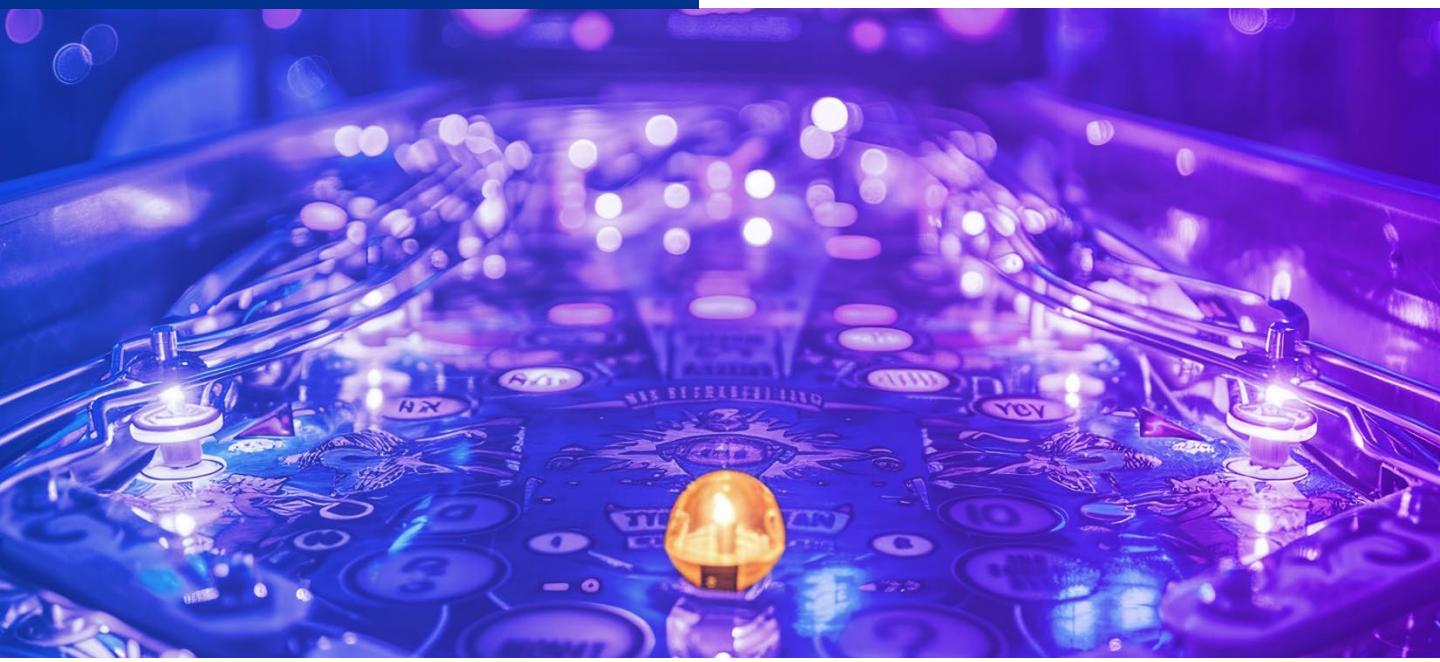
Extended Rulemaking Processes

Agencies will take measures to fortify their case for regulatory requirements and jurisdictional authority by:

- Seeking consumer voice and industry comments via RFIs, extended comment periods, etc.
- Providing indicators of potential regulations prior to releasing rulemakings through analytic/assessment analysis, reports, blogs, and speeches.
- Continuing to assert jurisdictional authority in enforcement and rulemaking procedures.

Agency Legal Actions

The uptick in legal actions both against and by agencies, particularly in areas such as anti-trust and labor practices, will continue to highlight the contentious and complex nature of regulatory enforcement.



Diverging Regulations Across Other Jurisdictions

State & Global Regulatory Activity

As federal rulemaking is slowed due to bipartisan divergence, state regulatory activity is expected to continue to increase, especially in areas such as AI, cybercrime, privacy, and “fair access” consumer/ investor protections. In addition, differences in global regulations and supervisory frameworks create varying requirements by geography or jurisdiction.

Operational and Compliance Risk

Divergences across states and between state, federal, and international regulations will increase regulatory complexities. These differences could potentially heighten reputational, compliance, and operational risks (and costs).

Actions

Assess governance structure for Risk and Compliance. Expanded roles in terms of both direct and indirect areas of Compliance coverage (e.g., AI, data and privacy, human rights, responsible business practices) and buy-in from the Board to drive initiatives.

Build/update process and control inventories dynamically linked to changes (e.g., regulatory, product, channels, etc.). Use of evolving advanced predictive analytics to help with scenario analysis and resiliency process and control enhancements.

Enhance automation to enable increased risk coverage and ongoing monitoring to supplement business unit activities. Deploy/enhance real-time reporting that is integrated across the business and risk and compliance. Expand compliance data analytics, threshold metrics/"near-misses", etc. in order to drive dynamic assessments of compliance effectiveness.

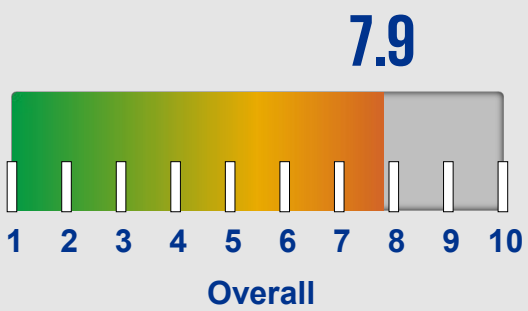
Conduct dynamic and ongoing skills, resourcing levels, asset allocation and technology investment assessments to identify the most important departmental needs to appropriately mitigate emerging risks. Expand analytical and technological skill sets to risk and compliance teams. Use alternative workforce models and investments in assets and technology (in relation to business functions) to effectively expand coverage and utilize valued skills to highest/best use.

Establish appropriate responsible and trusted technology and data processes, practices and controls 'by design' and through regular testing and assurance. Ensure the adoption and deployment of technology to further automate routines and expand the prevention/mitigation of risks. Incorporate the appropriate access to data and use of AI and other technology/ automation and analytics to both drive efficiencies in operations and better anticipate, measure and mitigate risk and compliance.

Trusted AI & Systems

In 2025, anticipate repeal of the current AI Executive Order and the establishment of a new AI Executive Order focused on prioritizing AI innovation and growth across all agencies. Expect continued application of existing regulations and frameworks to AI and systems alongside a push toward "non-regulatory approaches" such as industry/sector-specific policy guidance and the use voluntary frameworks and standards (such as the NIST AI Risk Management Framework), and test/pilot programs. The Administration and regulators will continue to focus on the interplay between trusted systems and potential cybersecurity, privacy and national security risks as well as increase their focus on the nexus between AI policy and energy policy and lessen the focus on potential "AI harms". Expect ongoing expansion of state bills/laws and legal challenges to serve as precedent for new policies and/or rulemakings; the significant volume of AI-related state activity will likely pressure Congress and the Administration to establish a federal AI policy framework.

Regulatory Barometer



7.4 Volume	8.3 Complexity	7.7 Impact
-0.7 Shift	Legal	State

Core Principles for Trusted AI

U.S. efforts to regulate AI and systems/technologies continue to evolve largely through guidance, laws/ regulations, and enforcement to address potential consumer harm. The regulatory focus will continue to align on core principles, though may be nuanced for specific agency and state focal areas.

These core principles include:

Fairness

AI and systems are deployed in a manner that:

- Mitigates the risk of bias, conflicts of interest, and other consumer harm.
- Incentivizes fair competition (e.g., interoperability and choice).

Explainability & Accountability

Developers, deployers, and acquirers are responsible for clearly demonstrating:

- Understanding of system inputs, applications, and outcomes.
- Clear disclosure providing stakeholders with an understanding of each AI/system, and evidence supporting the accuracy of claims (e.g., prevent "AI-washing").
- Efforts to monitor/mitigate risks around synthetic content, including AI-generated "deepfakes" (e.g., authentication, "watermarking").
- Human accountability at all levels of decision-making.

Risk Management

A risk management framework covering the full AI lifecycle (design, development, use, and deployment) and requiring:

- Governance policies and controls.
- Validation independent of design and development.
- Policies and practices to ensure "safe" design and implementation including safeguards against harm to people, businesses, and property and consistency with the intended purpose.

Security and Reliability

Safeguards to reinforce the reliability of AI and systems against potential risks or disruptions through:

- Testing and validation prior to public release and ongoing thereafter to assure AI and systems operate in accordance with their intended purposes and scope.
- Protections/controls against manipulation and unintended use (e.g., adversarial attack, data poisoning, insider threat.)

Data Privacy

Collection and use of consumer data comply with applicable data privacy and protection laws and regulations, and incorporate features to limit:

- Use of data to specific and/or explicit purposes, subject to permission, consent, opt-in/out and/or authorization, as required.
- Access to data and systems.
- Retention of data for only as long as needed.

Data Integrity

Data is assessed/tested for accuracy/quality, completeness, consistency, appropriateness, and validity prior to use and ongoing as part of the design and application of technological tools, promoting trust in the AI decisioning.

A Multifaceted Approach to Risk Management

With the core principles as a base, federal agencies will continue to apply existing and new guidance, regulations, and frameworks toward managing the risks related to AI and systems. Multiple public-private initiatives are underway to inform (through information sharing, testing, transparency) the understanding of, and promote innovation in, AI model development and related regulatory guardrails. Related state activity is also gaining momentum at both the legislative and regulatory levels.

The focus on risk management will cover the full AI lifecycle and include:

Frameworks

Cross-agency evaluation of risk management practices under:

- Existing laws, regulations and frameworks (e.g., consumer and employee protection laws and regulations, model and third-party risk management guidance).
- New, evolving, and anticipated frameworks, standards, and regulations (e.g., NIST's AI and Cybersecurity Risk Management Frameworks, ISO 42001, application of TCPA to AI-generated voice).

Governance

Cross-agency focus on robust, and effective governance practices, including:

- Understanding the inter-relationships among the core principles, changing societal dynamics and human behaviors, and AI risks.
- Implementing practices/parameters for development, implementation, and use (e.g., clear statement of purpose; sound design, theory, and logic).
- Testing and validation of systems and risks, including third parties.
- Promoting transparency (e.g., what data is used, how data is used, impact assessments) and accountability (e.g., claims, ethical application).

Purpose Limitation & Data Minimization

Driven by the proliferation of available consumer data, the volume of data needed to train AI models and systems, and the increasing number of applications of AI and systems, regulatory attentions and enforcement will focus on:

- Compliance with data privacy laws and regulations, including protections against disclosure of sensitive data including biometric, health, location, and personally identifiable information.
- Responsiveness to consumer data requests (e.g., corrections/revisions, consent, opt in/out, authorization(s), deletion).
- Protections against bias, including data enrichment, as well as protections against adverse threats such as cybersecurity breaches, data poisoning, and misuse of the model/data.
- Limitations, including collection, access, and use as well as permission(s), consent, opt in/out, and/or authorization.
- Retention, safeguards, and disposal practices (e.g., disposal of devices/ assets containing customer data).

Continual Improvement

Regulators will expect companies to demonstrate continual improvement of the risk governance/management/controls framework. Better practices are expected to evolve based on public/private information sharing (within and across organizations as well as across regulators) especially in areas such as risk management, decision making processes, responsibilities, common pitfalls, and TEVV (testing, evaluation, validation, verification).

AI Risk Challenges

The implementation of AI and systems is marked by complexity due to the speed of technological advancements, evolving standards, and the need for effective change management. Regulatory discord and legal challenges at the federal, state, and global levels may exacerbate these complexities.

Speed

The rapid pace of AI system development and deployment, both in-house and through third parties, requires agility in adapting to new applications of existing laws/regulations, evolving standards, and new requirements.

Transparency

Legislators and regulators are looking to impose guardrails that broadly will protect consumers, financial stability, and national security from potential misuse of AI and systems. Through laws and regulations, they are looking to hold model developers, deployers, companies, boards and managements accountable for AI and system applications and outputs, placing importance on the ability to explain, and disclose as required, the:

- Goals, functionality, safety, and potential impacts to both internal and external stakeholders.
- Identification, assessment, and mitigation of risks.
- Accuracy, clarity, and consistency, as well as supporting evidence for claims made and associated marketing.

Divergence

Even when aligned on the core principles, diverging regulatory frameworks and expectations across federal, state, and/or global jurisdictions or by industry or geography, could greatly expand the complexity of both risk and compliance challenges, and necessitate a reassessment of current and target state compliance functions/approaches to compliance risk assessments. Divergences are likely to develop when:

- Laws or regulatory and supervisory frameworks have a multi-jurisdictional reach/application.
- The outcomes of legal challenges inhibit or encourage rulemaking by setting a new precedent.

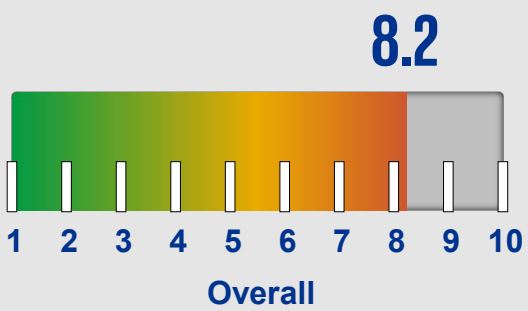
Actions

- **Establish and maintain a governance framework:** Implement tools and technology to support and operationalize a scalable governance framework that guides the design, use, and deployment of automated systems ensuring adherence to ethical standards, regulatory requirements, and best practices.
- **Conduct pre-deployment testing and ongoing monitoring:** Perform thorough pre-deployment 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.
- **Adapt to the speed of AI development:** Adopt a dynamic approach to new applications of existing laws/regulations, evolving standards, and new requirements by implementing streamlined processes for development, testing, and validation; robust training programs; arrangements to leverage external third-party expertise and technology; tailor strategies to meet unique demands and regulatory requirements across industries and geographies.

Cybersecurity & Information Protection

As cybersecurity risks remain a key concern across industries, and particularly relative to critical infrastructure and security, regulatory scrutiny of data security, data risk management, operational resilience, and incident response/ reporting will continue in 2025. Anticipate that federal regulatory activity will remain elevated driven by the complexities and interconnectedness of transactions, including the use of third-party AI/technology products and services and data protection/ privacy concerns. Similarly, anticipate a continuation of state adoption of cybersecurity laws and regulations.

Regulatory Barometer



7.3 Volume	8.8 Complexity	8.1 Impact
+0.7 Shift	Legal	State

Harmonization & Reciprocity

Alongside benefits of the expanding digital environment, looming threats and vulnerabilities spur calls for a unified approach to cybersecurity risk management. Under the National Cybersecurity Strategy, released in 2023 and updated in 2024, a whole-of-government effort has been underway to create a “unified cybersecurity framework” at the federal level, harmonize and streamline regulations, and establish reciprocal recognition amongst regulators and across industries.

A Cross-Sector Approach

Focusing initially on critical infrastructure sectors, initiatives in 2025 will consider:

- Setting baseline or minimum regulatory requirements across all sectors, including minimum accountability mechanisms for security and operational resilience.
- Harmonizing incident and ransom payment reporting requirements with other federal reporting regimes.
- Testing regulatory reciprocity frameworks through pilot programs.
- Supporting calls for legislation to set national cybersecurity and data privacy standards.

These efforts are separate from ongoing state-level legislative and regulatory activities related to cybersecurity and data privacy.

Supervision and Enforcement

With rising adoption of digital tools and services (e.g., cloud, e-communication technologies and platforms, fintech service providers), the volume and complexity of cyber threats (e.g., adversarial attacks, data poisoning, insider threats, and model reverse engineering) to critical infrastructure entities is increasing. In response, regulatory scrutiny is intensifying in areas of:

- **Risk Management**, across security-related risks (e.g., cyber/technology, operational, physical, third party) and in areas related to risk assessment, systems access, threat detection and vulnerabilities, reporting, recovery, and recordkeeping.
- **Data Management**, where regulators expect heightened standards related to data governance, tiering, lineage, and data quality to support enhanced reporting and risk management, as well as to cyber risk management (more targeted vulnerability and patch management) and privacy risk management (privacy rights management, privacy impact assessments).
- **Cyber Resiliency**, with a focus on demonstrable mechanisms to secure and fortify critical cyber infrastructure (e.g., protections against cyber incidents, technical vulnerabilities, and physical events and related business continuity planning).

Meeting Minimum Standards

At a minimum, regulators will continue to focus on companies' efforts to strengthen governance and risk management around the security of systems and data both internally and through affiliates and third/nth parties.

Regulatory areas in the spotlight may include:

Compliance

With existing security-related rules and requirements, such as the SEC Cybersecurity Final Rule for Public Companies, Interagency Guidance on Third-Party Risk Management, and the FTC Safeguards Rule as well as the potential for new rulemakings and frameworks/guidance specific to cybersecurity, data privacy, or AI.

Privacy Practices

As part of an ongoing focus on data minimization, usage, deletion/disposal, controls, and consent.

Data Classification/Tiering

Given the heightened focus on data governance and management practices over risk management data, regulators will increasingly assess data classification and tiering based on data sensitivity, integrity, availability, and criticality, with due consideration for data sovereignty and localization requirements under data privacy laws.

Parties & Providers

Including companies' abilities to demonstrate effective risk-based oversight for all types of relationships/ arrangements, giving consideration to market concentration, the interconnectedness of providers, and supply chain risks as well as assessing the provider's ability to meet compliance obligations (e.g., incident reporting requirements) and to protect data privacy/ security.

Staffing/Resources

To ensure that cyber/data personnel possess the specialized knowledge and skills necessary to identify, analyze, and remediate emerging threats, and also that the relevant workforce is adequately staffed and resourced.

Reporting Threats and Incidents

Increasing cybersecurity risks and expanding expectations around threat detection and monitoring are focusing regulatory attention to reporting timeliness and adequacy both internally and externally.

Anticipate regulators will continue to review:

Board/Management Reporting

The effectiveness of board and management engagement in cybersecurity risk management and governance including:

- Roles, responsibilities, and experience.
- Oversight of processes for assessing, identifying, and managing potential cybersecurity threats and threat actors.
- Frequency, timeliness, and accuracy of reporting as well as the reporting scope (e.g., line of business, enterprise-wide, regional).
- Speed of incident remediation.

Incident Reporting/Disclosure

The timeliness and transparency of reporting disclosure for identified significant, substantial, or material cybersecurity and/or data breach incidents and ransom payments. This includes notifications, as appropriate, to:

- The primary regulator.
- Other regulatory authorities (e.g., SEC, CISA, state authorities).
- Public disclosures (e.g., Form 8K, website).
- Impacted customers.

Actions

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.

Third party risk assessments: Maintain a broad inventory and perform a risk assessment of third parties involved in the delivery of business software and services to assess their operational viability, financial health, security practices, compliance history, and previous incidents. Assess potential for over dependence or over-concentration on a small number of parties/providers.

Resiliency: Cultivate a culture of resilience, embedding robust contingency plans that encompass not just IT infrastructure but also key business operations. Conduct regular impact assessments using a variety of scenarios.

Data Security: Build a comprehensive inventory of data (at rest and in transit) across the organization. Identify and label "crown jewel" data assets, and categorize and classify structured and unstructured data, and assess threats, vulnerabilities and risks. Align proactive monitoring and preventative data protection controls to identified data assets based on risk exposure such as Data Loss Prevention (DLP), encryption, data masking, and use of synthetic data to mitigate risk exposure to a level aligned with organizational risk tolerance and regulatory posture.

Recovery Planning: Evaluate the ability to handle recovery at scale and under pressure; develop/ modify the backup and recovery plan as appropriate.

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.

Enhance Vulnerability Management Practices: Deploy advanced tools and processes for continuous vulnerability detection. Prioritize remediation efforts based on risk assessments and promptly address vulnerabilities to mitigate potential threats.

Financial Crime

Heightened Risk

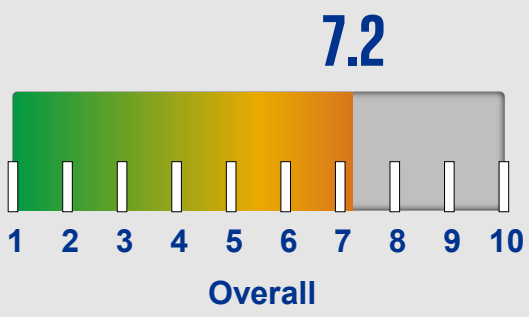
Data Lineage & Quality

Thresholds & Monitoring

Actions

Focus on financial crime regulation (inclusive of sanctions, anti-corruption, know-your-customer, anti-money laundering, beneficial ownership, etc.) is unlikely to abate in 2025. Anticipate expansion of regulatory coverage as well as challenges to legal jurisdictional authorities at the federal and state level to continue. Expect ongoing heightened supervision/enforcement against financial crime risks, including illicit and terrorist finance and sanctions compliance amidst rapidly evolving technology innovations and increasingly sophisticated financial crime patterns.

Regulatory Barometer



7.0 Volume	7.5 Complexity	7.0 Impact
-1.1 Shift	⟷ Legal	⟷ State

Heightened Risk

Regulators will continue to focus heightened supervisory and enforcement attention on financial crimes in 2025 due to the risks associated with rapidly evolving technologies, growing sophistication of threat actors, increasing numbers and complexity of threat attempts, and layers of interconnections and interdependencies within the financial system.

Regulators will be reviewing:

Inherent Risks

Including efforts to identify, manage, and mitigate risks derived from geopolitical divergences affecting the business and potential misuse/abuse of new or evolving technologies by malicious individuals or groups.

Priority Areas

Including efforts to factor FinCEN's national priorities into the AML/CFT risk management and governance frameworks, inclusive of KYB/KYC and CDD. Among these priorities are: i) corruption, ii) cybercrime (e.g., cybersecurity, virtual currency, malware/ransomware), iii) terrorist financing (foreign and domestic), iv) fraud (e.g., identity theft), v) transnational criminal organization activity, vi) drug trafficking, vii) human trafficking, and viii) proliferation financing.

Companies are expected to attract and retain skilled talent, enhance their AML Programs in response to the AML priorities, develop additional tooling and automation, strengthen third-party risk management, and make strategic investments to effectively manage these expanding areas of risk.

Potential/Anticipated Regulatory Changes

The regulatory landscape is poised for change with potential new and anticipated requirements and/or expectations to include:

- Modernization and enhancement of the AML/CFT program requirements across financial institutions (FinCEN proposal), to promote clarity and consistency across financial institutions and explicitly require implementation of a risk-based AML/CFT program with certain minimum components including a mandatory risk assessment process.
- Updates to the National AML/CFT Priorities (expected in 2025) and requirements (as proposed) that the priorities be included as a component in the risk-based AML/CFT program.
- Beneficial ownership reporting and related changes to CDD requirements.
- Multi-agency focus on sanctions activity and efforts to protect national security across industries, products, and services.
- Expanded regulatory coverage to "close the gap", including FinCEN's recent release of Final Rules that will require: i) most investment advisers to implement an AML Program under the Bank Secrecy Act, akin to the existing requirements for banks, broker-dealers and others; and ii) real estate professionals to report information on non-financed residential real estate transactions.

Data Lineage & Quality

Heightened Risk

Data Lineage & Quality

Thresholds & Monitoring

Actions

Regulators continue to look broadly at the strength of companies' data risk management and governance in key risk areas such as financial crimes. Throughout 2024 they have applied heightened expectations to both data and AML/CFT management, including policies, procedures, and accountability; data outputs (e.g., reporting, models, metrics); staffing/talent management (e.g., core skills/backgrounds); and third-party risks. Attention is also focused on companies' understanding and identification of risks around how data is collected, used, stored and shared, as well as how it is protected from misuse.

Anticipate regulatory interest in these areas in 2025:

Data Lineage

Level of process automation and coverage of the entire data flow (e.g., to consolidate data from different business units / subsidiaries) as well as the accuracy and granularity of the data.

Data Traceability

Demonstrable ability to trace and report on the relationship between data outputs and business processes, systems of record, and systems of origin at the customer and transaction level.

Data Quality

Understanding of available internal and external data sources as well as processes to manage and report on data quality issues.

Third-Party Data

Understanding data sourced from, or shared with, third parties, as well as data risk management and governance requirements embedded into third-party service agreements.

Data Risk Governance

Sustainable and robust processes and controls to identify, measure, monitor, manage, and report on risks around:

- Access.
- Authorization.
- Integrity/Quality.
- Collection, use, storage.
- Privacy and security.
- Retention and deletion.

Thresholds & Monitoring

Financial crime risks, exposures, and complexities are increasing alongside technological developments, geopolitical events, and evolving interconnections and interdependencies in financial networks, increasing the importance of continuous improvement in identifying, monitoring, and mitigating potential risks and suspicious activity.

Key areas where regulators will focus in 2025 include:

Risk Tolerance

Established periodic and documented risk assessment processes as well as board approval for risk tolerance levels consistent with the company's risk appetite.

Emerging 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., digital assets, sanctions evasion, malware/ransomware, human rights/forced labor, organized crime). and the adequacy of investment in staffing, training, and resources.

Transaction Monitoring/ Surveillance

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 and potential innovative technologies such as AI.
- Adequacy of investment in staffing, training, and resources.
- Regulatory attention in evolving areas such as BSA/ AML/CFT, trading activity, and KYC/CDD and beneficial ownership.
- Preparation for implementing risk-based compliance programs in priority areas.

Actions

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.

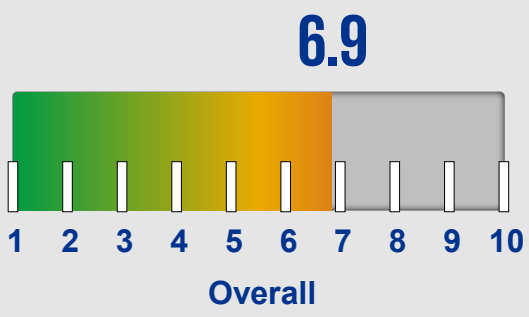
Strengthen security: Establish robust authentication and access protocols for real-time and faster payments to minimize account takeover and social engineering risks. Enhance controls around regulatory focus areas, such as malware, phishing, and identify theft in addition to areas of national AML/CFT priority such as corruption, cybercrime, terrorist financing, trafficking (drug, human), transnational criminal organizations, and proliferation financing.

Fraud & Scams

Nationwide consumer-reported fraud losses well exceed $10B annually, with regulatory alerts directly to consumers and companies being issued nearly every week. This, coupled with a new Administration focus on fraud, waste and abuse (particularly in/related to government spend), will help drive the focus in regulatory supervision of fraud model management, customer and party authentication, and investigation processes.

Anticipate expanding attention in monitoring and reporting practices as well as regulatory policy and alerts in areas of both fraud management and consumer data, particularly in areas such as online privacy, cybersecurity, identify theft, and AI-generated deepfakes. Likewise, state requirements will continue to increase in such areas of AI, privacy and access, causing potentially divergent requirements.

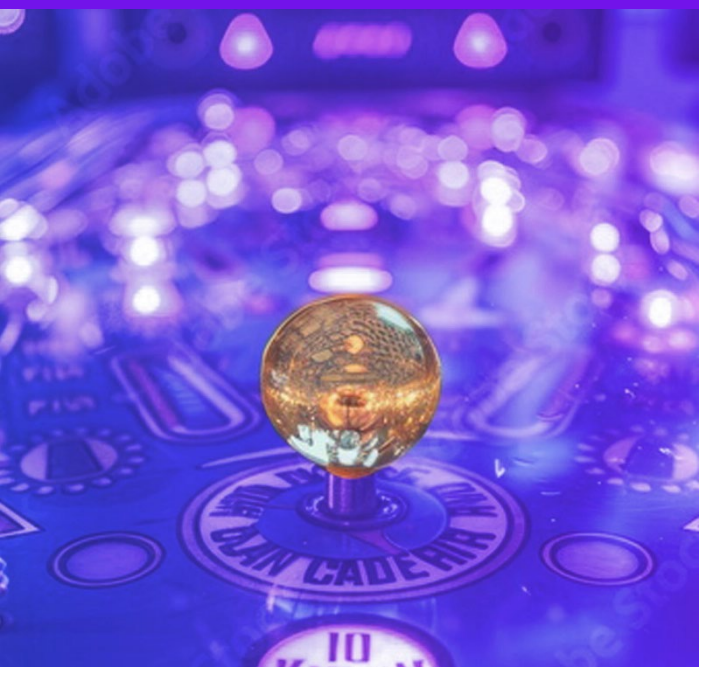
Regulatory Barometer



6.7 Volume	6.9 Complexity	6.9 Impact
+0.3 Shift	Legal	State

Sizing Exposures

As advancements in technology continue to rapidly evolve so too do the risks of fraud and scams along with increasing and significant impacts to consumers, companies, and national security. The magnitude of these risks - and the ties with other risk areas such as cybersecurity, AI, and data privacy - will focus regulators on areas of expanding threat and vulnerabilities.



Key considerations in assessing sizing exposures involve:

Regulatory Focus

Across industries, regulatory agencies' supervisory and enforcement activities are focused on mitigating expanding risks of fraud, waste, identity theft, and imposter and other scams, including those related to "predatory" pricing and payments. Regulatory expectations will include standardized processes and controls around access, authorization, data use, privacy, security, and sharing. Companies must continue to ensure the use of accurate data and controls to measure and manage risk exposure and reporting.

Data Sharing/Access

Given expansions to supply chains and arrangements with third parties and providers, regulators will have concerns for fraud risk as customer data potentially becomes more accessible across diverse platforms. To mitigate fraud and scams, risk management strategies must address vital areas such as large data models, third-party and affiliate data sharing, consent-based customer data sharing, payment verification procedures, and model development and validation.

Exposure Losses

The increasing volume and related costs of fraud and scams against individuals and businesses has led regulators to intensify their efforts to assess the breadth of fraud (e.g., numbers of individuals and/or products impacted) and impact severity through enhanced risk and fraud model management including considerations across:

- Existing and new products or services (e.g., digital assets, AI use and misuse (such as deepfakes)).
- Data privacy/information security (e.g., SpearPhishing threats, account takeovers).
- Consumer/investor protections and demographics.
- Types of fraud and scams (e.g., check, healthcare, synthetic identity frauds, and romance scams).
- Geographic operations.

Identification & Tips

Acting quickly and decisively to prevent, detect, and respond to fraud and misconduct concerns is essential to minimize disruption and loss. Anticipate increased regulatory attention to fraud identification, oversight, investigations, and mitigation.

For example, regulators will evaluate companies' activities related to:

Identification/Tips

Identification and escalation of potential cases of fraud, through active monitoring of:

- Fraud reports received from employee and vendor hotlines.
- Alerts generated by surveillance systems and models/thresholds.
- Investigations reports related to non-compliance with guidance and regulations (e.g., market manipulation, red flag indicators, securities registration, telemarketing sales).

Complaints Management

Ongoing and thorough reviews of customer complaints management with a focus on issues identification including trends/fact patterns, escalation, investigation, and resolution. Within the fraud and investigations management processes, regulators will evaluate the timeliness, substance, and completeness of responses/remediation to customer complaints, claims, and disputes as a measure of "fair treatment". They will also consider the clarity of consumer communications, including what is reimbursable as well as the consistency of responses and/or remediation between consumer groups. Key areas will include:

- Data sharing (e.g., use in large data models, sharing with third parties and affiliates, customer permissioned sharing (and new open banking rules)).
- Authorization/authentication procedures/protections.
- Account holds and freezes.
- Identity fraud (e.g., imposter scams, synthetic identity fraud).

Enhanced Oversight

The effectiveness of risk and compliance oversight of fraud and coordination across the AML/CFT, cybersecurity, and fraud functions. Regulatory attention will also focus on demonstratable, effective Board oversight and the implementation of threat detection/ monitoring processes that include:

- Maturity of endpoint detection and monitoring solutions.
- Coverage of threat intelligence (both on premises and cloud environments).

Internal Controls

To safeguard against fraud and other scams, as well as ensure consumer/investor protections, companies must establish effective internal controls for monitoring, detecting, and mitigating the attempts of threat actors.

Risk Management Program

Updates to fraud risk management programs to keep pace with evolving threats (in addition to effective internal controls, fraud model development and use, and assessments of consumer impacts). Regulators are currently focused on enhancements related to:

- Reporting on more categories of fraud and scams.
- Defining and clarifying when customers can be reimbursed.
- Implementing risk programs to identify and mitigate fraud and scams directed at vulnerable consumer groups (e.g., elderly, military).
- Detecting threats and ongoing monitoring and testing of fraud surveillance.

Data and Reporting

Processes and controls to effectively track and trace customer and transaction data. Examinations and reviews of risk management programs will assess a company's:

- Ability to trace and report on the relationship between data inputs, outputs and business processes, authoritative sources, systems of record, and systems of origin.
- Data quality management standards including accuracy and consistency in fraud models/surveillance.
- Established routines for data reconciliation/quality.

Expect heightened attention to processes and controls relating to:

Authorization

Consent management and customer authentication requirements, such as multifactor authentication, password protection, one-time passwords, biometrics, third-party access, tokens, and peer-to-peer platforms. Implementing safeguards and controls in these areas, aids in the prevention of unauthorized use of sensitive information as it creates barriers for illicit activities.

Resolution/Remediation

Regulators will continue to strongly encourage companies to bolster their risk mitigation and remediation efforts through self-identification, self-reporting, and accountability, as measures of responsiveness to:

- Fraud alerts.
- Customer complaints.
- Misconduct.
- Whistle-blower activities.

Actions

- **Add analytics and automation** to client and third-party onboarding.
- **Aggregate data and** reporting to have a single view of the customers o more effectively manage complex fraud activities and strike a balance between fraud controls and customer experience.
- **Eliminate antiquated** technology and evaluate/implement emerging regtech capabilities to enhance transaction monitoring.
- **Enhance fraud models** to align to consumer protection regulations, monitor for suspicious activities, and provide real-time notifications and alerts.
- **Evaluate and enhance,** as needed, processes for sharing information real-time across departments (e.g., fraud, cyber, disputes).
- **Establish a mature conduct risk program.**
- **Strengthen** controls in regulatory focal areas (e.g., FinCEN priorities).
- **Implement strong IAM strategies,** including PAM and MFA, to secure access to critical customer systems and data. Regularly review access privileges.
- **Integrate BSA/AML** requirements into KYC processes.
- **Conduct dynamic skills assessments** of staffing needs for day-to-day operations of fraud monitoring/identification, investigations, and escalations. Enhance processes and sharing of information real-time across departments (e.g., fraud, cyber, disputes).
- **Develop and promote customer education** and awareness campaigns.

Fairness & Protection

1 2 3 4 5 **6** 7 8 9 10

Access

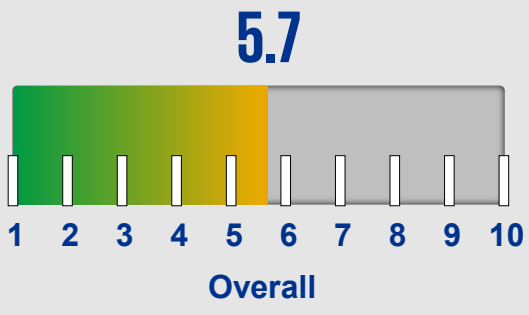
Internal Controls

"Harm"

Actions

Agency leadership mission changes as well as the successful legal challenges to jurisdictional authorities have delayed and/or limited the effect of certain consumer/investor protection regulations. ~~though~~ Existing regulations will still necessitate effective risk and compliance involvement and controls inclusive of product development, marketing, sales, servicing, complaints/claims management, and pricing/fees. The new Administration may look to redefine "fairness" and decrease "net new" federal regulatory activity in this area. Companies should anticipate an increase in state activity relative to individual consumer protections to fill perceived "gaps."

Regulatory Barometer



5.0 Volume	6.0 Complexity	6.0 Impact
-1.9 Shift	Legal	State

Access

The growing number and kinds of companies offering customers similar products and services, and the fact that these companies may operate under different legal authorities that may not be obvious to consumers/investors, raises potential risks and concerns. As innovative and new product/service offerings expand (e.g., crypto and digital assets) it will be key for regulators to both allow for access and do so in a way that keeps sound the guardrails around national security and data protections.

Regulatory Perimeter

Applying existing rules, standards, and frameworks to a broader range of new and novel entities, business combinations/arrangements, and products and to both "close the gap" in regulatory coverage and facilitate/promote access to innovations/developments Examples anticipated in the financial services industry include actions (e.g., rulemaking, enforcement) related to:

- Models/systems, including content limitations, claims/statements, data quality/protections
- Crypto and digital assets
- Expansion of coverage given potential for change in areas such as sanctions, trade compliance, etc.

Examinations Scope

Changes in agency leadership and impacts to agency priorities (e.g., CFPB, FTC, DOJ) may impact examination priorities and/or intensity over time. Regulators will examine for demonstrable evidence of compliance with changes to regulatory expectations and rules ~~related~~ in areas such as:

- New market structure rules (e.g., T+1 settlement cycle, Regulation NMS (order execution, minimum pricing increments, order competition)), including required disclosures and reporting.
- Product, service, and data/ information access (e.g., consumer opportunity to correct false/ fraudulent information, drug/ healthcare access and related "fair pricing").
- Testing and monitoring of AI, models, algorithms, and other decision-making processes used in connection with consumer/investor products and services.
- Merger applications – though influenced by the priorities of the Administration, proposed transactions may be subject to the DOJ/FTC 2023 Merger Guidelines.

Clarity & Accuracy

Access

Internal Controls

"Harm"

Actions

Expect that regulators will continue to hold companies to the standard of "say what you do, do what you say" – and for that standard to be applicable over the full consumer lifecycle (e.g., design/development of new products/services, marketing, sales, servicing).

These efforts will be seen in 2025 around:

Transparency

Ongoing focus on the clarity, completeness, accuracy, and consistency of statements and claims made regarding products and services in related marketing, advertising, disclosures, and communications directed toward the consumer.

Enforcement

Evaluation of whether:

- Products and services are offered on substantially the same terms to all consumers/investors.
- Products/ services are fulfilled consistently as claimed/ marketed and terms/features are clear, prominent, "fair and balanced," and not misleading to a "reasonable" consumer (e.g., use and capabilities of models and automated systems, deposit insurance claims and FDIC logo usage).
- Testimonials, endorsements, and third-party ratings in product/ service advertisements, marketing materials, and/or digital communications (e.g., websites, social media platforms) contain necessary/required disclosures (e.g., payment, affiliation).
- Fees are transparent and meet the requirements of existing laws, nor result in the potential for fraud, waste or abuse (e.g., particularly those in conjunction with government entities)

Consumer Reporting

Information reporting practices, including assessing processes and controls to:

- Ensure information accuracy and integrity and to mitigate against risk of loss of financial access (e.g., credit/debt collection practices.) due to errors or inconsistencies in reports.
- Provide consumers the opportunity to correct false or fraudulent information.
- Ensure timely investigations into issues (e.g., consumer complaints, unauthorized inquiries).
- Safeguard consumers against fraud, identity theft, and other scams/ risks.

"Harm"

Access

Internal Controls

"Harm"

Actions

Regulators expect companies to proactively and actively assess and mitigate the risk of harm to consumers/investors – both financial and non-financial - through their conduct, products, and services from a variety of perspectives including through design, terms, communications/ marketing, and support/ complaints management.

"Harmed Parties"

Regulators may ascertain potential and actual consumer harms through:

- Identification of potentially "harmed parties."
- Efforts to gauge the size/scale of potential impacts.
- Timeliness with which issues are identified, escalated, and resolved.
- Clarity of communications with "harmed parties."
- Remediation and/or restitution.
- Analysis of root causes and related accountability.

Notably, as AI systems develop, the Administration and regulators are expected to focus more on trusted systems and potential security risks (e.g., cyber, privacy and national security) and less on "AI harms".

Divergence

Regulators will continue to focus on complaints, claims, and disputes as a measure of "fair treatment," evaluating the timeliness, substance, and completeness of responses, as well as the consistency of responses between consumer groups and the level of responsiveness/ fair remediation in disputes.

With regard to fraud-related disputes and investigations, regulators continue to focus on areas such as data sharing (e.g., large data models, data sharing with third parties and affiliates, customer permissioned sharing), payments authentication procedures, model development and validation, account holds and freezes, and ongoing oversight and monitoring of synthetic identity fraud.

Actions

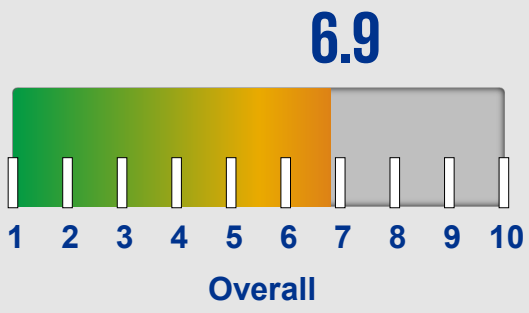
- **Access and Consumer Impact:** Consider the impact of services at large and enhance access to a broader range of consumers in line with existing regulations and regulatory changes, and areas of focus anticipated under the new Administration.
- **Appropriate Sales Practices:** Confirm marketing and promotions are not misleading.
- **Organization Disclosure:** Ensure consumer commitments are upheld and that disclosures are clear, accurate, and transparent.
- **The Consumer Lifecycle:** Assess the consumer journey (i.e., marketing, originations, services, default), as well as use/dependencies of third parties/nth parties in the provision of goods and services to the consumer.
- **Use of AI and Machine Learning:** Develop standard principles that support the deployment of thoughtful, unbiased, and explainable AI.

Financial & Operational Resiliency

The probability and potential impact of disruptions has increased driven by evolving technologies and a growing interconnectedness between financial and nonfinancial companies. Cross-agency regulatory focus on demonstrable financial and operational risk management capabilities will likely continue in 2025 inclusive of the ability to prepare for and withstand or recover from "shocks" as well as adapt to longer-term change.

Efforts to impose more stringent capital and liquidity requirements, however, may abate. Companies are, and will continue to be, required to take a risk-based approach to managing critical operations, third parties and disruptions/incident response while also establishing separate credible plans to maintain business continuity and to consider potential resolution in the event of severe distress .

Regulatory Barometer



5.3	6.9	8.0
Volume	Complexity	Impact

-1.7	⟷	⟷
Shift	Legal	State

Expanding Resiliency

In addition to concerns about the pressures that market stresses or adverse events—disruptions—can put on capital levels and liquidity sources, financial services regulators are now also focusing attention on companies' operational resilience and preparedness to withstand or recover from disruption.

In 2025 regulators are expected to focus on:

Capital

Ongoing efforts to finalize amendments to the large bank capital requirements (Category I to IV banking organizations) may be delayed or fully tabled. Regulators via supervision may also look to related areas of:

- Governance processes, data, models, system infrastructure, internal controls, and regulatory reporting.
- Stress testing frameworks, capital planning, and balance sheet management.

Liquidity & Funding

Ongoing attention to liquidity risk management, including:

- The diversity and stability of funding sources (to ensure resilience under adverse conditions).
- Operational readiness across the crisis continuum (i.e., early warning indicators to contingency funding to reverse repurchase agreements), including procedure knowledge and collateral availability.
- Integrated and effective early warning indicators and regularly updated contingency funding plans based on market shifts or strategic changes.
- Cost of funds vs cost of lending.

Potential changes to the current liquidity framework that may be considered/ carry forward to 2025 include consideration of:

- Minimum requirements for a readily available pool of reserves and pre-positioned collateral at the discount window.
- Partial limits on the extent of reliance on held-to-maturity assets in liquidity buffers.
- Recalibration of the deposit outflow assumptions for different types of depositors.
- Changes to the scope of application (e.g., lowering the asset thresholds).

Operational Resilience

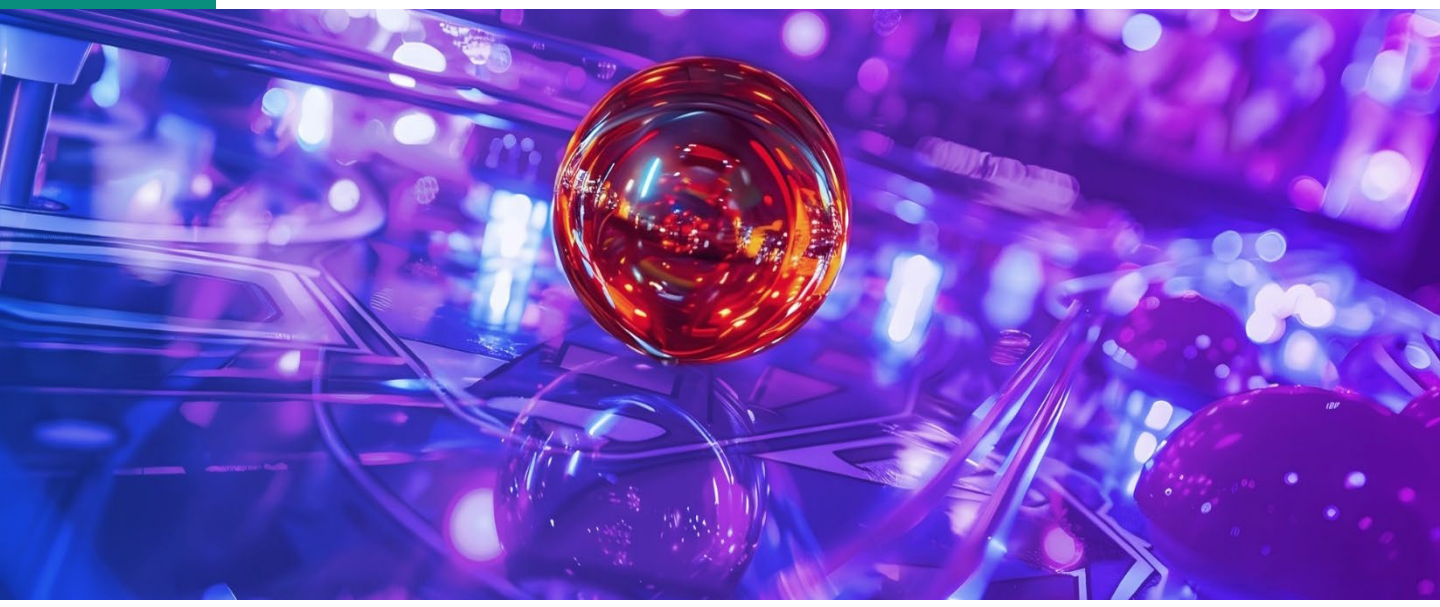
The growing threat landscape, potential failure points, and links between operational resilience and other areas of non-financial risk management (e.g., TPRM, cybersecurity) for large financial organizations as well as potential changes to supervision and oversight for large banks across risk pillars (e.g., credit, market, strategic, operational, legal, and reputational). Considerations include:

- A focus on critical operations and third parties that support them.
- Minimum requirements for critical operations, such as:
  - Clear definitions for identifying “critical activities” and core business lines.
  - Tolerance(s) for disruption informed by risk appetite, scenario analysis, and recovery maps.
  - Scenario testing to inform tolerance parameters and understand interconnections and interdependencies.
  - Governance and risk management practices, including TPRM, communications and reporting, business continuity management, and operational risk management.

Recovery/Continuity

The reasonableness and credibility of contingency and business continuity planning to preserve ongoing operations and limit losses during severe stress/ disruption scenarios given financial and nonfinancial risks and impacts. Elements of the regulators’ focus will include:

- Identification of resources (i.e., people, processes, technology, facilities, and information) required for critical operations and core business lines.
- Readiness to respond to most likely risk scenarios and coordination or response between tactical teams such as Business Continuity, Disaster Recovery, and Cyber and Crisis Management.
- Disaster recovery and business continuity testing with third parties associated with critical operations and core business lines when possible.
- Communications with internal and external stakeholders.
- Integration of risk management systems into organizational structures and decision-making processes to reduce the likelihood of operational incidents and limit losses in the event of business disruption.



Continuity & Resolution

Regulators are looking for companies to demonstrate that they have planned for and are prepared to weather stresses to their operations, including establishing recovery plans designed to continue business following adverse events (e.g., natural disaster, technology failures, human error) as well as resolution plans designed to carry out various steps (e.g., mergers, divestitures, dissolution) in cases where a company is in material financial distress or failure.

Business Continuity Plans

Regulatory focus is on the adequacy and effectiveness of contingency and business continuity planning to ensure ongoing operations and limit losses during severe business disruptions, including:

- Planning appropriate to size, risk profile, activities, complexity (e.g., vulnerabilities, recovery options/barriers, impact assessments, escalation procedures, communications and reporting).
- Identification of known and emerging threats, vulnerabilities, and triggers.
- Identification of resources (e.g., people, processes, technologies, critical third parties) necessary to perform critical operations and/or deliver core business lines within defined disruption tolerances and options for recovery (including execution and timing).
- Assessment of impacts and results of disaster recovery and business continuity testing (both in-house and with third parties, conducted periodically and modified as needed based on the impact assessments with tracking for remediation of identified gaps) related to critical operations and core business lines as well as to material entities and potential obstacles (e.g., legal, market, regulatory).

Resolution Plans

Expectations around robust planning, documentation, and reporting for potential rapid and orderly resolution in case of insolvency or failure. Regulators will focus on many elements in the resolution planning process including:

- Identified strategy for resolution (e.g., single or multiple point of entry), the separability of parts, and the viability of the chosen strategy.
- Failure scenario(s) for testing based on assessments of vulnerabilities, such as capital, liquidity, operational issues, etc.
- Organizational structure (e.g., legal entities, core business lines, affiliates, cross-border) and governance mechanisms (e.g., .
- Critical operations and services, core business lines, and franchise components (if applicable), as well as associated key personnel.
- Capital structure, funding sources, asset portfolios, valuations, off-balance sheet exposures, etc. (if applicable).
- Information systems, licenses, intellectual property, digital services and platforms.

Tolerance & Testing

Disruption tolerances—coupled with rigorous scenario testing and robust third-party oversight—form the cornerstone for safeguarding companies and their critical operations and core business lines/services against severe but plausible risks. Operational resilience transcends all risk pillars (e.g., credit, market, strategic, operational, legal, and reputational) and these should be factored into analysis and review/testing.

In 2025, regulators will be assessing:

Tolerance(s) for Disruption

Set at both the enterprise level and for identified critical operations and core business lines, considering:

- Risk appetite for weathering disruption from operational risks given risk profile and capabilities of supporting operational environment (e.g., systems, processes, expertise).
- Scenario analysis and recovery maps.
- Board approval/oversight of identified critical operations, core business lines, tolerance testing, evaluation, and validation.

Scenario Testing

With emphasis on testing failure scenarios that demonstrate material financial distress. Focus remains on:

- The ability to remain within set tolerances through severe, but plausible, disruption scenarios including potential risks identified through operational risk management, the internal audit function, business continuity planning, and resolution/ recovery planning.
- Understanding interconnections and interdependencies within and across critical business operations and services, and core business lines and capabilities, including third-party risks and critical technology services.

Parties & Providers

Ongoing expectations for governance and risk management of third-party arrangements, particularly those associated with critical operations and services or core business lines. Regulators will expect:

- Third-party relationships to not compromise the ability to perform critical operations and deliver core businesses within disruption tolerances.
- Verification that third parties have sound risk management practices and controls to mitigate disruption consistent with the tolerance level.
- Identification of additional/alternative third parties that may be able to assist if the current third party cannot deliver services including consideration of transition timeframes; data-related risks; joint intellectual property; and potential impacts to customers.
- Risk-based oversight, such that more rigorous oversight is afforded third parties that support higher-risk and critical activities.

Actions

Strengthen Operational Resilience:

- Focus on identifying and protecting critical operations and core business lines through rigorous scenario testing and validation against severe but plausible disruption scenarios.
- Invest in security measures and risk management practices to safeguard against potential threats and minimize the impact of disruptions, including identifying alternative paths/providers.

Improve Governance and Risk Management:

- Ensure that Boards and senior management are actively involved in approving the identification of critical operations, setting disruption tolerances, and overseeing the periodic review and testing of operational risks and resilience strategies.
- Prioritize investments in technologies and cultural changes that enhance operational resilience and establish clear accountability for managing resilience across the organization. Integrate technology-specific resilience measures into risk management frameworks. Develop adaptive strategies to withstand technological disruptions and regularly test and update continuity plans.

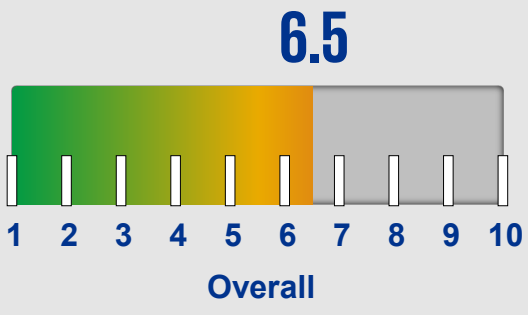
Enhance Business Continuity and Disaster Recovery Planning:

- Regularly update and test business continuity and disaster recovery plans and risk/impact assessments, including those involving third parties, to ensure they are adequate to sustain operations during severe disruptions.
- Integrate operational risk management into organizational decision-making, with a focus on identifying and mitigating risks associated with business processes, technology, and third-party engagements.

Parties & Providers

Given increasing reliance on and complexities in third-party/provider relationships as well as growing interdependencies and interconnectedness between and among companies and industries, regulators will continue to assess risks for supervised companies across such areas as compliance, fraud/waste, data management, cybersecurity, financial crimes, and fairness. Supervision and enforcement in 2025 is likely to focus on risk management oversight practices (throughout the relationship lifecycle and particularly to "critical" providers/relationships) and may also focus directly on service and technology providers as well as government provisions and reporting.

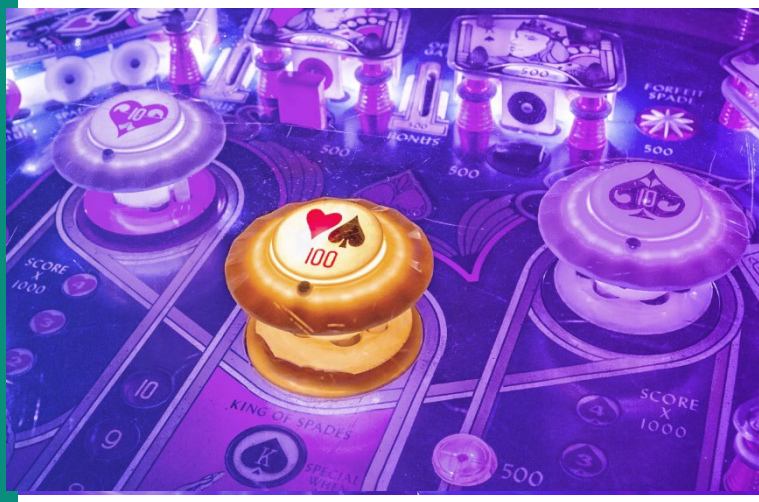
Regulatory Barometer



6.2 Volume	6.7 Complexity	6.6 Impact
-1.8 Shift	Legal	State

Risk Coverage

The scope of third parties, providers and related business arrangements is broad, encompassing direct, indirect, and "nth" party relationships. Such complexity elevates risks to companies and their customers and may draw heightened attention from regulators (and sometimes the public.)



- Data practices, including use and security of customer information (e.g., data collection, ownership, access, use, maintenance, protection and security, and deletion).
- New or novel arrangements and features (e.g., bank-nonbank/fintech arrangements with long chains of providers).
- Comprehensiveness and clarity of contracts, tailored to the nature and scope of the arrangement and including delineation of responsibilities, performance measures, data obligations (e.g., access, ownership), adaptive clauses for changing regulatory requirements and/or market conditions, and terms related to default and termination.

Regulatory Pressure

Driven by increasing dependencies and interconnections between companies, as well as the complex ecosystems underlying the delivery mechanisms to customers, regulators will continue to assess third-party risk management expectations/pressures with a focus on:

- Risk-based management (i.e., based on the size, complexity, and risk profile of the company and the nature of the relationship with the third party), with more rigorous oversight of third parties supporting "higher risk" or "critical activities."
- Contingency plans for replacing third parties as needed.
- Risks associated with the non-delivery of goods and services by third parties (e.g., reputation, compliance, and strategic risk related to a third party's failure to perform as agreed).

Supervisory & Stakeholder Focus

Stakeholders and regulators are particularly focused on:

- Arrangements supporting "critical activities."
- Elements supporting operational resiliency (e.g., tolerance for provider / supply chain disruptions; incident response/business continuity plans; scenario testing/validation of interconnections/interdependencies).
- Financial and compliance risks.
- Reputational risks (e.g., ethical, sustainable supply chain).

Key features of "critical activities" might include activities that: i) pose significant risk to the company if it fails to meet expected agreements, ii) have significant customer impacts, or iii) have significant impact on the company's financial condition or operations.

Risk-Based Approach

Under a risk-based approach, companies will be expected to establish strategic plans for managing third-party and provider risks, focusing on due diligence, oversight, and governance throughout the relationship lifecycle.

Relationship Lifecycle

Consistent management of risk across the company and throughout the relationship lifecycle, irrespective of the type of relationship or activities involved. Key features include:

- An assessment of risk for each third-party relationship (during planning, due diligence, selection, contract negotiation, and monitoring), tailored to the specific size, complexity, and risk profile of the company and the nature of the relationship with the third party.
- Ranking of each third-party and provider arrangement based on the risk posed to the company, with parties and providers involved in “higher risk” and “critical activities” (as defined by the company) subject to more rigorous oversight.
- Alignment with procurement and vendor management activities for risk management consistency.

Governance

The proliferation of available consumer data, the volume of Clear oversight and accountability mechanisms regardless of how TPRM and governance processes are structured (e.g., dispersed across business lines or centralized under specific function(s)). Regulators will look for key governance practices (commensurate with size, risk, and complexity) including:

- Delineation of roles, responsibilities, performance metrics, and standards for the Board and management.
- Board approval of the TPRM program, risk appetite, disruption tolerances, and, in some cases, the selection of third parties supporting “higher risk” and “critical activities.”
- Board participation in the strategic plan.
- Periodic independent audits of the TRPM program.
- Documentation/reporting channels both within the company and to/from third parties.

Regulators will assess:

Strategic Plan

A strategic plan to direct the TPRM program for all party and provider relationships, including the allocation of resources, establishment of infrastructure, implementation of technology controls, and enhancement of organizational capabilities. Third-party relationships / arrangements are reevaluated through ongoing monitoring to discern whether they continue to align with the company’s strategic plan/goals.

Monitoring & Metrics

Due diligence, risk assessments, continuous monitoring, and informative performance indicators and metrics are essential to managing third-party relationships, and in facilitating strategic alignment throughout the relationship lifecycle.

Due Diligence

Relationships with parties and providers should align with the strategic goals, business objectives, and risk appetite of a company. Companies will be expected to assess, and document their capability to identify, monitor, and control the risks posed by a party/provider, commensurate with the level of risk and complexity of the relationship, taking into account the party's/provider's:

- Business strategies, goals, relevant experience, and legal/ regulatory compliance.
- Ownership structure and financial condition.
- Human resources (e.g., staffing, experience, culture).
- Governance and risk management, including cyber/ information security.
- Reliance on other parties (e.g., subcontractors).

Monitoring

On an ongoing basis, companies will be expected to evaluate a third party's/provider's practices and adherence to company policies, standards, and thresholds; a key area of focus will be the controls related to sensitive systems or data. Regulators will likely expect companies to be able to demonstrate:

- Confirmation of the quality and sustainability of a third-party's practices and controls, escalation of significant issues or concerns, and appropriate response when identified.
- Evaluation of the effectiveness of the third-party relationship, including whether it continues to align with the company's strategic goals, business objectives, risk appetite.
- Periodic (or more frequent, where appropriate) monitoring for third-party relationships that support "higher risk" activities, including "critical activities."

Performance Measurement

Regulators are emphasizing the need to assess the effectiveness of both individual third-party relationships, and the entire TPRM program through metrics such as dynamic risk thresholds; key performance indicators; and scorecards to align/measure compliance with service-level agreements, contractual provisions, regulatory expectations, and legal requirements. These measures should be in line with company policies and procedures and serve as a framework for evaluating and maintaining the integrity of third-party relationships.

Actions

Centralize Oversight and Governance: Firms should utilize a multidisciplinary approach to risk management of parties/providers ("TPRM") by adopting a "hub and spoke model" to facilitate comprehensive identification and mitigation of risks and enable independent oversight of the TPRM function. The TPRM function would act as a hub with a central leadership team responsible for setting policies, standards, reporting and risk appetite of its operation, and would be supported by subject matter experts from relevant risk domains (e.g., privacy, cyber, BC, DR, etc.) to provide insights and execution while coordinating across the business line "spokes." Alignment and integration with procurement and vendor management practices to drive consistency in execution is key.

Employ a Risk-Based Approach: Adopting a risk-based approach is paramount to drive efficiency across the relationship lifecycle. This approach involves focusing efforts on third parties/ providers that pose the highest risk to the company, based on factors such as data access, service criticality, operational resiliency, and regulatory impact.

Enrich data associated with service: In order to adopt a risk-based approach, it is important to gather the right data about the service up front in terms of how the service will be delivered and controlled (e.g. What process steps will service support?; What products are dependent on party/provider for delivery?; What controls at the third party will manage risk and compliance requirements? Are subcontractors involved in delivery? Will Artificial Intelligence be used in delivery of service?)

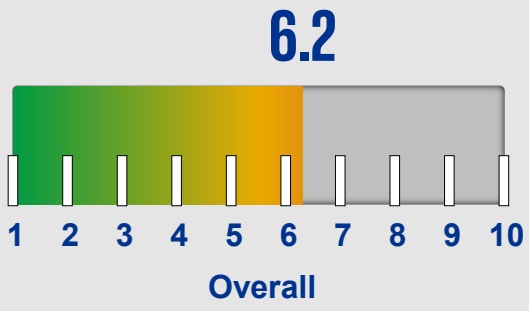
Develop Strong Ongoing Monitoring: To ensure that party/provider risk is accurately measured and mitigated, firms need to perform ongoing monitoring of party/provider risk profiles and contract performance. Risks assessments should incorporate a comprehensive inventory of risks based on direct experience, market developments, and/or strategic business changes, and be conducted during the contracting phase and refreshed on a regular basis. (For example: Develop cloud governance programs aligned with cybersecurity strategies. Tailor security measures to address the unique risks of multi-cloud environments and enhance monitoring of cloud-based incidents.)

Ensure TPRM meets or exceeds global and jurisdictional regulatory expectations: The location of a party/provider (and supply chain providers) does not relieve the company of its responsibility for compliance with all applicable laws and regulations, including ensuring that the party/provider also meets those obligations.

Governance & Controls

Companies will need to continue to act on prior regulatory findings in the area of heightened risk management and governance amidst changing levels of regulatory intensity. Companies will continue to be held to high expectations to enhance risk controls in areas such as cybersecurity, information protection, AI, and financial crime. However, investigations and enforcement actions related to corporate compliance, voluntary self-disclosures of misconduct, risk management programs, and individual accountability, though important, are anticipated to likely decrease in 2025.

Regulatory Barometer



5.9 Volume	6.3 Complexity	6.3 Impact
-0.3 Shift	Legal	State

Controls

As the complexity of the business operating environment increases, regulators expect a company's governance and controls frameworks to fully incorporate policies and procedures that provide reasonable assurance of effective risk mitigation, efficient operations, reliable financial reporting, and compliance with laws and regulations.

Governance

The governance framework is comprised of the rules and practices by which the board ensures transparency, fairness, and accountability in how a company operates and communicates with its stakeholders. Regulators will assess the:

- Clarity of roles, responsibilities, ownership, and accountability across all lines of business, Compliance, and Audit (i.e., three lines of defense).
- Appropriateness of talent management, including skills development, recruitment, succession planning, and training (e.g., staffing to develop/deploy AI and other systems).
- Stature-afforded risk functions (e.g., autonomy, empowerment, visibility).
- Evidence of credible challenge and dynamic risk assessment in support of the design, effectiveness, and sustainability of risk controls.

Coverage & Quality

Key areas of regulatory interest include the:

- Alignment of controls with the risk assessment results.
- Content and quality of the controls inventory (e.g., right controls).
- Adequacy, coverage, and effectiveness of controls testing as well as timeliness to remediate identified gaps and efforts to converge testing functions and/or streamline redundancies/overlaps while ensuring risk and compliance critical challenge.
- Integration of controls with risk assessments and the ability to demonstrate actions taken (e.g., enhancements) based on assessment insights or events and/or failures.
- Demonstrable efforts to guard against overconfidence and "risk complacency".

Data

Regulators are intensifying their scrutiny of companies' data management and data governance practices over risk management data, from aggregation capabilities to internal risk reporting practices. This focus on RDARR (risk data aggregation and risk reporting) is part of the regulators' increasing supervisory and enforcement activities in areas of both financial and non-financial risk. Areas of heightened supervisory focus, where companies are expected to both demonstrate existing and sustainable control elements, include data:

- Assessment of data risks associated with RDARR, with associated data risk taxonomy and minimum control requirements.
- Processes and controls for understanding the data sources and also around data access, authorization, use, privacy, security, and sharing.
- Deficiencies in data, data outputs, or reporting (e.g., data quality, timeliness, accuracy, traceability, metrics, models).
- Data management, including access controls; practices related to collection, retention, disposal; third-party governance/agreements; and reporting capabilities at the lines of business and enterprise levels.
- Companies' ability to train, recruit, and retain, skilled talent resources to identify, measure, manage data risk management processes.
- Model risk management and TPRM with regard to advanced technologies/AI.

Universe & Tiering

An assessment of the adequacy of the scope and breadth of the "data universe" including:

- The types of data and reports covered by the RDARR standard, including metrics, models and reporting (e.g., risk, regulatory, compliance).
- Whether data classification, tiering, and risk ratings reflect the sensitivity, integrity, availability, and criticality of the data to the company.

Governance & Management

Expectations around data governance and management will include:

- Clearly defined and formalized documentation of the governance model (i.e., roles, responsibilities, and accountabilities for the board, management, and across the business, Compliance, and Audit; policies, standards, and procedures), including mapping, ownership, and ongoing testing and monitoring of controls.

Lineage

Companies are expected to have robust data lineage controls in order to demonstrate their ability to trace and report on the relationship between data outputs and business processes, sources, and systems of record and origin. Regulators will evaluate the level of process automation and coverage of the entire data flow (e.g., to consolidate data from different business units/ subsidiaries), compensating controls where automation is unavailable, and the accuracy and granularity of the data.

Issues Management

In 2023, financial services regulators noted that supervisory findings were increasing, and that the vast majority of outstanding issues were related to governance and controls. Accordingly, going into 2025, governance and controls are a supervisory priority for individual companies and across the sector, including issues related to operational resilience, cybersecurity, and TPRM.

Heightened Standards

Through effective governance and control processes, regulators expect companies to be able to proactively identify potential issues prior to regulatory, Compliance and/or Internal Audit findings, and to minimize their impact to the company. Heightened expectations are focused on the:

- Completeness and quality of the issues inventory with a focus on root cause identification and analysis, and inclusive of issues associated with third-/nth-party arrangements.
- Demonstrable “risk reduction” across open issues life cycle, and governance throughout the issues management life cycle (e.g., planning, implementation, validation, closure).
- Identification and resolution of issues across business functions and across risk tiering, in addition to associated testing, critical challenges, and validation of sizing, mitigation, and resolution.
- Demonstration and validation of sustainability.

Change Management

Organizations must not only comply with evolving risk management standards but must also maintain resiliency and adaptability through effective change management, a critical feature in continuous process enhancement and strategic risk framework adjustments.

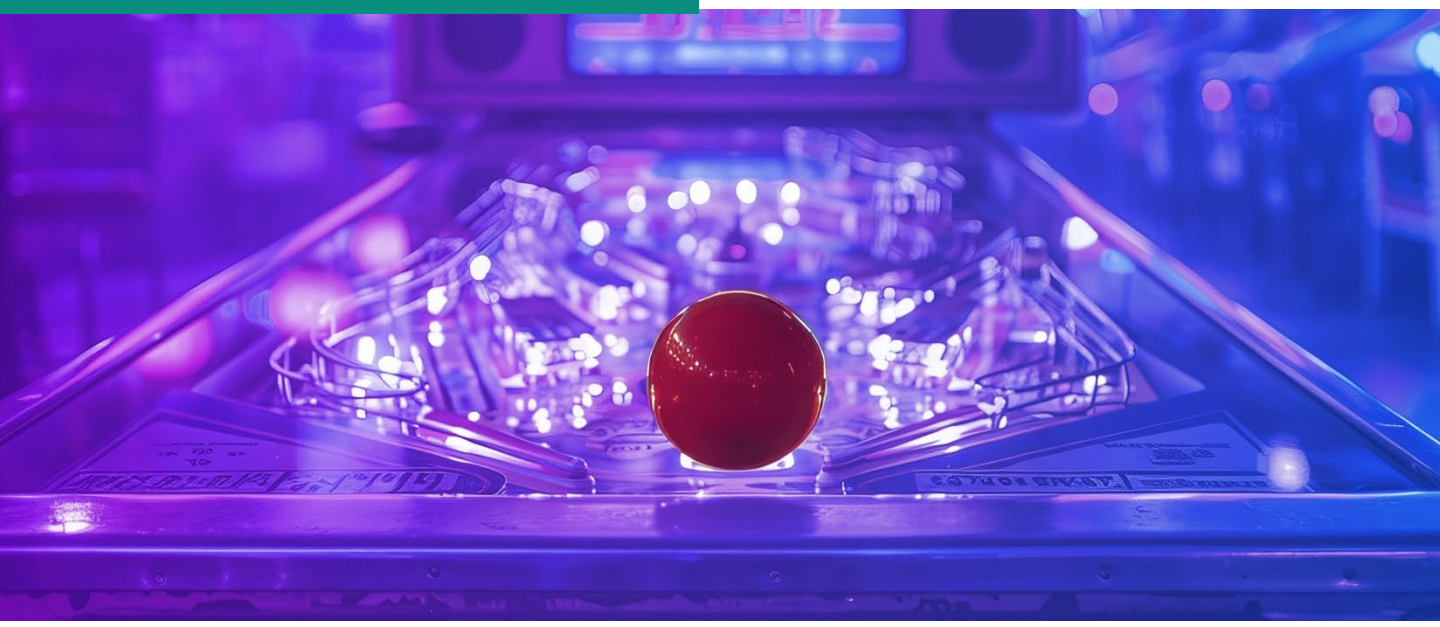
Processes

Anticipate intensifying regulatory pressure on robust change management processes for:

- Completeness and quality of the issues inventory with a focus on root cause identification and analysis, and inclusive of issues associated with third-/nth-party arrangements.
- Demonstrable “risk reduction” across open issues life cycle, and governance throughout the issues management life cycle (e.g., planning, implementation, validation, closure).
- Identification and resolution of issues across business functions and across risk tiering, in addition to associated testing, critical challenges, and validation of sizing, mitigation, and resolution.
- Demonstration and validation of sustainability.

Review & Enhancement

Regulators will look for periodic review of, and changes/enhancements to, the risk management framework to reflect industry developments and other changes to the company's risk profile due to internal or external factors (e.g., new products, M&A, negative news, systems changes, regulatory changes). Regulators will look for risk and controls functions to be a part of continued business, operational, and technology change.



Actions

Strengthen risk and control methodologies: Strengthen methodologies 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, role of independent review / challenge, and remediation measures to address identified deficiencies in a sustainable manner. Ensure that processes are mapped/tied to controls and regulatory and policy requirements.

Review testing coverage: Review overall approach to testing governance and processes (e.g., controls testing, toll-gate testing, substantive/outcome-based testing) with an eye to ensuring proper balance of testing routines as well as increasing / adjusting coverage commensurate with the changing risk profile. Invest in automation, analytics, and process improvements (including methodologies) to meet stakeholder expectations.

Be explicit on standardized data controls: Ensure that there are standardized data controls aligned to data risks. Define clear guidance and scope for the lines of businesses and functions on the application of minimum control requirements and how to operationalize controls expectations.

Reassess issues management: Reassess the issues management process, from definitions, intake, severity levels and processes through clarity to resolution timeliness through issue life cycle. Ensure appropriate Quality Assurance and routine/ongoing critical challenge. Build and utilize root cause, data analytics and trending of issues, with demonstrable incorporation of learnings into risk and compliance enhancements.

Support sustained change: Integrate methods to support change in risk and governance frameworks including critical challenge (e.g., escalation procedures, actions initiated, decisions made, and proof of altered/terminated paths based on risk determinations); document root cause analysis and remediation; automate controls where possible; conduct ongoing monitoring and testing of sustained change.

Position, scale, and reward risk management: Appropriately position, scale, and reward risk management and compliance; hold individuals accountable, incentivize appropriate behavior, and penalize misconduct, including through compensation clawbacks and financial sanctions.

Markets & Competition

1 2 3 4 5 6 7 8 9 10

Market Disruption

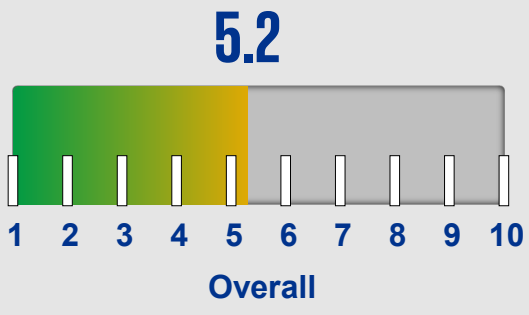
Fair Competition & Trade

Regulatory Perimeter

Actions

Regulators look to promote “fair” market competition and minimize “harmful” competitive impacts through antitrust/ anticompetitive laws. Federal regulators intensified their scrutiny of M&A activities using these laws, and looked to expand their existing authorities, risk standards, and frameworks to include “non-traditional” competitors. A rise in legal challenges disputing regulators’ jurisdictional authorities, coupled with the Loper Bright decision, has limited these efforts; this, in combination with the priorities of the new Administration, may alter the focus on, and pursuit of, antitrust/anti-competitive supervision and enforcement in some industries in 2025. State activity/ scrutiny, however, will likely continue; expect states to focus on managing risks associated with rapid innovation, consumer protection, transparency, and fairness.

Regulatory Barometer



5.6 Volume	5.3 Complexity	5.0 Impact
-1.7 Shift	Legal	State

Market Disruption

In today's dynamic business environment, the landscape of markets and competition is continuously evolving, shaped by a variety of forces such as legislation, regulatory change, M&A activity, new technologies, geopolitical events, and consumer demand. Regulators are concerned with addressing the challenges of market disruption, compliance with antitrust and anti-competition laws, and ensuring that novel market dynamics do not undermine fair competition or consumer interests.

Antitrust/Anticompetition

Market disruptions challenge the status quo of industries and market practices. Across industries, regulators, including enforcement agencies, assess proposed M&A transactions for potential anticompetitive/ adverse outcomes such as:

- Increased costs for consumers, making products and services less affordable/available.
- Limited choices for consumers, as fewer providers operate in the market.
- Suppression of competition or shift toward increased consolidation and/or monopolization, hindering healthy market dynamics.
- A reduction in innovation, as monopolistic entities have less incentive to innovate.
- Elimination of nascent competitors, which can stifle new and innovative market entrants.
- Harms to markets for workers, creators, suppliers, and other providers.

Discord/Instability

Constant flux in market conditions—be it geographic shifts, economic fluctuations, or the rapid adoption of new technologies like Generative AI—as well as increasing interconnectedness of business sectors/industries may place many companies in a reactive or responsive mode to market changes and potentially strain resource allocations and elevate risks.

Fair Competition & Trade

Regulatory efforts to increase transparency, promote fair competition, and ensure consumer and investor protections may ease in 2025, reflecting more favorable policies in some industries toward M&A transactions/reviews and related actions impacting market structure.

In particular:

Mergers & Acquisitions

Reviews of mergers and acquisitions transactions will continue to hinge largely on an evaluation of anticompetitive impacts, (informed by DOJ/FTC Merger Guidelines and Premerger Notification Rules, and FDIC and OCC Merger Policies) nuanced by the priorities of the administration, which may reflect a less stringent interpretation of those policies/positions, including:

- Concentration, measured from various perspectives such as geography, products/services, platforms, or supply chains.
- Competition, potentially including a broader definition of competitors (e.g., geographically relevant, other types of firms, markets for workers, creators, suppliers).
- Convenience and needs of the community, including assessment of impacts to different customer segments and continued availability of comparable products/services.
- Financial and market stability, especially in financial services where regulators may expect the resulting entity to be less financially risky than the individual merging companies and asset size will factor into the competitive analysis.

Anticipate the trajectory of M&A activities to continue to be shaped by macroeconomic conditions, such as interest rates, inflation, the administration's priorities, and geopolitical events.

It is possible that as regulators review proposed M&A transactions, they may coordinate among themselves, aligned by industry (e.g., banking regulators) or with DOJ and/or FTC (e.g., under the 2023 Merger Guidelines), which could introduce some uncertainties to the review process (e.g., differing views on competitive effects, time to review).

Market Structure

Recent actions taken by regulators in an effort to maintain a fair, balanced, and competitive market environment, include:

- Federal/State Rulings: Actions to address antitrust/anticompetition issues related to monopoly power, market consolidation, limitations on consumer choice.
- SEC Market Structure Rules and Amendments: Rules and amendments to improve transparency in retail investment trading and provide retail investors with clear insights into the operations of the market (e.g., best execution, order competition, minimum tick size).
- FDIC and OCC Merger Policy Statements: Reiterating a principles-based standard for evaluating bank mergers, emphasizing a review process to safeguard against adverse impacts to competition and the financial system.
- FTC/DOJ Premerger Notification Rule: Amendments to provide greater insight into potential competitive effects of proposed M&A transactions both horizontally and vertically.

Notably, companies are rapidly innovating and reaching the market at a pace that exceeds regulators' abilities to monitor and manage many of these advancements, potentially leading to a company achieving a dominant position and stifling competition.

Regulatory Perimeter

Market Disruption

Fair Competition & Trade

Regulatory Perimeter

Actions

As markets evolve and change, regulators must adapt. Examples that will likely continue into 2025 include:

Regulatory Expansion

In the financial services sector, banking regulators have looked to expand their supervisory and enforcement activities to encompasses new products/services/activities (e.g., credit, bank-nonbank BAAS agreements) and "non-traditional" competitors (e.g., technology providers, payments providers, fintech and Insurtech companies, and nonbank service providers along with the growing presence of private funds and "shadow banks"). In the short-term this trajectory is likely to continue (though may change in time).

Given the new Administration, expect evolving changes to regulatory contraction/expansion depending on industry and sector.

New Laws and Regulations

In addition to leveraging existing rules and risk standards, individual states are adopting new laws and regulations to address emerging challenges and expand jurisdictional authority in areas such as fair banking practices (e.g., Florida), AI (e.g., Colorado, Tennessee), cybersecurity (e.g., New York), and sustainability (e.g., California, Texas). Often provisions/standards adopted in one state will serve as a model for other states.

Complacency with Growth

Even amidst regulatory change, regulators will continue to focus attention on risk management (financial and non-financial), governance, and controls for companies exhibiting:

- "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).

While innovation and change continue to outpace the regulators, companies should expect regulators to take a retrospective view of risk management and controls compliance.

Actions

- **Regulatory Impact Assessment:** Determine the direct and indirect risks/impacts of applicable regulations and emerging regulatory trends to lines of business, third-party strategy, products, services, and technology and system readiness; execute on changes, as appropriate.
- **Compliance Management:** Evolve risk and compliance programs (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 fair outcomes.
- **Growth and Risk:** Evaluate the relationship between growth and risk coverage to ensure efficient deployment of scarce resources (i.e., gearing ratio).
- **Effects on Competition:** When engaging in M&A activities, ensure preparedness through explainability of both the quantifiable and nonquantifiable effects on competition (e.g., access, product/ service availability, pricing, employment, supply chain resilience). Focus on access to money – through branch and ATM access post any M&A activity.
- **Parties and Providers:** Monitor risk profiles of parties, providers, and intermediaries on a regular basis, including assessment of changes in the business environment (e.g., concentration, interconnectedness via nth parties and supply chains, data ownership); expand party/ provider relationships to prevent over-dependence on one party/ provider or industry and promote market competition; focus on the growth of third party providers who in and of their own service provisions could provide concentration risk (e.g., cloud providers).

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
- **Overall** - 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.
    - **Shift -** difference of overall Barometer score from projected “current state” 2025 to new Administration impacts.

** 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.*

Relevant Thought Leadership

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

Subscribe on LinkedIn
A monthly newsletter for market signals and insight on regulatory, risk, and compliance

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

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

Definition of Terms

- **AI:** Artificial Intelligence
- **AML:** Anti-Money Laundering
- **ATM:** Automated Teller Machine
- **Automated systems:** As defined by CFPB, DOJ, DOC, and EEOC, software and algorithmic processes, including AI
- **BAAS:** Banking As A Service
- **BHC:** Bank Holding Company
- **BSA:** Bank Secrecy Act
- **CDD:** Customer Due Diligence
- **CFPB:** Consumer Financial Protection Bureau
- **CFT:** Countering the Financing of Terrorism
- **CISA:** Cybersecurity And Infrastructure Security Agency
- **DOJ:** Department of Justice
- **EFTA:** Electronic Funds Transfer Act
- **ERM:** Enterprise Risk Management
- **FDIC:** Federal Deposit Insurance Corporation
- **FinCEN:** Financial Crimes Enforcement Network
- **FINRA:** Financial Industry Regulatory Authority
- **FRB:** Federal Reserve Board
- **FTC:** Federal Trade Commission
- **GenAI:** Generative Artificial Intelligence
- **GLBA:** Gramm-Leach-Bliley Act
- **HHS:** Department Of Health and Human Services
- **IAM:** Identity and Access Management
- **IT:** Information Technology
- **ISO:** International Organization for Standardization
- **IRS:** Internal Revenue Service
- **KYB:** "Know Your Business"
- **KYC:** "Know Your Customer"
- **M&A:** Mergers and Acquisitions
- **MFA:** Multifactor Authentication
- **ML:** Machine Learning
- **MRM:** Model Risk Management
- **NIST:** National Institute Of Standards And Technology
- **NLP:** Natural Language Processing
- **OCC:** Office of the Comptroller of the Currency
- **PAM:** Privileged Access Management
- **RFI:** Request For Information
- **PII:** Personally Identifiable Information
- **RDARR:** Risk Data Aggregation and Risk Reporting
- **SAR:** Suspicious Activity Report
- **SEC:** Securities and Exchange Commission
- **SIF:** Synthetic Identity Fraud
- **TCPA:** Telephone Consumer Protection Act
- **TEVV:** Testing, Evaluation, Validation, Verification
- **TPRM:** Third-Party Risk Management
- **UDAAP:** Unfair, Deceptive, or Abusive Acts or Practices
- **UDAP:** Unfair or Deceptive Acts or Practices

Contact

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

01 Regulatory Intensity

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

02 Trusted AI & Systems

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

Bryan McGowan
Principal, Trusted AI Leader,
US Consulting
bmcgowan@kpmg.com

03 Cybersecurity & Information Protection

Mihai Liptak
Managing Director, Cyber & Tech Risk
mliptak@kpmg.com

Mick McGarry
Principal, Cyber & Tech Risk
hmcgarry@kpmg.com

Matt Miller
Principal, Cyber & Tech Risk
matthewpmiller@kpmg.com

04 Financial Crime

Dan Boylan
Principal, Forensic
danielboylan@kpmg.com

John Caruso
Principal, Forensic
johncaruso@kpmg.com

Charlie Jacco
Principal, Cybersecurity
cjacco@kpmg.com

05 Fraud & Scams

Pete Bradford
Managing Director, Forensic
pbradford@KPMG.com

Steve D'Antuono
Partner, Forensic
sdantuono@KPMG.com

Chad Polen
Partner, Regulatory & Compliance
cpolen@kpmg.com

06 Fairness & Protection

Stefan Cooper
Principal, Regulatory & Compliance
stefancooper@kpmg.com

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

07 Financial & Operational Resilience

KB Babar
Principal, Regulatory & Compliance
kbabar@kpmg.com

David Tarabocchia
Principal, CIO Advisory
dtarabocchia@kpmg.com

08 Parties & Providers

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

Jen Shimek
Principal, Forensic
jshimek@kpmg.com

09 Governance & Controls

Joey Gyengo
Principal, Audit & Controls
jgyengo@kpmg.com

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

Tyler Williamson
Managing Director, Cyber & Tech Risk
twilliamson@kpmg.com

10 Markets & Competition

Henry Lacey
Principal, Transaction Strategy
hlacey@KPMG.com

Mike Sullivan
Principal, Regulatory & Compliance
mmsullivan@KPMG.com

Learn about us: **kpmg.com**

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