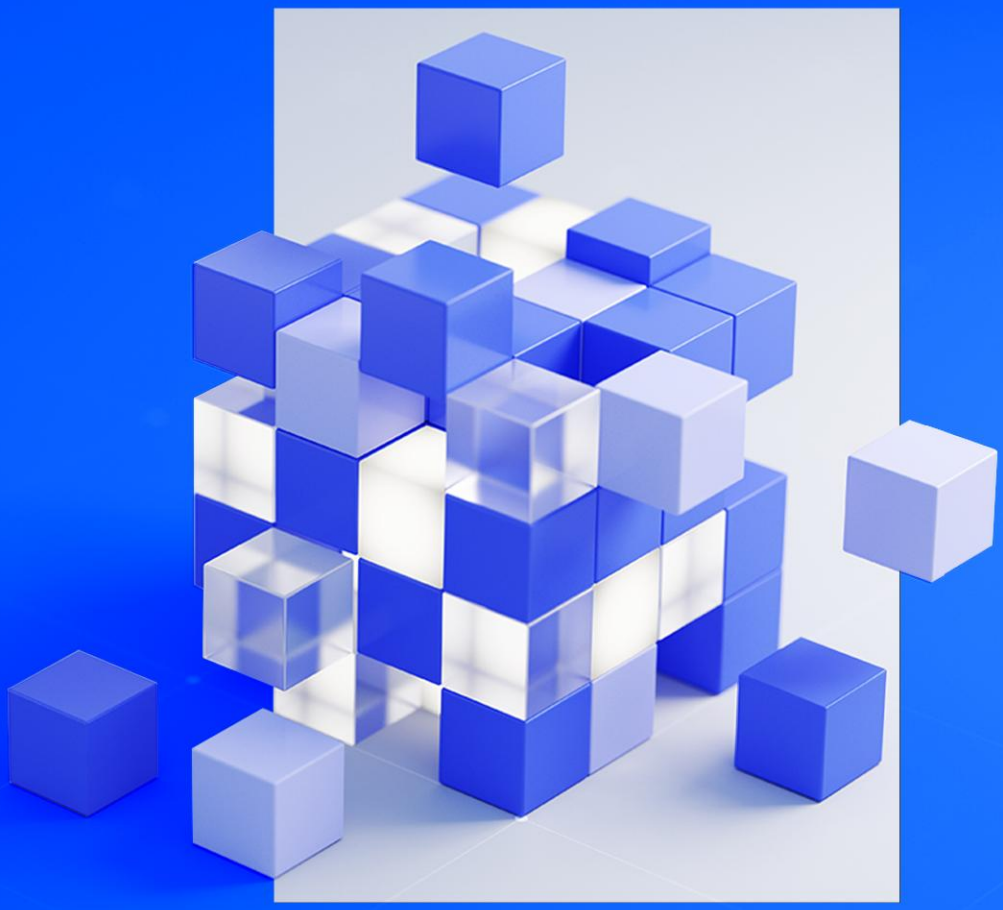
KPMG

Ten key regulatory challenges of 2026 for TMT

Balancing the regulatory stack



Foreword

The Technology, Media, and Telecommunications (TMT) industry is at the forefront of innovation, constantly reshaping how we live, work, and connect. This rapid advancement, however, brings an increasingly complex and fragmented regulatory landscape. Now more than ever, TMT leaders must navigate a delicate balancing act: pursuing groundbreaking innovation while ensuring robust control, maintaining market speed while building long-term resilience, and modernizing for the future while ensuring stability.

This paper delves into the most pressing issues facing the industry. Based on emerging regulatory signals, we have identified ten challenges that are impacting business. From the responsible adoption of disruptive technologies like AI and the ever-present threat to cybersecurity, to the expanding regulatory perimeter that now scrutinizes financial transactions, content moderation, and fraud prevention on tech platforms, the responsibilities of TMT companies have never been greater.

The signals are clear: regulators globally no longer view tech platforms as neutral infrastructure, but as a critical front line in protecting consumers, ensuring market fairness, and even safeguarding national security. This shift demands a new level of proactive engagement and a strategic approach to compliance that is agile enough to adapt to diverging rules across state, federal, and international jurisdictions.

This report provides a vital roadmap for TMT leaders to anticipate and manage these regulatory shifts. By understanding the challenges and embracing the recommended actions outlined within, organizations can not only mitigate risk but also build trust and create sustainable, long-term value. We hope you find it an invaluable resource as you navigate the exciting and challenging road ahead.

Vijay Subramanyam

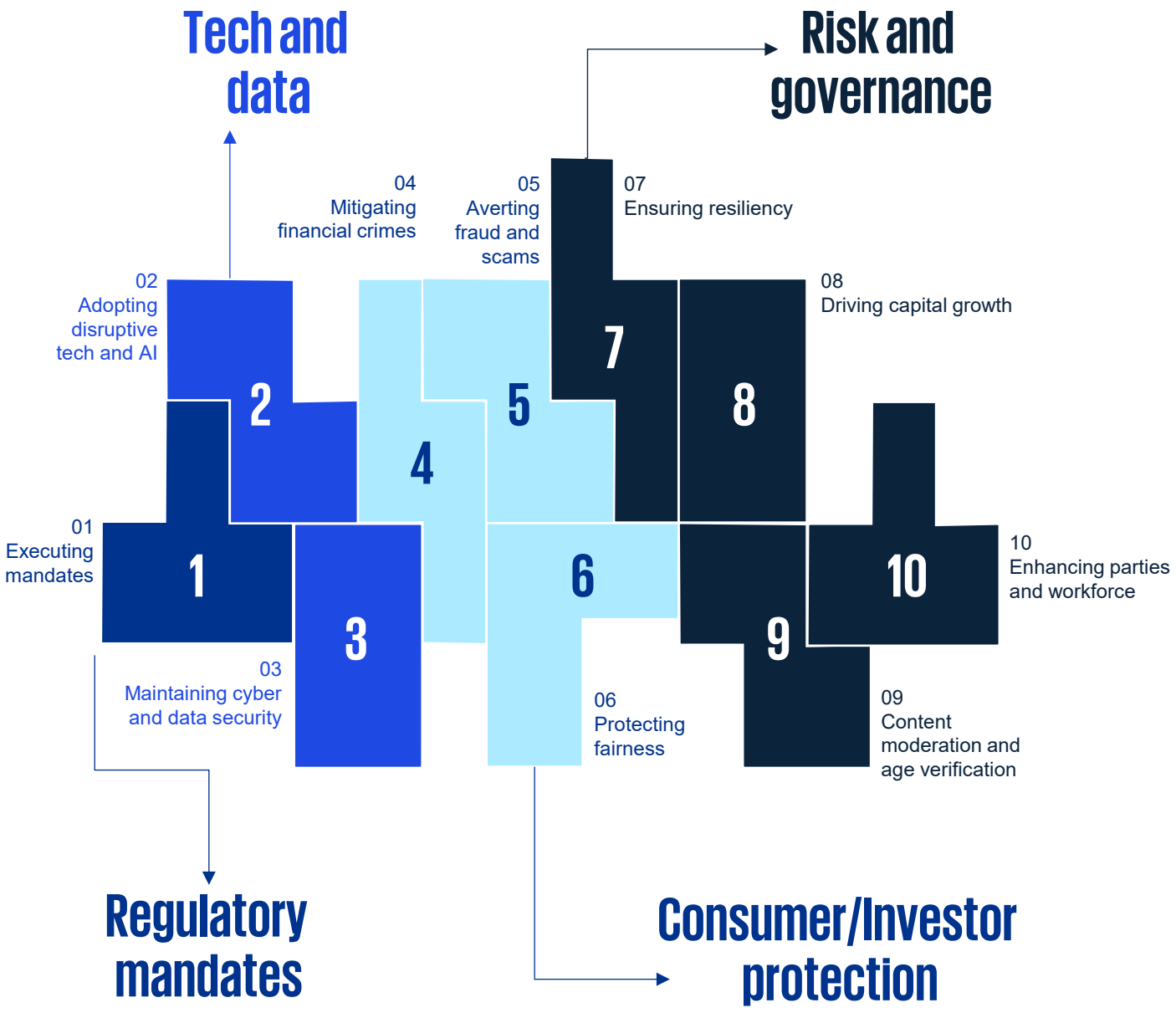
Principal, Advisory
TMT Sector Consulting Leader
vijaysubramanyam@KPMG.com
LinkedIn

Lisa Rawls

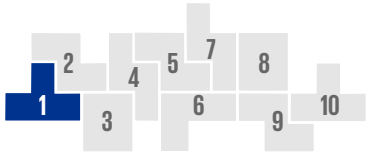
Principal, Advisory
TMT Sector Risk Leader
lisarawls@kpmg.com
LinkedIn

Ten key regulatory challenges of 2026 for TMT

TMT leaders face the challenge of balancing innovation against control, speed against resilience, and modernization against stability. Based on emerging regulatory signals, here are ten key challenges categorized by risk area:



01 Executive mandates



Signal 1

Presidential executive orders

Executive orders have prioritized national security and consumer data protection through new safeguards for AI and digital assets, while also seeking to streamline regulations to foster innovation and secure US leadership in the global digital economy.

What to watch

- Fractured regulatory landscape across state, federal, and global jurisdictions
- Supply chain regulations aimed to remove foreign adversary technology from the telecommunications supply chain
- Increased regulation on the protection of US data, including restrictions on bulk data transfers to “countries of concern.”

Recommended actions

- Design comprehensive risk and compliance programs that can optimize global regulatory coverage while minimizing impact on speed to market.
- Review your third-party risk management program to ensure you are mapping component origins and ensure compliance with national security directives.
- Review your data warehouse inventory and data movement controls to identify and de-risk any exposure to processes that could bulk transfer data to countries of concern.

Signal 2

Regulatory divergence

The US regulatory patchwork of conflicting state laws creates significant compliance friction for Big Tech, especially as federal policy prioritizes innovation over strict oversight. This reliance on self-governance marks a sharp departure from the more prescriptive global standards emerging across Europe and APAC.

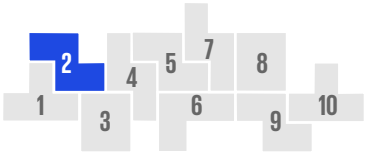
What to watch

- Continued divergence between federal, state, and global regulations
- Rapid growth in regulatory changes across jurisdictions
- Regulations are struggling with the conflict of keeping AI safe with out impeding the ability for Tech firms to ship products quickly.
- Potential streamlining of international laws and regulations

Recommended actions

- Baseline your compliance programs to be agile to answer the complex framework of regulations while still maintaining your own community guidelines.
- Establish benchmarks for online harms to provide a standard of measurement to more accurately quantify and mitigate risk.
- Build control frameworks that give you greater coverage of regulations without creating a large number of new controls.

02 Adopting disruptive tech and AI



Signal 1

Model risk management

Federal banking regulators continue to reiterate that existing guidance and risk frameworks remain fit for purpose in supervising AI applications, but recent statements suggest some revisions may be needed.

What to watch

- Potential revisions to existing model guidance for AI-specific use cases
- Potential enhancements to nonmodel risk frameworks to address transverse risks
- Increasing numbers of bank/fintech relationships; heightened attention to third-party risk management (TPRM)
- Growing acceptance that not all AI is a model
- Consideration of new approaches for AI that is not a model

Recommended actions

- Update model governance standards to explicitly incorporate evaluation, monitoring, and documentation requirements tailored to AI-specific behaviors and risks.
- Embed AI-related risk dimensions—such as data provenance, emergent behavior, and explainability—into existing nonmodel risk frameworks to ensure consistent oversight of risk.
- Strengthen TPRM protocols by requiring enhanced due diligence, continuous monitoring, and contract controls for AI-enabled bank/fintech partnerships.
- Establish clear criteria and guidance to differentiate models from nonmodel AI tools to ensure appropriate and proportional governance.
- Develop a fit-for-purpose oversight approach for nonmodel AI that focuses on lifecycle controls, transparency, and operational risk management rather than traditional model validation.

Signal 2

Complexity and divergence

Divergent actions at the federal and state levels create risk and compliance challenges, such as executive directives promoting national security and innovation while a proliferation of state laws and regulations seek to set guardrails.

What to watch

- Introduction of new laws and regulations that facilitate recommendations in the AI action plan
- Potential revision/rescission of federal rules identified as inhibiting AI innovation and infrastructure
- Ongoing introduction of new laws and regulations with varying scope and scale across all 50 states
- Continued calls for federal preemption or moratoriums on enforcement of certain state AI laws
- Potential for increased risks from inaction in the absence of proactive federal regulatory activity

Recommended actions

- Monitor and assess new federal AI laws and regulations to align internal policies with emerging requirements from the AI action plan.
- Monitor the progress of federal rules that impede AI innovation and build an adaptable strategy that accounts for changes in federal AI rulings.
- Establish a systematic process to track and interpret evolving state-level AI laws to ensure compliance across all jurisdictions.

02 Adopting disruptive tech and AI (continued)

Signal 3

Public-private partnership

Executive policy to create conditions for private sector-led innovation to flourish and enable AI adoption

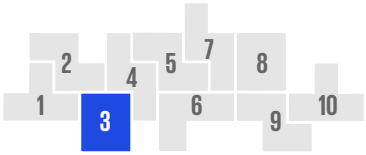
What to watch

- Potential changes to regulatory processes identified by private industry as inhibiting AI innovation
- Availability of regulatory sandboxes across different agencies
- Streamlined permitting for data center and energy infrastructure and other incentives at the federal/state levels
- Stakeholder engagement on a Federal Reserve "payment account" for fintechs

Recommended actions

- Strengthen senior-level engagement with supervisory agencies to shape a more agile regulatory environment that enables the organization to deploy advanced AI capabilities while maintaining trusted risk standards.
- Prioritize long-horizon investments in next-generation compute and energy infrastructure by leveraging federal and state incentives, ensuring the firm has the capacity to scale AI responsibly and competitively.
- Participate in controlled regulatory pilot programs that provide early visibility into supervisory expectations and accelerate our readiness for emerging AI governance models.

03 Maintaining cyber and data security



Signal 1

A tale of evolving threats

The increasing digitization of services expands the attack surface, while the sophistication of threats continues to grow.

What to watch

- The evolution of AI-powered cyber threats, such as automated vulnerability discovery and the use of deepfakes for social engineering
- The emergence of new attack vectors targeting interconnected IoT devices and the software supply chain
- The development of new regulations mandating "secure by design" principles and specific security standards for digital services and AI systems

Recommended actions

- Adopt a "Zero Trust" security architecture that assumes no user or device is inherently trustworthy, requiring verification for every access request.
- Invest in an attack surface management platform and AI-powered threat detection tools to gain visibility and proactively defend the expanding digital footprint.
- Integrate security into the entire software development lifecycle (DevSecOps) to identify and remediate vulnerabilities before services are deployed.
- Conduct regular threat modeling exercises that incorporate potential AI-based attack vectors.

Signal 2

A tale of two continents

The EU has a comprehensive rule-making approach, while the United States relies on an enforcement-led model that is subject to administrative shifts.

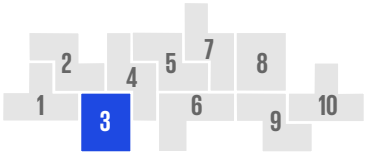
What to watch

- How each EU member state transposes the NIS2 Directive into its national law, as there may be variations
- The first major enforcement actions under the Digital Markets Act (DMA), Digital Services Act (DSA), and the upcoming AI Act to understand how regulators interpret and apply these complex new rulebooks in practice
- Any changes in leadership and stated priorities at US regulatory bodies such as the FTC and DOJ, particularly following administrative shifts; also, watch state developments

Recommended actions

- Begin a thorough gap analysis now to determine how your organization's current security posture measures up against the stringent risk management, incident reporting, and supply chain security requirements of the NIS2 Directive and other global and US regulations.
- Given the shifting nature of US enforcement, build a flexible compliance program based on risk management principles rather than a rigid, rules-based checklist. This allows for adaptation to new priorities without a complete overhaul.
- Establish a governance model with regional expertise. Empower an EU-focused team to manage compliance with the prescriptive rulebooks (NIS2, General Data Protection Regulation (GDPR), AI Act) and a US-focused team to navigate the nuances of state laws and federal enforcement actions.

03 Maintaining cyber and data security (continued)



Signal 3

A tale of sovereignty

Driven by concerns over national security, economic independence, and data privacy, nations are increasingly seeking to control their own digital infrastructure and data, leading to a fragmentation of the global internet.

What to watch

- 5G spectrum allocation as the EU and US have pursued different strategic paths, complicating global network and hardware strategies
- The emergence of data sovereignty laws, such as India's Digital Personal Data Protection Act, that mandate local data storage, driving demand for in-country data centers; increased scrutiny of cross-border data flows and the legal mechanisms that govern them

Recommended actions

- Develop and invest in flexible, multiband hardware and chipset designs that can be software-configured to operate across the different frequency bands prioritized by both the US and the EU.
- Create adaptable product development roadmaps that account for region-specific compliance requirements, especially for AI.
- Establish regional data governance strategies and infrastructure to comply with data sovereignty and localization rules.
- Invest in flexible, hybrid cloud architectures that can accommodate different sovereignty requirements.

Signal 4

A tale of division

In the absence of comprehensive federal legislation in key areas, a growing patchwork of state-level laws for data privacy and AI is creating a complex and costly domestic compliance landscape for technology, media, and telecommunications (TMT) companies. And the executive order may not stop it.

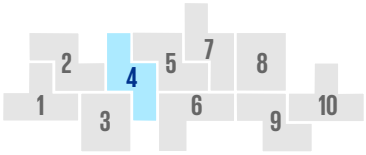
What to watch

- States are beginning to introduce their own AI-specific bills regulating the use of automated decision-making systems, adding to the fragmented legal landscape.
- The definition of what constitutes a "sale" of data differs significantly. For example, some states define it narrowly as a monetary exchange, while others define it to include sharing data for "other valuable consideration," which has major implications for online advertising.
- California's Age-Appropriate Design Code Act (AADC) goes far beyond the federal Children's Online Privacy Protection Act (COPPA). It requires online services likely to be accessed by children to implement a wide range of design changes and data protection features by default.

Recommended actions

- Develop a baseline of "highest common denominator" privacy and AI governance standards that can satisfy the strictest state laws.
- For high-risk applications (such as hiring or credit), prioritize the use of explainable AI. Ensure your teams can reasonably explain how a system arrived at a decision, which is a common requirement in emerging legislation.
- Engineer your websites and applications to recognize and honor universal opt-out signals, such as the Global Privacy Control (GPC). This provides a scalable technical solution to manage opt-out requests across multiple jurisdictions.
- Implement “privacy by default" as the universal standard: If your service is likely to be accessed by minors, configure the product to apply the most protective settings (e.g., location tracking off, public profiles disabled, direct messaging restricted) as the default for all users.

04 Mitigating financial crimes



Signal 1

Modernization

As tech and telecom companies integrate payments, digital wallets, and complex ad economies, they are being pulled into the regulatory perimeter of the BSA/AML framework. Simultaneously, this framework is being reformed to be more "risk-based," focusing on national security priorities. For TMT, this means regulators will apply financial integrity rules to new and evolving services—from ad networks to in-app economies—demanding a sophisticated, risk-based compliance approach where none may have existed before.

What to watch

- Increased scrutiny from FinCEN and other regulators on the role of digital advertising networks as a potential vector for trade-based money laundering
- The extension of sanctions enforcement to cloud service providers and other infrastructure platforms, holding them accountable for hosting wallets or services tied to designated entities
- Growing pressure on telecom carriers to enhance identity verification and security protocols to combat SIM-swap fraud as a critical component of financial crime prevention

Recommended actions

- Map your financial touchpoints: Identify every point where money moves on your platform, from ads and in-app purchases to carrier billing, to define your overall financial crimes risk exposure, and take into account regulated versus unregulated products.
- Calibrate your risk-based approach: Align your compliance programs with FinCEN's national priorities, and focus enhanced diligence on high-risk areas such as digital assets and creator payment ecosystems.
- Vet your fintech partners rigorously: Implement a strict due diligence and ongoing monitoring process for all payment partners to ensure their compliance programs are robust enough to protect your platform from inherited risk.
- Integrate financial crimes signals: Break down silos between your fraud prevention, ad policy, and payment integrity teams to detect potential anomalies that could indicate money laundering, sanctions evasion, or other financial crimes.
- Harden identity and access controls: For telcos, enhance security against SIM-swap attacks. For platforms, strengthen know your customer (KYC) and authentication for all users of payment services to prevent account takeovers that enable financial fraud.

Signal 2

Recalibration

Regulators are recalibrating their focus by adopting the TMT sector's own tools—AI, blockchain analytics, and digital identities—to scrutinize for high-risk financial activity. As traditional bank reporting thresholds may rise, the enforcement lens will sharpen on less-regulated value transfer systems within tech platforms, such as in-app economies and advertising spend, holding them to a higher, tech-driven standard.

What to watch

- FinCEN guidance on the use of AI for transaction monitoring, setting a new compliance standard for tech payment services
- The use of blockchain analytics by OFAC and FinCEN becoming a standard tool to link illicit actors to specific activities on tech platforms
- A push for platforms to adopt verifiable digital identity solutions to strengthen their KYC processes

Recommended actions

- Leverage your tech for compliance: Use your native AI and data analytics capabilities to build real-time monitoring systems for detecting suspicious financial activity on your platform.
- Prepare for digital asset scrutiny: If integrating stablecoins, proactively build a compliance framework that anticipates tailored regulations, including robust transaction monitoring and information sharing capabilities.
- Monitor for displaced financial risk: Be aware that as traditional banking rules change, your platform may become a more attractive target for money launderers. Risk models need to be adjusted accordingly.

04 Mitigating financial crimes (continued)

Signal 3

What to watch

Sanctions

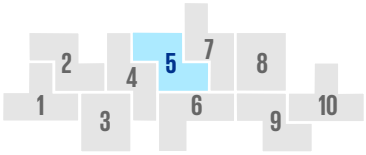
Sanctions are now a primary tool of national security, and the enforcement perimeter has expanded directly to the TMT ecosystem. Tech platforms, cloud providers, and telecom carriers are no longer seen as neutral infrastructure but as a critical front line, expected to actively prevent sanctioned states, companies, and individuals from using their services, software, and networks.

- New OFAC guidance specifically clarifying the sanctions compliance obligations for Cloud Service Providers, app stores, and digital advertising networks
- Sanctions being levied against specific software companies or online platforms as a penalty for failing to block sanctioned actors from their services
- An increased focus on dual-use technologies, requiring TMT firms to prevent their services from being used by sanctioned regimes for military or surveillance purposes

Recommended actions

- Make sanctions a core tech risk: Integrate sanctions list screening into all customer onboarding processes, including for cloud services, app developer accounts, and advertising clients.
- Implement sophisticated geolocation blocking: Move beyond simple IP blocking and invest in technology to detect and block users attempting to circumvent geo-restrictions from sanctioned jurisdictions via VPNs or other anonymizers.
- Monitor for prohibited end-use: Develop risk-based controls to identify customers who may be reselling your services to sanctioned entities or using them for prohibited purposes, such as military or intelligence applications.

05 Averting fraud and scams



Signal 1

Fast and furious

Generative AI is industrializing fraud, allowing criminals to launch sophisticated attacks such as deepfakes, synthetic identify fraud, and automated phishing campaigns at a scale and speed that outpaces traditional defenses. This requires a cohesive and technology-enabled approach to risk fraud management.

What to watch

- Heightened regulatory attention on the effectiveness of fraud detection for AI-generated content, with specific mandates for labeling and watermarking
- Increased pressure on telecom carriers from regulators such as the US FCC to implement AI-powered network analytics to block AI-generated scam calls
- Escalation in scale and sophistication to potentially be considered an issue of national security, leading to regulatory activity
- Forthcoming NACHA fraud monitoring rules for ACH payments

Recommended actions

- Fight AI with AI: Deploy automated, AI-powered defenses to detect and block synthetic media, AI-generated text, and other machine-driven fraud patterns in real time.
- Plan for “deepfake zero hour": Establish a rapid-response protocol to instantly contain viral deepfakes or AI-driven misinformation during a crisis, protecting your brand and users.
- Design for defense: Embed antifraud technologies such as content watermarking and behavioral analytics directly into your product development lifecycle, making security a feature, not an afterthought.
- Verify, then trust: Overhaul your KYC processes with advanced tools to detect and block synthetic identities and AI-generated profiles at onboarding.
- Run AI "fire drills": Conduct regular threat simulations of sophisticated, AI-powered attacks to identify and remediate gaps in your defensive posture before a real event occurs.

Signal 2

Reprioritizing enforcement

In response to public pressure, regulators are shifting the burden of liability from individual fraudsters to the underlying TMT infrastructure. Enforcement now focuses on the failure of platforms and carriers to prevent foreseeable harm, treating this as a core compliance failure.

What to watch

- Broader application of consumer protection laws, such as the EU's Digital Services Act, to hold very large online platforms liable for systemic failures in preventing widespread scams
- Continued enforcement focus on retail investor protections, scrutinizing the misuse of search and social media to promote financial fraud
- Focus on retail investor protections, including false and misleading statements and misuse of technology to commit fraud

Recommended actions

- Build your “duty of care" case: Formally document all proactive steps taken to prevent fraud, creating a defensible record to demonstrate compliance and responsible governance to regulators.
- Make fraud a C-suite issue: Elevate fraud prevention from a back-office policy function to a core compliance mandate, led by a senior executive with clear accountability and authority.
- Create a "no scammers allowed" on-ramp: Implement a rigorous, multi-factor “know your business customer" process to vet all new advertisers and developers before they can access your platform.
- Empower a "scam kill switch“: Authorize a dedicated team to immediately suspend fraudulent campaigns and accounts based on clear evidence, prioritizing user safety over revenue.
- Engage regulators proactively: Don't wait for an inquiry. Openly communicate your antifraud investments and results to key agencies to build trust and help shape practical future regulations.

05 Averting fraud and scams (continued)

Signal 3

Convergence of scams

Modern scams converge across the TMT ecosystem, where a fraudulent ad leads to a malicious text message, which directs to a fake app. Regulators now expect every company in this chain, from the social platform to the telecom carrier, to take responsibility for their link.

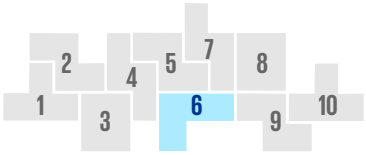
What to watch

- The sophistication and variety of scams will continue to evolve at a quicker pace than regulatory frameworks, meaning bad actors will remain more flexible than regulators.
- New fraud vectors developing around emerging technologies such as tokenized assets and the metaverse (e.g., fake digital products, fraudulent exchanges, and imposter avatars)
- Increasing regulatory requirements for interoperability and data sharing between TMT companies for the express purpose of tracking and mitigating cross-platform fraud campaigns

Recommended actions

- Establish a centralized fraud risk management organization: Break down internal silos by creating a cross-functional team that centralizes intelligence from security, safety, and product teams to get a unified view of threats.
- Join the industry "neighborhood watch": Actively participate in ecosystem-wide threat sharing programs to exchange data on emerging scams and bad actors with other platforms, carriers, and banks.
- Know your link in the "fraud chain": Map exactly how your service is used in common scam lifecycles to identify the single most effective point where you can intervene and break the chain.
- Warn users at the point of risk: Deploy dynamic, real-time warnings and educational pop-ups to users when they encounter high-risk scenarios, such as suspicious links or unsolicited investment advice.
- Automate your "911 call": Build automated pipelines to report identified illegal activity and fraudulent actors directly to the appropriate law enforcement agencies, demonstrating good faith and accelerating action.

06 Protecting fairness



Signal 1

Fair to the consumer

Prioritize transparent data practices and ethical conduct, which is essential to navigate increasing regulatory scrutiny and maintain customer trust.

What to watch

- Global data privacy regulations for embedding "Data Privacy by Design" in all processes
- Regulatory expectations for data integrity and implementing robust data governance
- Consumer and regulatory demands to ensure responsible content

Recommended actions

- Mandate privacy impact assessments for all new projects. Embed privacy experts in development teams to ensure data minimization, user consent, and security controls are built into every product from concept to launch, meeting global standards such as GDPR.
- Establish a central data governance council with leaders from Legal, IT, and business units. Task them with creating a master data catalog, defining data quality standards, and assigning clear ownership for all critical data domains to ensure integrity.
- Develop a public content moderation framework with clear standards for prohibited content. Implement a transparent, multitiered appeals process for users to challenge decisions and publish regular reports to demonstrate fairness and accountability.

Signal 2

Fairness access

Proactively address regulatory policies such as net neutrality, and ensure AI and service delivery models are nondiscriminatory to maintain market acceptance and avoid legal challenges.

What to watch

- Digital platforms and AI interfaces that are accessible to people with disabilities
- Shifting government policies and potential reforms regarding net neutrality

Recommended actions

- Mandate adherence to Web Content Accessibility Guidelines for all products. Combine automated testing in development pipelines with regular manual audits by accessibility experts and users with disabilities to ensure genuine usability beyond baseline compliance.
- Task your public policy team with tracking net neutrality legislation and regulatory dockets. Develop scenario-based playbooks for network management and pricing to ensure the business can quickly adapt to potential rules on paid prioritization, throttling, or other issues.

06 Protecting fairness (continued)

Signal 3

What to watch

Digital fairness

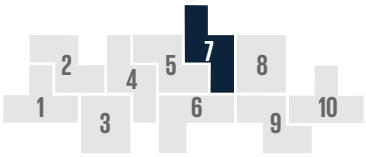
Digital fairness signals that integrating consumer protection, fair access, and ethical AI into core business strategy is essential for long-term viability in a globally scrutinized market.

- Consumer protection and fairness for core risk management frameworks to reduce legal exposure and regulatory risk
- New AI laws and public demand for establishing robust AI governance
- Tension between government and user rights, balancing lawful government requests with user privacy commitments through clear, published transparency reports and policies

Recommended actions

- Update your enterprise risk management framework to add consumer fairness as a formal risk category. Require business units to identify and report on risks such as algorithmic bias and dark patterns as part of their standard quarterly reviews.
- Create a cross-functional AI governance committee with executive authority. Task them with maintaining an AI model inventory, set firmwide standards for development, and implement a mandatory ethical review process for all high-risk AI systems before deployment.
- Create a strict, lawful request policy defining clear criteria for validating government data demands. Publish a biannual transparency report detailing the volume and type of requests received globally, and what percentage of those resulted in data disclosure.

07 Ensuring resiliency



Signal 1

Business continuity and resiliency planning

In response to increasing threats to information and technology security and complex interdependencies, regulators expect organizations to create plans to address critical functions, service-level agreements, and significant disruptions.

What to watch

- Risk assessment and management: Identify, assess, and manage risks such as cyber threats and infrastructure failures.
- Redundancy and failover systems: Ensure systems have redundancy and failover capabilities to maintain operations during disruptions.
- Cybersecurity and data protection: Strengthen cybersecurity measures and establish robust data protection and recovery protocols.
- Crisis management and communication: Develop and regularly update crisis management frameworks and communication plans.

Recommended actions

- Conduct regular risk assessments, implement mitigation strategies, and update plans based on emerging threats.
- Implement and regularly test failover systems and maintain redundant infrastructure.
- Conduct security audits, enforce advanced cybersecurity measures, and ensure effective data backup and recovery.
- Rehearse crisis response through regular drills, designate communication teams, and ensure clear communication channels.

Signal 2

Technology interconnectedness

Elevated levels of operational risk reinforce the importance of operational and technology resilience, business continuity and incident response plans.

What to watch

- Dependency mapping: Understand the dependencies between internal systems and external services and how interconnected technologies are linked.
- Interoperability and standards: Ensure that systems are interoperable and comply with industry standards to facilitate seamless integration and operation.
- Network resilience: Assess and strengthen network resilience to ensure continuous operation despite connectivity disruptions or failures.
- Third-party and cloud services management: Manage risks associated with third-party services and cloud providers that are integral to business operations.

Recommended actions

- Create detailed maps of system dependencies, both internal and external, and regularly review and update these maps to reflect changes and/or updates.
- Adopt and implement industry standards/protocols and perform regular testing to ensure interoperability among systems.
- Establish robust network redundancy, conduct stress testing, and deploy distributed networks to enhance resilience against failures.
- Establish strong vendor management practices, conduct regular assessments of third-party risks, and have contingency plans for provider disruptions.

07 Ensuring resiliency (continued)

Signal 3

Data centers

As critical hubs for information storage and processing, data centers must prioritize reliability, efficiency, and security. Ensuring robust energy management, optimal environmental controls, stringent physical security measures, and comprehensive disaster recovery strategies are essential to maintaining operational continuity and safeguarding critical data.

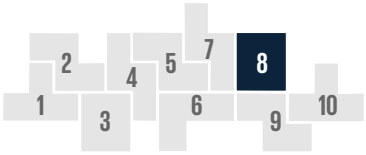
What to watch

- Data center build strategy: Ensure facilities have redundancy and failover options to maintain operations during outages, including energy availability and reliability of the grid.
- Temperature and environmental controls: Maintain optimal environmental conditions to prevent hardware failure due to overheating or other environmental factors.
- Physical security: Protect data centers from unauthorized access and physical threats.
- Energy efficiency and sustainability: Ensure that data centers operate in an energy-efficient and environmentally sustainable manner.

Recommended actions

- Assess data center design strategy for redundant power supplies (including energy availability and grid reliability), network connections, and failover systems; regularly test and review these components.
- Assess data center design strategy for the installation of advanced HVAC systems, monitoring for temperature, humidity, and airflow, and plans to conduct regular maintenance.
- Assess multilayered security measures, including biometric access controls, surveillance systems, and security personnel.
- Assess energy strategy for energy-efficient technologies, the monitoring and optimization of energy usage, and strategy to explore renewable energy sources, as deemed necessary.

08 Driving capital growth



Signal 1

Digital infrastructure

The rise of AI and data-intensive applications is fueling massive investment in the "picks and shovels" of the digital world. The strategic goal is to own the essential infrastructure that will power the next wave of digital innovation.

What to watch

- Continued consolidation in the telecom sector around fiber and wireless assets
- The growing role of private equity in funding and consolidating digital infrastructure
- The impact of new technologies such as IoT and AR/VR on infrastructure requirements

Recommended actions

- For telecommunications companies, prioritizing investment in fiber network expansion and spectrum acquisition is key. Secure the foundational assets for 5G and next-gen services. Owning the network infrastructure provides a long-term competitive advantage and creates new revenue streams from enterprise and consumer applications.
- Data center operators should focus on developing green and efficient solutions to attract hyperscalers and other large clients. Address the massive power consumption of data centers. Sustainable solutions reduce operating costs, meet corporate ESG mandates, and are a key decision factor for large-scale cloud providers.
- Investors should consider the long-term growth potential of digital infrastructure as a critical enabler of the digital economy.

Signal 2

AI growth

AI is the dominant force, prompting a "capital expenditure super cycle" in the technology sector. Significant investment is pouring into developing large language models, AI-native platforms, and the specialized hardware (such as high-performance chips) required to power them.

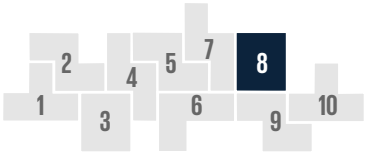
What to watch

- The M&A landscape for AI start-ups, with a continued focus on "acqui-hiring" and technology acquisition
- The build-out of specialized AI cloud infrastructure and associated capital expenditures
- The flow of venture capital into new AI application and platform companies

Recommended actions

- For TMT companies, it is crucial to justify AI investments with clear business cases and ROI projections. Go beyond the hype. Develop detailed financial models and key performance indicators to measure the true impact of AI on revenue growth, cost savings, and operational efficiency before committing significant capital.
- Scrutinize the capital allocation strategies of companies investing heavily in AI. Assess whether capital is being used for long-term value creation, such as developing proprietary technology, or for short-term, expensive talent acquisition with questionable returns.
- All stakeholders should monitor the impact of AI investments on market concentration and competition. Track M&A activity and the market share of dominant firms.

08 Driving capital growth (continued)



Signal 3

Antitrust and M&A

A new era of aggressive antitrust enforcement in both the US and EU is having a "chilling effect" on large-scale M&A, making regulatory risk the single most significant challenge to deal execution.

What to watch

- The outcome of ongoing antitrust lawsuits against major tech companies on both sides of the Atlantic
- Whether a potential shift in the US administration leads to a more permissive M&A environment
- How the EU enforces the M&A reporting requirements under the DMA

Recommended actions

- Closely monitor legal precedents. Adjust M&A strategies and risk assessments based on the evolving interpretation of antitrust laws by regulators.
- Develop flexible, scenario-based M&A plans. Be prepared to accelerate or delay transactions based on shifts in the political and regulatory climate following an election.
- Engage with legal counsel specializing in EU competition law. Proactively adapt deal structures and reporting processes to comply with regulations such as the DMA.

Signal 4

Expanding digital reach

In TMT, expanding digital reach drives capital growth by building data-rich, direct-to-consumer relationships that attract investors seeking scalable, personalized business models and creating fundamental, long-term enterprise value.

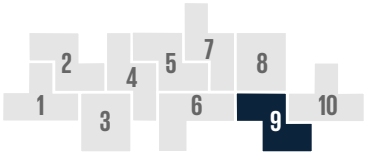
What to watch

- The ratio of lifetime value to customer acquisition cost for digital channels to ensure scalability and profitability
- Merger and acquisition activities and venture capital investments targeting companies with innovative digital platforms or significant user bases

Recommended actions

- Allocate capital to build or acquire robust and scalable digital platforms that can support a growing user base and increasing data volumes.
- Identify and pursue strategic partnerships or acquisitions that can accelerate the expansion of your digital reach, whether through technology, talent, or market access.
- Develop strong data analytics capabilities to gain insights into consumer behavior, personalize user experiences, and optimize marketing efforts.

09 Content moderation and age verification



Signal 1

Content moderation

A global regulatory wave, including new laws in Australia, the UK, EU, and US, is challenging platform self-governance with legal obligations. These regulations hold platforms accountable for systemic risks, transparent content moderation, and the removal of content that threatens public safety and national security.

What to watch

- Increased enforcement of the DSA and introduction of additional codes
- The expansion of "duty of care" obligations to new jurisdictions and content types
- A fragmented US landscape with state-level content laws emerging alongside federal executive pressures

Recommended actions

- Develop a content moderation framework that establishes a high baseline for safety while allowing for regional adaptations to comply with specific laws.
- Engineer your systems to support transparency reporting and user-facing appeals mechanisms, which are core requirements of the DSA and a growing global standard.
- Implement moderation methods that are demonstrably effective at keeping children from harmful content and removing adult content such as NCII.

Signal 2

Age verification

Regulators in Australia, the UK, and US are authoring regulations that mandate age verification practices and the implementation of the highest privacy settings for services likely to be accessed to children.

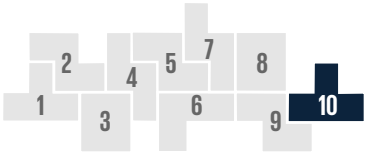
What to watch

- An increase in guidance on what is sufficient age assurance
- A wave of US states introducing versions of the California Age-Appropriate Design Code (CA AADC)
- Increased regulatory scrutiny of the effectiveness and privacy implications of age verification methods

Recommended actions

- Adopt “safety by design”: embed child safety principles and age-appropriate design into the entire product development lifecycle.
- Implement “privacy by default": configure services that may be used by minors to apply the most protective settings as the default for all users, in line with the high standard set by the CA AADC.
- Develop a multi-faceted age verification strategy: invest in a flexible portfolio of age estimation and verification to ensure compliance across different jurisdictions and risk levels without creating unnecessary user friction.

10 Enhancing parties and workforce



Signal 1

Supply chain risk

The focus of risk management has shifted from securing the individual company to securing its entire ecosystem of third-party relationships, including vendors, suppliers, and partners. A company's risk is now inextricably linked to the security posture of its providers.

What to watch

- The development of new regulations governing supply chain integrity and third-party data access
- The potential for cascading supply chain failures caused by a single compromised provider
- Scrutinizing the provenance and legal rights of data used to train third-party AI models and verifying compliance with open-source software licenses during M&A due diligence

Recommended actions

- Get ahead of new supply chain and data access regulations by establishing a dynamic monitoring framework to anticipate regulatory shifts in key markets and proactively map their specific impact to your third-party ecosystem.
- Implement a supply chain stress-testing program. By actively simulating provider failures, the exercise can uncover hidden dependencies and build robust contingency plans to ensure operational continuity during a crisis. Companies are diversifying their supply chains away from single-country dependencies.
- Embed a Digital Provenance workstream into M&A due diligence. This involves a forensic analysis of AI training data and a deep scan for open-source license compliance to prevent inheriting costly legal issues and assess the true value of technology investments.

Signal 2

Resource risk

The stability of the power grid and the availability of land and water have become critical third-party dependencies for the TMT sector, elevating utilities and even local communities to the status of essential providers whose approval and reliability are paramount.

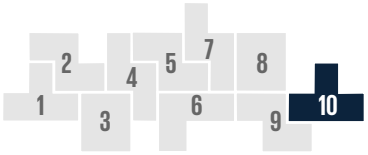
What to watch

- Signs of grid instability in key regions as AI-driven energy demand surges. Monitor how grid operators respond and whether infrastructure upgrades can keep pace with the unprecedented consumption growth from data centers.
- Emerging regulations from local governments aimed at curbing data center energy and water use. Monitor policy proposals that could directly impact future site selection, data center design, and long-term operational costs.

Recommended actions

- Conduct a grid-vulnerability and geographic risk assessment. This involves mapping critical data center locations against regional grid stability forecasts, identifying sites most at risk of AI-induced power volatility, and creating detailed mitigation plans for those high-risk zones, including securing priority access or backup generation.
- Establish a strategic energy sourcing and innovation program. The mandate of this group should be to actively pilot and evaluate the feasibility of alternative energy—such as on-site generation, microgrids, or partnerships for next-gen nuclear—for both new and existing data center builds to create a diversified, resilient energy portfolio.

10 Enhancing parties and workforce (continued)



Signal 3

What to watch

Workforce risks

The traditional TMT talent model is broken. In a hypercompetitive market, critical AI skills have a short half-life, creating constant, expensive churn. Companies struggle to find, upskill, and retain talent while generative AI simultaneously reshapes job roles.

- The evolution of generative AI's impact on job roles, specifically which tasks are fully automated versus which are augmented, and the resulting shifts in team structure and required human skills
- Shifts in employee expectations regarding radical flexibility, personalized career paths, and the demand for purpose-driven work, which will influence company loyalty and retention
- The widening gap between the skills required for next-generation technologies (e.g., quantum computing, advanced AI) and the output of traditional education systems

Recommended actions

- Implement an aggressive, continuous upskilling program that is deeply embedded in daily workflows. This means treating skill development as a core, measured business function—akin to R&D—not an occasional HR initiative. This approach is essential to close critical skill gaps and maintain a competitive advantage.
- Develop a forward-looking, strategic workforce planning model that actively forecasts future skill needs based on a long-term roadmap. Proactively build robust talent pipelines by diversifying sourcing through targeted acquisitions and structured internal mobility programs.
- Redesign job roles to strategically integrate AI as a collaborative copilot for employees. Focus on automating repetitive, low-value tasks to augment human capabilities. This frees up talent to concentrate on complex problem-solving, creativity, and high-value strategic work that drives innovation.

How KPMG can help

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 US 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.

This thorough foresight is especially critical in the TMT space, where rapid innovation frequently intersects with complex, evolving oversight. The TMT sector professionals at KPMG understand today's changing and challenging environment. Our network combines industry knowledge with technical experience to provide insights that help leaders transform and simplify their complex business models.

With a keen understanding of the changing marketplace, our professionals go beyond today's challenges to anticipate the potential long- and short-term consequences of shifting business, as well as financial and technology strategies. We also work with clients to explore potential obstacles to change and collaborate on critical decisions that can help deliver real value to their businesses.

According to Source's Perceptions of Consulting in Technology, Media and Telecoms 2025 report, KPMG was ranked #1 by clients for overall quality of work in TMT, #1 for HR & change management in TMT, and #1 for financial management in TMT. This study surveyed 678 TMT executives, directors, and senior managers from diverse global organizations (83 percent with over $500 million in revenue) to understand their perceptions of leading consulting firms, from initial awareness through direct client experience.

To explore further insights, please visit the KPMG US technology, media, and telecommunications industry web page.

Regulatory Alerts
Quick-hitting summaries of specific regulatory developments and their impact on businesses across industries.

Points of View
Insights and analyses of emerging regulatory issues impacting businesses across industries.

In case you missed it

Ten Key Regulatory Challenges of 2026

Download
Scan the QR code to obtain a copy on your mobile device.

Subscribe
Don't miss out. Scan the QR code to get the latest or **click here**

For more information, contact us

Vijay Subramanyam
Principal, Advisory
TMT Sector Consulting Leader
KPMG US

Vijaysubramanyam@kpmg.com

LinkedIn

Lisa Rawls
Principal, Advisory
TMT Sector Risk Leader
KPMG US

lisarawls@kpmg.com

LinkedIn

John Kemler
Principal, Advisory
Digital Platform Safety Leader
KPMG US

jkemler@kpmg.com

LinkedIn

Laura Byerly
Managing Director
Regulatory Insights
KPMG US

lbyerly@kpmg.com

LinkedIn

We would like to thank our contributors to this report:

Anita Barksdale, Managing Director, TMT Cyber and Tech Risk, KPMG US
Matthieu Chabelard, Principal, TMT Forensic, KPMG US
Chris Schneider, Partner, TMT Forensic, KPMG US
Matt Tobey, Principal, TMT Cyber and Tech Risk, KPMG US
Rory Wilson, Managing Director, TMT Forensic, KPMG US
Koen Klein Tank, Partner, IT Advisory and Assurance, KPMG in the Netherlands
Manon van Rietschoten, Senior Manager, IT Advisory and Assurance, KPMG in the Netherlands

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

Learn about us: **kpmg.com**