Tech regulation continues. Is your enterprise compliance ready?

pwc

Technology companies are entering a new phase of regulation, and many probably aren't prepared yet. Shaped during an era of growth and limited government oversight, these companies historically viewed new regulations as an occasional distraction that's handled, often ad hoc, by their compliance and legal teams. Back then, the volume of regulatory change was manageable and there wasn't a pressing need to build a formalized approach to regulatory response and readiness.

As we enter 2025, that's all about to change. A new wave of global tech regulations and standards is taking hold and expanding in the European Union, United Kingdom, India, South Korea, Canada and elsewhere. Domestically, the states are racing to enact new laws governing AI, privacy and content moderation. The Justice Department recently issued a final rule to prevent foreign adversaries from accessing Americans' bulk sensitive personal data. And the Trump administration, despite its deregulatory posture overall, has signaled an appetite for new oversight on questions of Section 230 liability, content moderation, AI, immigration and trade with foreign rivals.

In this environment, the industry's long-standing, reactive approach to compliance is no longer viable. Responding to regulations only after they're issued may have worked in the past, but it's become too costly, inefficient and risky with today's emerging, often overlapping rules. Risk, compliance and legal teams at tech companies should accept this reality and face it head-on, learning from other sectors and building a fit-for-purpose compliance infrastructure. This shift calls for adopting an agile compliance model that integrates regulatory readiness across strategy, products and operations.

A brave new regulatory landscape

Policymakers at home and abroad are advancing new guardrails around technology at a dizzying pace. This trend reflects a broader societal shift in awareness of the potential harm that emerging tech, large digital platforms and the widespread collection of personal data might pose if left unsupervised.

The new guardrails fall into five categories.

Artificial intelligence

There is a focus on responsible use, transparency, and accountability in AI systems.

Digital safety

Governments prioritize regulations to protect users from cyber threats and online harms.

Digital competition

Regulatory authorities address digital competition concerns to promote fair practices and foster innovation.

Privacy and data protection

Strengthened privacy regulations globally empower individuals and enhance data protection and transparency.

Cybersecurity

Governments implement stringent cybersecurity regulations to enhance protection against cyberattacks and data breaches.

1 **Artificial intelligence.** AI capabilities are evolving rapidly and regulators are sprinting to keep pace with Responsible AI regulation. The speed of the technology advancements, combined with the regulatory response, is testing the limits of compliance and risk management programs at companies of all sizes and in all sectors. For tech companies, the challenge is, of course, more acute.

2 **Digital safety.** New requirements around online safety are proliferating. These include laws protecting users of digital platforms (especially children) from harmful content, and requiring platforms to take preventive steps, provide safety tools and disclose metrics on their efforts to remove harmful content. Some also require a mechanism for users to challenge a platform's content-moderation decisions.

3 **Digital competition.** Efforts abroad to counter US tech companies' market dominance and foster homegrown innovation are gaining ground. These laws prevent perceived anti-competitive practices in the digital economy and attempt to eliminate barriers to entry and level the playing field for market participants.

4 **Privacy and data protection.** Another active category of tech regulations is privacy. Historically a higher priority internationally, privacy and data protection requirements have flourished domestically in recent years, especially among individual states.

5 **Cybersecurity.** One of the biggest categories of existing and emerging tech regulations is cybersecurity and operational resilience. In Europe alone, several major regulations have been adopted recently and will take effect soon. At home, there are new federal requirements around critical infrastructure and efforts to harmonize a multitude of existing cyber rules. Some states, notably California and New York, are advancing their own cyber rules.

For examples of recently implemented tech regulations, see the list in the appendix.

The hidden cost of reactive compliance

Many in the tech industry could find themselves unprepared for this regulatory environment and they're inching toward a compliance crisis. Why? Consider how most tech companies approach regulations compared to their peers in other sectors. Rather than build infrastructure to manage continually evolving requirements — something that banks, hospital systems and insurance companies have been doing for decades, although not always in an integrated manner — the tech industry has generally taken a reactive, siloed and often federated approach.

> **"Responding reactively to each new regulation (initial workaround, customer care, remediation, litigation and penalties) is often costly and inefficient."**

This can work with the effort of smart people doing the right thing, but as compliance requirements continue to grow, this fragmented approach is unsustainable. Responding reactively to each new regulation (initial workaround, customer care, remediation, litigation and penalties) is often costly and inefficient. The work usually isn't scalable, with each response producing unique solutions that typically won't translate to the next big regulation. Even for the same regulation, a company's response may not be consistent across the enterprise, but rather, a patchwork of solutions, each one tailored to a different line of business.

And so, the cycle of ad hoc solution-building continues, throwing good money after bad and creating unnecessary risk.

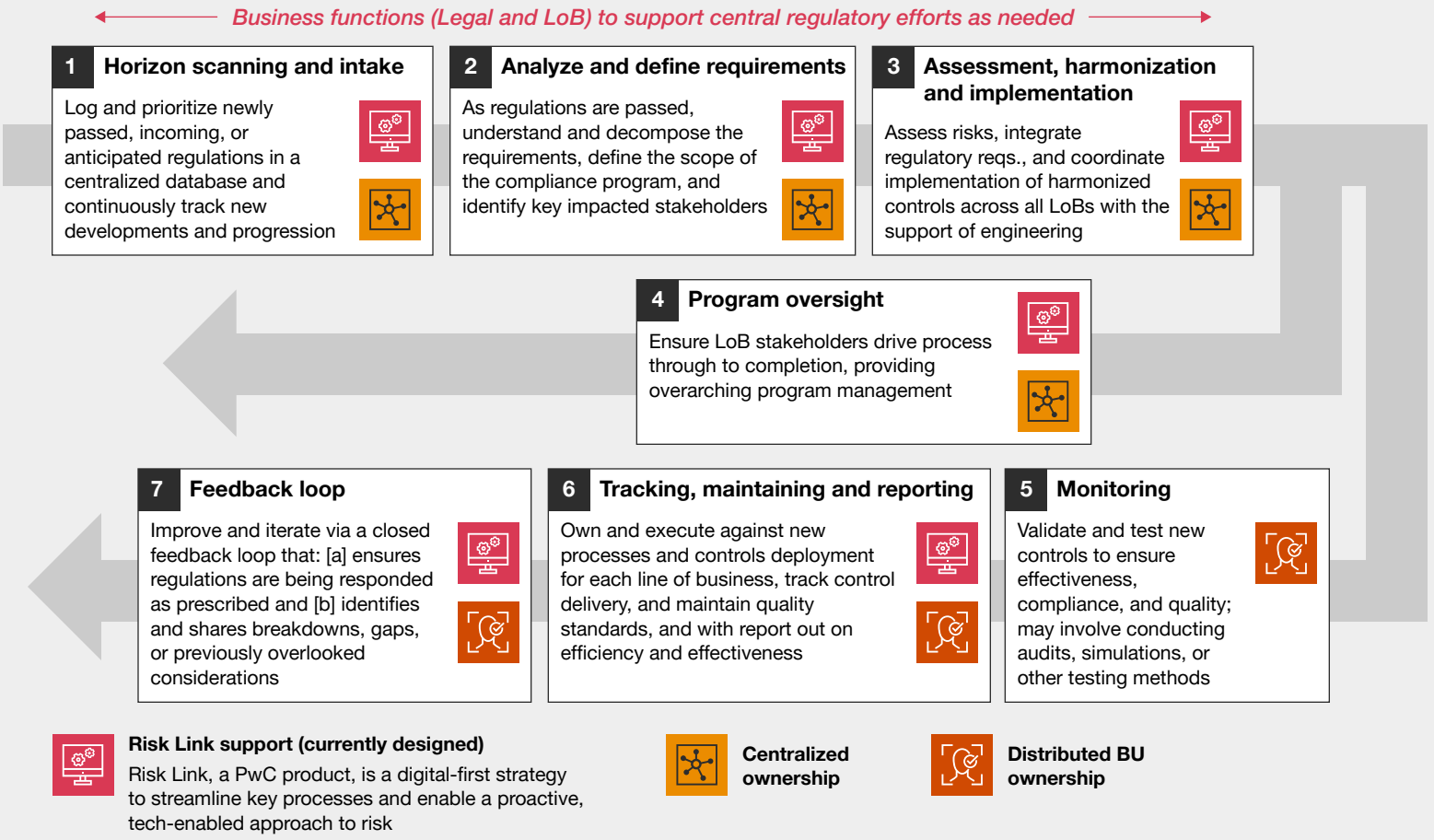
What's more, the true cost of reactive measures is often grossly underestimated. While planned spending on compliance infrastructure sits in the risk leader's budget and is easy to track, reactive costs are dispersed across the business — legal, product, engineering, operations, marketing, government relations — and include harder-to-quantify costs like lost opportunities, product delays and reputational damage.

For that matter, spending on proactive measures can be misleading, too. Investing in compliance infrastructure won't help if it's siloed or can't be adapted to handle new requirements in multiple jurisdictions. True readiness requires a deep understanding of the regulatory landscape, one that informs the company's compliance and risk management strategy, the people it hires and the processes, systems and tools it adopts. It also requires a unified model for managing new regulations, one that eliminates duplication, supports agility and enables consistent, robust compliance across lines of business.

Operationalizing regulatory readiness

To achieve regulatory readiness, consider what your peers in other sectors have done to operationalize compliance. A common thread in how others manage regulatory change successfully is a model that drives shared enterprise standards and a consistent approach across the organization, all in a well-coordinated manner. That doesn't necessarily mean a rigid, top-down approach across all lines of business and geographic markets. There's a continuum of potential approaches, some of which may allow for a centralized regulatory strategy while also enabling decentralized decision-making for specific products or local laws.

7 steps to regulatory readiness



The right approach may vary for different entities, depending on their organizational structure, culture and geographic footprint. However, what's true for all successful compliance models is that they involve consistency in execution across the enterprise, be that centralization or strong coordination, to help eliminate wasteful duplication and workarounds and to support agile, consistent and strategic compliance outcomes.

Enterprise compliance: Where to start?

Implementing a strong and effective compliance model begins with establishing a unified approach to monitoring regulations, breaking them into actionable requirements, applying them across the organization and implementing readiness measures. This framework will help your organization consistently assess, manage and mitigate risks across all existing and incoming policies, standards and regulatory obligations, fostering consistent compliance and driving operational efficiency. Once this consistent and integrated approach is established, the application can be decentralized or federated, provided that each downstream team adheres to a shared methodology, technology stack and governance structure.

Drawing on lessons learned from organizations that underwent similar transformations, we've identified several practical steps to help you launch or enhance your own programs.

1

Build on what you already have

Most companies already have some form of compliance functions, governance and controls. Assess your existing structures to identify what you can leverage or scale. A cohesive regulatory readiness program should serve as the convener across risk/compliance, business and engineering teams, aligning everyone around a single framework.

2

Create a cross-functional committee

This isn't just a legal or compliance responsibility — success hinges on collaboration across multiple functions, including engineering, product, operations and so on. While one team may take the lead, broad engagement is essential for translating legal requirements into practical controls and features. Consider forming a standing committee to regularly align on new obligations, milestones, progress and risks.

3

Embed compliance early and often

Many companies wait until late-stage development or post-launch to tackle compliance. By building compliance into the product life cycle — starting at the design phase — you can help reduce risk, avoid surprises and speed time-to-market.

4 Leverage a common control and compliance baseline

You probably already have controls in place — whether for privacy, cybersecurity or previous regulations like DMA and DSA. By harmonizing these controls into a single baseline, you'll gain visibility into what's covered and what remains exposed. AI can help efficiently map new regulatory obligations to your existing baseline and address any gaps in a systematic, prioritized way.

5 Use technology wisely (there's no silver bullet)

AI and automation can streamline your regulatory processes from triaging and assessing new regulations to mapping requirements against existing controls. However, human oversight remains vital. Inputs must be accurate, contextualized and reviewed by specialists to enable tailored, relevant outputs. Technology is a powerful multiplier, but people ultimately drive the final decisions.

6 Cultivate a culture of compliance

Product changes alone won't solve the problem. Train employees on emerging regulations, encourage open communication about risks and foster a sense of shared responsibility. Compliance shouldn't be viewed as a check-the-box exercise.

7 Stay ahead of the next wave

New regulations are emerging daily, making this an ongoing effort rather than a one-time exercise. A key element of any readiness program is the ability to anticipate what's on the horizon through active monitoring, industry engagement and legislation tracking. By keeping an eye out for proposed regulations, you can move strategically instead of scrambling to react.

Appendix: A sampling of recent tech regulations

Tech companies are facing growing requirements from across the globe. Here's a selection of laws and regulations recently adopted or proposed as of this paper's issuance. This list is designed to be illustrative. Some items will be rolled back or modified, while new ones will continue emerging, which is why it's critical that companies have the capability to manage changing requirements.

1

Artificial intelligence — Laws, regulations and standards that impose guardrails around AI system development, deployment and use.

Jurisdiction	Regulation or standard	Status
United States	NIST AI Risk Management Framework	Adopted
	EO on artificial intelligence	Rescinded
	Joint CFPB, DOJ, EEOC and FTC statement on enforcement efforts against discrimination and bias in automated systems	Adopted
	California 2024 AI legislative package	Adopted
	Colorado SB 24-205	Adopted
	Colorado Regulation 10-1-1	Adopted
	Utah Artificial Intelligence Policy Act	Adopted
	Tennessee's Ensuring Likeness, Voice, and Image Security (ELVIS) Act	Adopted
Australia	Australia's Artificial Intelligence Ethics Principles	Adopted
	Voluntary AI Safety Standard	Adopted
	National framework for the assurance of artificial intelligence in government	Adopted
Brazil	AI Regulation Bill No. 2338/2023	Proposed
Canada	AI and Data Act	Proposed
China	Algorithmic Recommendation Regulation	Adopted
	Deep Synthesis Management Regulation	Adopted
	Measures for the Management of Generative AI Services 2023	Adopted
European Union	AI Act	Adopted
	AI Liability Directive	Proposed
India	Digital India Act	Proposed
International	ISO/IEC 42001	Adopted
	OECD Recommendation of the Council on Artificial Intelligence	Adopted
Saudi Arabia	AI Adoption Framework	Adopted
South Korea	Bill on Fostering the AI Industry and Securing Trustworthy AI	Proposed
United Kingdom	Consultation on Copyright and Artificial Intelligence	Proposed

2

Digital safety — Laws, regulations and standards that impose user safety requirements for online platforms and services, including restrictions on illegal and harmful content (especially directed at children), fraudulent advertising, disinformation and harmful algorithms.

Jurisdiction	Regulation or standard	Status
United States	California Age-Appropriate Design Act	Adopted
Australia	Online Safety Act	Adopted
	Online Safety Industry Codes	Adopted (Phase 1)
European Union	Digital Services Act (DSA)	Adopted
	Regulation to address the dissemination of terrorist content online	Adopted
Ireland	Irish Online Safety and Media Regulation Act	Adopted
India	Digital India Act	Proposed
	India IT Rules 2.0	Adopted
South Korea	Act on Protection of Digital Service Users	Adopted
Thailand	Digital Platform Services Law	Adopted
United Kingdom	Online Safety Act	Adopted

3

Digital competition — Laws, regulations and standards that govern competition between tech companies or digital platforms.

Jurisdiction	Regulation or standard	Status
United States	DOJ/FTC merger guidelines	Adopted
Australia	News Media and Digital Platforms Mandatory Bargaining Code	Adopted
Chile	Horizontal Merger Guidelines	Adopted
European Union	Digital Markets Act (DMA)	Adopted
	Data Act	Adopted
India	Digital Competition Act	Proposed
South Korea	Online Platform Monopoly Guidelines	Adopted
United Kingdom	Digital Markets, Competition and Consumers Act 2024	Adopted
	Digital markets competition regime guidance	Adopted

4 **Privacy and data protection** — Laws, regulations and standards that impose guardrails around the collection, handling, use and sharing of personal or sensitive data.

Jurisdiction	Regulation or standard	Status
United States	EO restricting bulk data transfers	Adopted
	DOJ rule implementing EO on bulk data transfers	Adopted
	Protecting Americans' Data from Foreign Adversaries Act (PADFA)	Adopted
	Protecting Americans from Foreign Adversary Controlled Applications Act	Adopted
	HIPAA security rule amendments	Proposed
	California DELETE Act	Adopted
	Maryland Online Data Privacy Act	Adopted
	Minnesota Consumer Data Privacy Act	Adopted
	Oregon Consumer Privacy Act	Adopted
	Delaware Personal Data Privacy Act	Adopted
	New Jersey S332	Adopted
Canada	Bill C-26	Proposed
China	Personal Information Protection Law	Adopted
European Union	Data Act	Adopted
	EU-US Data Privacy Framework	Adopted
India	Digital Personal Data Protection Act, 2023	Adopted
Saudi Arabia	Personal Data Protection Law	Adopted
United Kingdom	Data Protection and Digital Information Bill	Proposed
	Data (Use and Access) Bill	Proposed

5 **Cybersecurity** — Laws, regulations and standards that govern cybersecurity and cyber resilience.

Jurisdiction	Regulation or standard	Status
United States	EO on Strengthening and Promoting Innovation in the Nation's Cybersecurity	Adopted
	Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA)	Adopted
	CISA rules implementing CIRCIA	Proposed
	SEC cyber disclosure rule	Adopted
	Quantum Computing Cybersecurity Preparedness Act	Adopted
	NYSDFS cyber regulations	Adopted
	California cyber regulations	Proposed
China	CAC Security Assessment Measures	Adopted
European Union	Cyber Resilience Act	Adopted
	NIS-2 Directive	Adopted
	Digital Operations Resilience Act (DORA)	Adopted
	Regulation on Machinery 2023/1230	Adopted
	Critical Entities Resilience Directive	Adopted
United Kingdom	Product Security and Telecommunications Infrastructure Act	Adopted
	Cyber Security and Resilience Bill	Proposed
	Consultation paper 26/23 — Operational resilience: Critical third parties to the UK financial sector	Adopted

Contact us

Jason Pett
Partner, Global TMT Risk Leader
PwC US
jason.pett@pwc.com | LinkedIn

Matt Kral
Principal, Cyber, Risk & Regulatory
PwC US
matthew.s.kral@pwc.com | LinkedIn

Sara Putnam
Partner, US TMT Risk Leader
PwC US
sara.putnam@pwc.com | LinkedIn