POINT OF VIEW

Top compliance challenges facing the technology industry in 2025

By Kaitlin Kirkham-Cooper
Managing Director, Protiviti

In the fast-paced world of technology, both regulators and companies face challenges applying existing laws to new and rapid developments. Given the high stakes of non-compliance, which may lead to business restrictions, technology companies' senior management, boards and compliance teams must clearly understand current and emerging risks, ensuring that they have effective people, processes and controls in place to manage these challenges.

Consider the goals of technology regulation: protecting consumers, safeguarding children, promoting fair competition, preventing misinformation, bolstering national security, upholding ethical standards, ensuring nondiscrimination, promoting industry resilience and fostering sustainability. The technology sector is navigating an increasingly complex regulatory landscape shaped by diverse oversight.

protiviti®
Global Business Consulting

In the United States, President-elect Donald Trump, along with a Republican-controlled Senate and House, is expected to create a business-friendly regulatory environment for the sector. However, there is considerable uncertainty about how the new administration's policies on China, tariffs, and corporate taxes will unfold. For more insights, read our report on "Trump 2.0: Possible Winners and Losers."

As we considered what compliance challenges are likely to be top of mind for technology companies in 2025, we compiled a list consisting of both regulatory and business risks. The list, while not exhaustive or ranked, highlights priorities likely to garner attention from companies and regulators. The evergreen topics of data protection and security are integral to these themes.

Finally, not all priorities of challenges impact every tech company equally, given the sector's diversity, but they are expected to be focal points in the coming year.

Key takeaways

1 Navigating regulatory complexity

Establish a strong compliance framework to prepare your organisation for evolving and increasingly complex global regulations.

2 Leading in responsible tech

Set industry standards through ethical practices in AI and online safety, shaping the future of technology.

3 Championing online safety

Demonstrate commitment to social responsibility by creating safer digital environments, especially for children.

4 Compliance-by-design advantage

Enhance business efficiency and mitigate risks by integrating compliance into your core operations.

5 Leveraging transparency

Turn regulatory demands into strategic benefits by promoting transparency and strengthening consumer trust.

2025 compliance priorities for technology companies

1. Responsible AI
2. Online safety
3. Child protection
4. Antitrust/competition
5. Operational resiliency
6. Third- and fourth-party risk management
7. Sanctions/export controls/ investment restrictions
8. Compliance by design
9. Evidencing the compliance effort
10. Talent resourcing

Regulatory-driven risks

Responsible AI

Lawmakers, governments, standard-setting organisations and regulators across the globe are focused on ensuring that proper guardrails exist to manage the risks of artificial intelligence (AI). Notable examples of AI governance frameworks published to date include the OECD Principles on AI, the Asilomar AI Principles, the U.K. Government Centre Data Ethics Innovation Guidance Framework, the Singapore Model AI Governance Framework, the NIST AI Risk Management Framework and the EU AI Act, the last arguably the most significant AI regulation to date issued by any jurisdiction. Technology companies, as providers and users of AI, need to understand and address the standards already issued, both as they relate to the technology industry directly and as they relate to industries to which technology companies provide AI services and products. Just as importantly, technology companies need to continuously monitor developments in this space to understand how they may impact their business today and their strategic plans.

Online safety

For the technology industry, online-safety regulations are aimed at creating a safe digital environment that may require, depending on the specific law or jurisdictions, adhering to data protection requirements and cybersecurity standards; and overseeing online intermediaries and platforms to prevent illegal and harmful activities online, including the spread of misinformation. While the United States lags in passing comprehensive content-moderation regulations, the global regulatory environment, particularly in Europe, is requiring technology giants to address these risks. Notable examples of online safety laws are the EU's Digital Services Act, the U.K.'s Online Safety Act, Australia's Online Safety Act and several regulations aimed specifically at child protection, which because of their significance we have identified as a separate priority. These regulations introduce the first set of comprehensive obligations that require technology platforms to take accountability and provide proactive oversight over what and who is on their platforms.

Child protection

Safeguarding children from harmful content, cyberbullying, sexual exploitation and other online threats and protecting the mental health of children are existing social issues that have recently become widespread government priorities. These concerns are reflected in proposed bills such as the U.S. Kids Online Safety Act (KOSA), the U.S. Children's Online Privacy Act 2.0 (COPPA 2.0), and implemented regulations such as the U.K. Online Safety Act — Volume 2 South Korea's Youth Protection Revision Act, and Germany's Network Enforcement Act, among others. The U.S. environment is further amplified on these topics by lawsuits brought by state attorneys general against some technology companies.

For most technology companies, safeguarding children is not just a regulatory compliance obligation, it is also a matter of corporate ethics and social responsibility. Many technology companies have pledged in their names and through membership in organisations such as the Internet Watch Foundation to make online experiences safer for children.

Antitrust/anticompetitive risk

In recent years, several technology companies have faced significant litigation related to antitrust and anticompetitive practices. These cases, which often call for increased regulation of the technology industry and sometimes for company breakups, stem from concerns that the dominance of large technology companies may hinder competition. To some extent, this risk is influenced by politics — the views of the party currently in power — but it represents an ongoing, significant threat to the technology industry's largest players. In Europe, the implementation of the Digital Markets Act (DMA) has fundamentally changed the way large technology companies (called gatekeepers by the regulation) are developing their products and going to market, posing a threat to bottom-line profits.

Operational resiliency

Operational resilience remains a priority for the technology industry in part because it is critical to maintaining market trust, but also because technology companies that provide services to financial institutions and critical infrastructure, for example, may be subject to resilience requirements directed at these industries. The EU Digital Operational Resilience Act (DORA) and its counterparts in the U.K. (U.K. DORA) and Australia (CPS230) are examples of how this would work for technology companies that provide services to the financial services industry. Technology companies that provide services such as cloud computing services, data analytics platforms, and cybersecurity solutions that are critical to the operations of financial services companies will be required to ensure that their services comply with the operational and security standards imposed by these financial services-focused requirements and may be subject to regulatory review. Similar requirements have long existed in the U.S. under the Bank Services Company Act but have received even more attention in recent years in large part because of the high number of large-scale cyber breaches, which many believe will be exacerbated by bad actors using AI.

Third- and fourth-party risk management

Third- and fourth-party risk management is often embedded in operational resilience requirements. DORA, for example, requires, among other things, that technology companies provide critical services to be transparent about their subcontractor arrangements, to perform appropriate due diligence and risk assessments of their contractors, to include in their contracts with subcontractors the mandate that subcontractors comply with DORA, and that subcontractor arrangements have exit strategies that allow for terminating a relationship without disrupting critical operations.

Other regulatory programs, though, may also impose third- and fourth-party risk management requirements on technology service providers. For example, technology companies providing critical services to the government may also be subject to explicit third- and fourth-party risk management requirements. In the U.S., for example, the Federal Risk and Authorisation Management Program (FedRAMP) prescribes specific third- and fourth-party risk management requirements for technology companies providing cloud services to federal agencies.

Beyond regulatory requirements and industry standards, the importance of third- and fourth-party risk management is further amplified by the increased threat of security breaches. Developing a clear understanding of who your third- and fourth-party service providers are and managing the risk associated with those providers through contracting, enhanced due diligence and ongoing monitoring is becoming more complex but essential.

Sanctions/export controls/investment limitations

The escalation of geopolitical tensions across the globe has subjected the technology industry to a growing number of requirements aimed at protecting the national security of the West and its allies and, in the case of the U.S., maintaining its competitive position versus China. These requirements include economic sanctions prohibiting dealings with certain countries, entities and individuals; export controls that preclude providing certain hardware and software to prohibited jurisdictions and parties; and restrictions on Chinese investment in U.S. technology and vice versa. While coordination among the Western allies has been significantly enhanced over the last two-plus years, there are differences in how various jurisdictions have set and apply restrictions that can complicate compliance. Like other requirements discussed above, there is also an expectation that sellers of prohibited or restricted goods and services understand the entire supply chain, including the ultimate destination and end user of the goods and services.

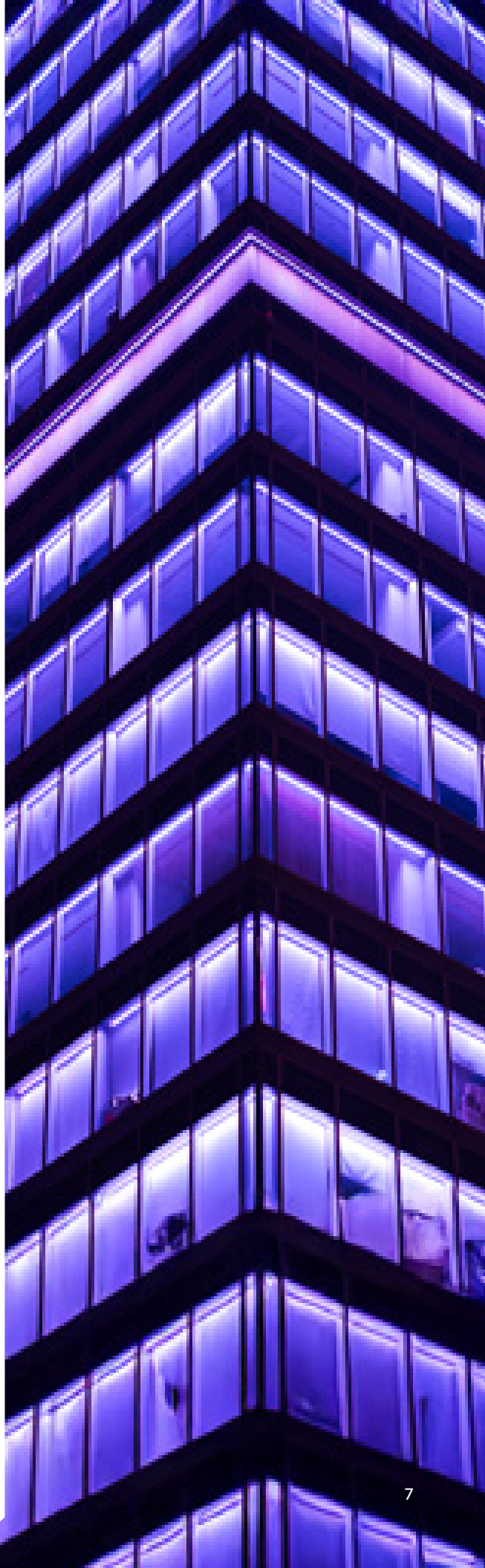
Given the significant challenges they face related to data security, regulatory compliance, and supply chain disruptions, technology companies must clearly define and continuously monitor their network of third- and fourth-party partners to effectively manage risks and ensure operational resilience.

Business environment risks

What should be evident from the sections above are the complexities and evolving nature of the compliance requirements facing the technology industry, the impact of cross-border laws and regulations and differing cultural views, daunting logistical challenges such as monitoring in real time billions of web pages and apps, often-competing priorities (e.g., privacy vs. safety), and extensive flow down requirements because of the industries served — all of this against a backdrop of antitrust and anticompetitive challenges that require the biggest companies to engage in continual extensive lobbying and advocacy efforts to educate various audiences about a company's operations and the benefits provided. All these factors add to the compliance challenges faced by technology companies and place a premium on how technology companies manage compliance.

Effective compliance programs, regardless of industry, share some common attributes: senior management and board of director support; comprehensive understanding and assessment of the requirements and risks; an adequately resourced (in terms of people and tools) compliance function; clear delineation of roles and responsibilities; documented policies and procedures; a compliance training program; a comprehensive management information system; and periodic independent assessment of the effectiveness of the compliance effort.

As technology companies focus on how they are addressing their compliance obligations in 2025, we believe the three areas discussed below warrant special attention. All three are aimed at enhancing the efficiency, effectiveness and sustainability of the compliance program.



Compliance by design

One of the strengths of the technology industry is, of course, its capacity to innovate. While innovation and regulation may seem at odds, the breadth of compliance requirements faced by the industry and the consequences of noncompliance argue for a compliance-by-design approach that integrates compliance considerations into the design and development processes of business operations, systems, products, and services from the very beginning, not after the fact. As an example, this may mean integrating some compliance and legal functions into the first-line functions like product and engineering teams and building in processes that require that products are coded with risk and compliance in mind as part of the software development lifecycle.

The benefits of a compliance-by-design approach include reduced exposure from identifying and mitigating risks early on, cost efficiency by avoiding the refitting that is often required when compliance requirements are considered later in the process and a more sustainable framework for supporting company growth. For many technology companies, this approach would require a significant cultural change, which is likely to be met by resistance. Ensuring that there is appropriate management-level support and tone at the top is critical for the compliance effort to be successful.

Enhanced program documentation

Increasingly, regulators, as well as the independent assessors and auditors stipulated by enforcement and/or certain regulations, are asking for evidence of compliance and regulations are requiring more disclosures. For an industry that prides itself on its agility and ability to move quickly, the show-your-work mindset does not come naturally. Technology companies need to understand all their reporting and disclosure needs, be able to access efficiently the information needed to respond to these needs, and review and analyse the information submitted for completeness and accuracy. Ideally, reporting, external assessment and disclosure requirements are managed centrally and proactively. Trying to respond to these needs on an ad hoc basis with responsibility distributed throughout the company increases the risk that reporting obligations will not be met or will be met late, and that conflicting information is provided.

Similarly, regulations like the DSA and the DMA mandate independent audits of the compliance programs of technology-platform companies. Documenting risks and controls, developing standard operating procedures, and ensuring that sample evidence can be generated are critical activities to guaranteeing the successful outcome of these independent audits.

Resourcing

An effective compliance program requires skilled resources who are vested with the authority, senior-level support, and resources necessary to direct and support a company's compliance efforts. In highly regulated industries (which the facts make clear include the technology industry), the compliance program is directed by a formal compliance function. For many technology companies where the concept of a compliance function is new, building the function will require recruiting talent from other industries, upskilling current personnel or a combination of both. It will also require rethinking the roles and responsibilities of others throughout the organisation and establishing rules of engagement for how different parties and groups partner to achieve the company's compliance objectives. Many factors influence what the right compliance structure may look like, including if an internal audit function exists, what role legal will play in the process of regulatory compliance, and the company's overall risk appetite and compliance strategy. This is not an easy undertaking and often will need to be an iterative process to determine the structure that best meets the company's needs.

About Protiviti's compliance risk management practice

There's a better way to manage the burden of regulatory compliance. Imagine if functions were aligned to business objectives, processes were optimised, and procedures were automated and enabled by data and technology. Regulatory requirements would be met with efficiency. Controls become predictive instead of reactive. Employees derive more value from their roles. The business can take comfort that its reputation is protected, allowing for greater focus on growth and innovation. Protiviti helps organisations integrate compliance into agile risk management teams, leverage analytics for forward-looking, predictive controls, apply regulatory compliance expertise and utilise automated workflow tools for more efficient remediation of compliance enforcement actions or issues, translate customer and compliance needs into design requirements for new products or services, and establish routines for monitoring regulatory compliance performance.

About the author

Kaitlin Kirkham-Cooper
Managing Director, Protiviti

Kaitlin Kirkham-Cooper is a managing director in Protiviti's Risk and Compliance practice, based in the firm's San Francisco office. Kirkham-Cooper, who focuses on risk and compliance issues affecting the technology industry, has more than 15 years of cross-industry experience working with clients to enhance their business performance by successfully implementing risk, compliance and governance change and optimising their risk and compliance arrangements. She can be reached by email at kaitlin.kirkham-cooper@protiviti.com.