Ahead of the Curve

Building a Resilient, Future-Ready Online-Safety Compliance Function

Kaitlin Kirkham-Cooper
Managing Director, Risk & Compliance

Roxanne Miller
Director, Risk & Compliance

Bridget Ostojic
Associate Director, Risk & Compliance

Eli Valenzuela
Senior Manager, Risk & Compliance

protiviti®
Global Business Consulting

The pace of global online-safety regulation continues to accelerate rapidly as governments introduce more prescriptive rules to protect minors and at-risk users. Global jurisdictions are not only emulating established models such as the EU Digital Services Act (DSA) but also competing to introduce stricter requirements for online platforms and technology firms of all sizes.

A notable shift is the move from high-level principles to very structured compliance expectations — particularly in areas such as transparency reporting, where regulations like Brazil's Digital Estatuto da Criança e do Adolescente (ECA) and the EU DSA now mandate detailed, multielement disclosures of operational metrics.

As a result, technology platforms of every size, from well-resourced enterprises to small, young online platforms, must navigate an increasingly fragmented and overlapping regulatory landscape. Each jurisdiction layers its own distinct requirements, often overlapping or adjacent to one another, yet each demanding careful attention to its nuances.

For organisations operating with limited compliance teams, this means interpreting complex regulatory intent across several frameworks simultaneously, assessing the impact of those requirements, and having to prioritise response positions and solutioning decisions with far too little time and capacity to address them all adequately.

Doing nothing or too little is costly

All the while, regulators are moving quickly into enforcement, with investigations already underway in key jurisdictions such as the European Union and the United Kingdom following the implementation of the Digital Services Act and the UK Online Safety Act. The financial penalties for noncompliance are just the beginning.

For technology platforms whose core value proposition depends on user trust, data integrity and uninterrupted service, the deeper consequences — reputational damage, operational disruption and the erosion of user relationships that underpin their entire business model — can be far more devastating.

Beyond financial penalties, the consequences of doing nothing — or acting too late — may include reputational damage, operational disruption, and the erosion of user relationships.

Emerging regulatory observations

Over the past few years, dozens of new online-safety laws and regulations have been introduced globally, most centered on protecting minors and other vulnerable groups from harmful content. But what is most significant is not just the volume of new legislation, but also the fundamental shift in how that legislation is written.

Earlier frameworks largely imposed content-based prohibitions, instructing platforms on what they could not host. This new wave of laws is instead mandating how platforms must operate. Requirements for transparency reporting, algorithmic auditing, and accountability and ownership of risk are becoming standard features of modern online-safety regulation.

This is a profound change: Compliance is no longer demonstrated by the absence of illegal content, but also by the presence of documented, functioning systems designed to prevent it.

To prioritise effectively, many technology firms focus on two key factors: urgency and effort. Regulations with active enforcement (e.g., investigations or requests for information) or near-term requirements—such as reporting, audits, or product changes—typically take precedence.

Despite regional differences, regulators are increasingly requiring enforceable systems—not just policies. Operational readiness is becoming the defining measure of compliance success.

Table 1: *Across jurisdictions, requirements are converging around three themes: risk assessment, transparency and proactive operational controls.*

Jurisdiction*	Regulation	Most significant compliance obligation	Actions for technology firms
EU	Digital Services Act (DSA) — Article 28 Guidance	Conduct risk assessment for protection of minors and implement mitigation measures	Align to a standard risk framework; embed risk checks into product lifecycle; evaluate effectiveness of mitigations
Brazil	Digital ECA	Biannual transparency reporting; risk assessments relating to child safety	Build centralised data pipelines; institute standardised reporting; align moderation data sources
Indonesia	PP TUNAS	Child safety risk assessments covering age verification, parental consent, and profiling restrictions	Develop risk models; integrate into product design workflows; document processes
Australia	Online Safety Act (Phase 2)	Expanded monitoring of harmful content (e.g., self-harm, gambling)	Enhance classification systems; update moderation policies; scale monitoring
U.S. (South Carolina)	Age-Appropriate Design Code (AADC)	External audits; implementation of controls to prevent harm to minors	Establish audit-ready documentation; strengthen data protection and child safety controls

Strategic recommendations for technology platforms

A more structured and integrated compliance model is critical for companies to be able to manage complex requirements across many jurisdictions with lean teams. Here are some recommendations for tech firms.

1. Build a strong regulatory intake process

Leading technology firms treat regulatory intake as a core capability. Strong intake processes help teams quickly understand new requirements so they can:

- Assess applicability and potential business impact.
- Understand whether existing processes or controls currently address the new requirements.
- Translate new legal requirements into operational actions.
- Implement operational changes across product and/or process.

2. Eliminate fragmentation — the biggest hidden cost of compliance

A critical step in enabling efficiency in a compliance program is first understanding which internal processes support multiple regulatory requirements (e.g., age-assurances processes, complaint handling, etc.).

Once identified, and as a best practice, tech firms should develop one streamlined process that is compliant across regulations to reduce duplication, streamline workflows and improve consistency.

Practical ways to achieve this alignment include the following:

- Create a centralised inventory of regulatory requirements to ensure legal and compliance alignment on scope of work and roadmap.
- Use consistent methodologies for risk assessments and transparency reporting wherever possible (e.g., aligning inherent and residual risk calculation methodologies).

Tech firms should develop a streamlined process that aligns with multiple regulatory frameworks to reduce duplication, streamline workflows and improve consistency.

While some regulations require specific formats, standardisation can still be applied across core processes to improve efficiency.

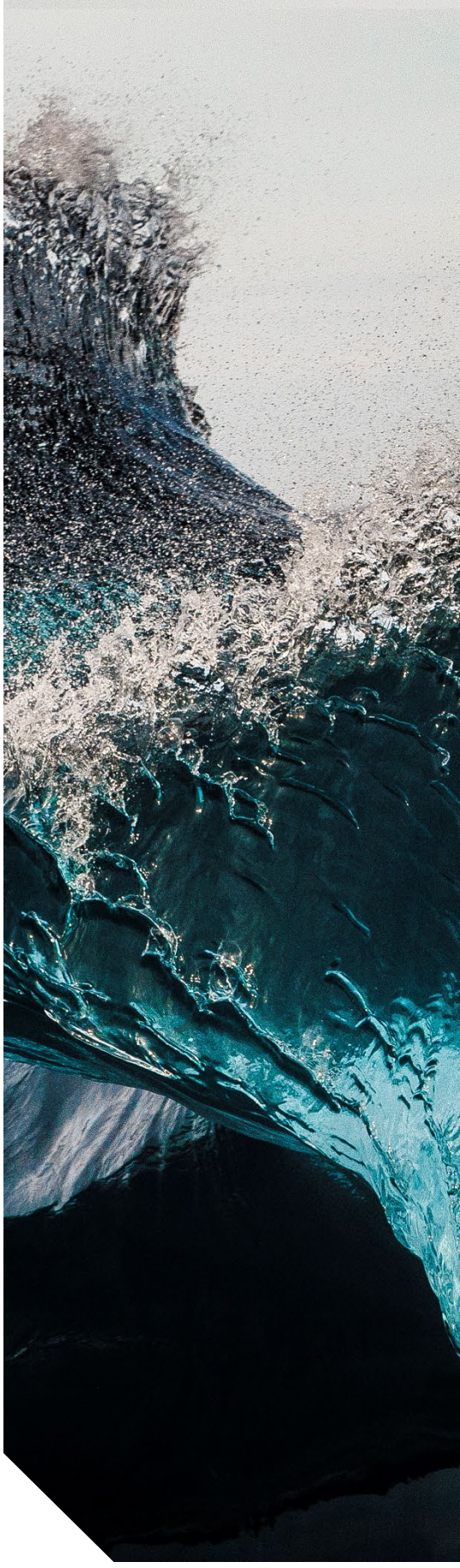
- Establish a structured process for identifying product and feature changes, with clear criteria to determine when these changes trigger new or updated compliance requirements.
- Design compliance controls that can be reused across multiple regulations (e.g., the DSA, the OSA, and Brazil's Digital ECA), rather than building separate solutions for each. This reduces duplication and makes it easier to adapt as new regulations emerge.

3. Embed compliance accountability at the business level

Leading organisations are moving beyond compliance-only support models and making business teams directly accountable for compliance as the first line of defense. In this model, compliance and legal functions provide independent oversight and guidance, while day-to-day responsibility sits within product, engineering and operational teams.

The following actions can help organisations make this shift and embed compliance into day-to-day decision-making:

- Through the regulatory intake process, assign specific compliance obligations (e.g., transparency reporting inputs, mitigation controls) directly to business teams.
- Incorporate compliance goals into performance metrics and leadership objectives so accountability is systematic and measurable, not informal.
- Assign accountability for documentation and reasoning behind key product decisions that are relevant to safety and/or compliance obligations (e.g., design choices, key risk indicators, exception handling logic and trade-offs considered).



4. Develop a strong understanding of regulator priorities and business impact

A clear understanding of regulatory priorities helps keep compliance programs and legal strategies aligned with emerging expectations. While many organisations have legal teams responsible for one-on-one engagement with jurisdictional regulators, keeping a pulse on regulatory action in the industry and among peer organisations can be a helpful way to identify future regulatory trends and focus areas proactively.

Beyond tracking new laws, organisations should monitor enforcement actions, regulator statements and published guidance. Without this, they risk focusing on outdated interpretations and misallocating resources. Here are additional recommendations:

- Take part in industry consultations, public comment periods and direct conversations where possible.
- Follow enforcement actions, official statements and regulatory publications to learn how requirements are interpreted and applied.
- Use insights from engagements and monitoring to inform resource allocation, training priorities and technology investments.

5. Leverage AI across the full compliance lifecycle

AI's greatest compliance impact may be its ability to expand capacity, not merely improving efficiency. It helps lean teams address more regulations with greater confidence.

Tech companies are increasingly using AI to support compliance activities — especially in areas such as regulatory monitoring, obligation mapping and reporting support. Here are additional ways to use AI proactively:

- **Impact assessment and obligation mapping**: Once new requirements are identified, AI systems can map them to internal processes, controls and systems, providing an initial view into gaps and areas requiring remediation.
- **Transparency reporting**: Some regulations require detailed disclosures across numerous data points. AI can automate

AI's biggest compliance impact may be expanding capacity, not just improving efficiency. It helps lean teams address more regulations with greater confidence.

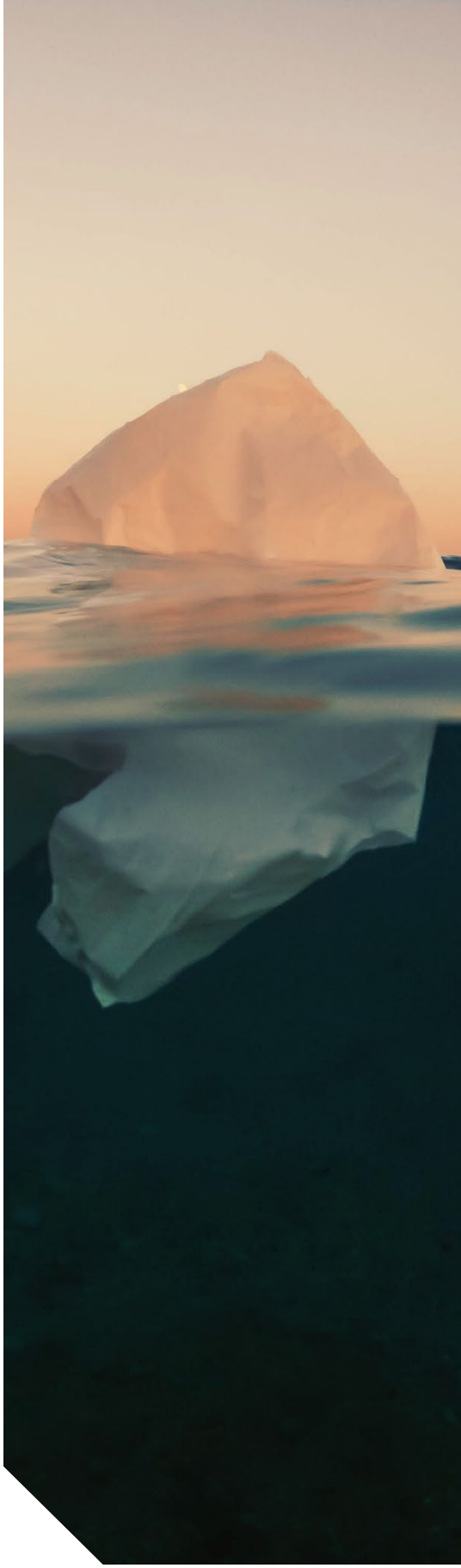
data collection across multiple systems, check for consistency, and help standardise reporting templates.

- **Continuous compliance monitoring**: Use AI to detect patterns and flag risks early — for example, identifying abnormal moderation outcomes before they escalate.
- **Advanced detection capabilities:** AI enables platforms to deploy more effective detection tools to identify, monitor and proactively remove illegal or harmful content. Additionally, AI can enhance quality assurance processes for moderation and evaluate the quality of automated and human decision-making.

A defining moment for compliance

Online-safety regulation has evolved to expect continuous oversight, increased transparency, and real-time answers to regulators, users and boards alike. To make these expectations a reality, reactive compliance is no longer a sustainable — or cost-effective — strategy.

This is a defining moment: Technology firms must build integrated, scalable operations that are nimble and adaptable. Those that move decisively toward this goal will earn user trust, strengthen resilience and shape what responsible digital platforms look like going forward.



About the authors

Kaitlin Kirkham-Cooper
Managing Director

Kaitlin is a managing director in Protiviti's Risk and Compliance practice, where she leads the Risk and Compliance Technology sector. She consults with large organisations in managing all types of regulatory and operational risks. Kaitlin has participated in compliance reviews and remediation projects for global technology and financial services and banking institutions, addressing various risks including privacy.

Roxanne Miller
Director

Roxanne is a director in Protiviti's Risk and Compliance practice working with technology and financial services organisations on compliance and operational risk management. Roxanne has experience in the United States and Asia Pacific regions with remediation and project management of complex regulatory issues, compliance program build and scale, compliance risk assessment, issue management, and internal audit.

Bridget Ostojic
Associate Director

Bridget is an associate director in Protiviti's Risk and Compliance practice and a subject matter expert in online safety. She advises technology clients on the fast-evolving regulatory landscape governing digital platforms, including the EU Digital Services Act (DSA) and UK Online Safety Act (OSA), while bringing broad experience across privacy, regulatory compliance, and enterprise risk management.

Eli Valenzuela
Senior Manager

Eli is a senior manager within Protiviti's Risk and Compliance practice, focusing on the technology and financial services industries. Eli leverages her project management expertise to support technology firms, evaluating their risk assessment processes. She has also supported remediation projects for large financial services companies.

Protiviti (www.protiviti.com) is a global consulting firm that helps clients transform and protect their businesses, and respond to planned and unexpected events. Through a network of more than 90 offices in over 25 countries, Protiviti and its independent and locally owned member firms deliver deep expertise and tailored capabilities across technology, artificial intelligence, data, operations, finance, legal, compliance, HR, marketing, digital, risk, and internal audit—enabling organisations to accelerate innovation, navigate risks and safeguard what matters most.

Named to the Fortune 100 Best Companies to Work For® list since 2015, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

protiviti®