Reinventing Compliance: Speed Up, Don't Trip Up!

BY **DAVID TOH**

As regulatory requirements grow more complex and interconnected, traditional compliance approaches risk becoming a drag on growth, innovation and organisational agility. Boards must therefore rethink compliance, not simply as a control function, but as a strategic capability.

The compliance ecosystem is becoming more complex and interconnected, driven by transformation, cross-industry reinvention and evolving business models. Global regulation, driven by macroeconomic forces and crises, continues to increase in complexity and cost.

Some companies have responded by evolving their processes and adapting their technology and talent models to mitigate risk, manage cost and generate insight more effectively. For others, increasing complexity has diverted management attention, strained resources and undermined confidence – affecting their ability to pursue strategic and competitive goals.

PwC's *Global Compliance Survey 2025* highlights the scale of the challenge:

- 77 per cent of respondents say their company has been negatively impacted, to some or a great extent, by compliance complexity across multiple growth-related areas.
- 51 per cent identified cyber security and data privacy/protection as top compliance priorities.

Compliance technology is helping companies improve risk visibility, respond faster to compliance issues, strengthen reporting and increase productivity and efficiency.

For boards, the challenge is not simply to ensure that the organisation complies with applicable requirements. It is to ensure that compliance supports, rather than constrains, the organisation's ability to adapt, innovate and create value.

The compliance ecosystem

Businesses today operate in a dynamic and interconnected risk environment across markets, value chains and industries.

Regulation is intended to support healthy markets, strengthen resilience and protect stakeholders. Compliance is therefore a baseline requirement for companies seeking to build trust and operate in a global market that increasingly expects transparency and high standards of conduct. An effective compliance system can also strengthen an organisation's ability to anticipate and manage risks, sustain competitive positioning and pursue new opportunities.

Regulation now touches almost every aspect of a company, including products and services, governance and transparency, reporting, taxation, sustainability, IT and data, ethics and behaviour, workforce matters, health and safety, and trade and sanctions.

Technology sits at the centre of many of these developments. Executives surveyed by PwC ranked technology highly on their compliance agenda, with cyber security and data protection/privacy among the leading priorities.

However, even Chief Information Security Officers report lower confidence than CEOs in their organisations' cyber compliance capabilities, highlighting gaps in areas such as artificial intelligence (AI), resilience and critical infrastructure.

Corporate governance, anti-bribery and anti-corruption, anti-money laundering and fraud also remain high priorities. Nearly 90 per cent of respondents reported that the breadth of their compliance responsibilities had increased over the previous three years.

At the same time, companies are entering new markets and sectors, creating new regulatory exposures. PwC's 28th Global CEO Survey in 2025 found that almost 40 per cent of CEOs believe their companies had started competing in new sectors over the last five years. As business models evolve and industry boundaries converge, companies are increasingly operating in unfamiliar regulatory domains.

Technology and data are reshaping both compliance strategies and talent requirements. The resulting risks are increasingly interconnected and cannot be managed in isolation.

AI is an emerging example. While ranked among the top three compliance priorities primarily in the technology, media and telecommunications industry, AI-related risks are expected to rise across industries. Organisations are developing AI usage policies and responsible AI frameworks to support adoption while managing associated risks.

The cost of regulatory complexity

The regulatory environment is increasingly viewed as a barrier to reinvention, with compliance complexity a significant contributing factor. 85 per cent of survey respondents said compliance requirements had become more complex over the last three years.

The impact is being felt across sectors, including financial services, industrials and services, consumer markets, health industries, and technology, media and telecommunications. More than three-quarters of respondents say compliance complexity had negatively affected their organisations across multiple growth-related areas.

The effects extend beyond the compliance function. 90 per cent of respondents say rising complexity had negatively affected their ability to implement and maintain IT systems and data. Requirements have also become more stringent across areas such as cyber security, AI, cloud, data privacy, operational technology, digital resilience and third-party providers.

There is a human cost, too. More than four in five respondents say that increasing compliance complexity affects their ability to transform. This is compounded by geopolitical volatility and the challenge of establishing enterprise-wide standards while navigating different requirements across jurisdictions.

Boards should therefore consider whether compliance processes are creating unnecessary friction. Rather than treating compliance as a standalone control activity, organisations should look for opportunities to embed it into broader business optimisation and simplification initiatives.

Technology at the heart of compliance

Technology is increasingly used to automate, optimise and accelerate compliance activities. Training, risk assessment, and compliance and transaction monitoring are among the leading use cases, followed by customer due diligence and regulatory disclosures and reporting.

More than 80 per cent of companies surveyed plan to increase investment in technology to automate and optimise compliance. Technology investment is already delivering benefits through improved risk visibility, faster identification and response to compliance issues, more insightful reporting and faster decision-making, contributing to greater productivity and efficiency.

Technology can also help organisations consolidate compliance and control activities by:

- Sharing technology across first-, second- and third-line teams.
- Mapping compliance controls across functions.
- Rationalising and consolidating data to provide a single source of truth.

However, technology is not a solution in itself. Data reliability and availability remain challenges, alongside gaps in skills and experience needed to manage and use data effectively.

AI presents further opportunities. Almost half of CEO respondents identify integrating AI into technology platforms, business processes and workflows as a major priority over the next three years. While most respondents believe AI will have a net-positive impact on compliance, nearly a third have yet to pilot or use AI for any compliance activities.

The hesitation is understandable. 89 per cent of respondents expressed some or significant concern about data privacy and security in relation to AI adoption, alongside concerns about misuse and

Guidance for Boards

As the compliance landscape evolves, boards should consider three priorities.

First, keep the compliance risk universe current.
The enterprise risk management framework should be reviewed regularly to ensure that it reflects changes in the operating environment, emerging technologies, business models and regulatory expectations. Boards should also have a dedicated forum for structured discussion of compliance risks, emerging trends and their implications for strategy.

Second, understand the business impact of compliance complexity.
Boards and management should work with compliance teams to identify where regulatory requirements are creating unnecessary cost, duplication or delays. Opportunities to simplify processes should be incorporated into broader transformation, data and workforce initiatives.

Compliance performance metrics should also strike an appropriate balance between value protection through risk mitigation and value creation through growth, efficiency and cost control.

Third, establish the foundations for responsible AI adoption.
Boards should oversee a responsible AI framework that supports confident adoption while addressing privacy, security, data quality, governance and decision-making risks. Compliance should also be incorporated into broader enterprise data and technology transformation initiatives.

Compliance leaders should identify practical AI use cases, align with the board on the target compliance technology environment and establish clear measures of return on investment.

misinformation, data validity, governance and AI-supported decision-making.

For boards, this reinforces the need to balance AI ambition with appropriate governance and controls (see box, "Guidance for Boards").

Staying ahead

The scale of regulatory change, shifting stakeholder expectations and evolving industry ecosystems mean that the traditional response of adding more people and controls is no longer sustainable.

A more strategic approach is needed. Compliance-by-design integrates technology, talent and strategic intent to streamline processes, improve connectivity across functions and embed data-driven capabilities within the organisation.

Done well, this can enable companies to anticipate risks and threats, navigate regulatory complexity with greater speed and confidence, and strengthen trust.

For boards, the objective should not be to choose between compliance and growth. The opportunity is to build a compliance capability that enables both, helping the organisation keep pace with regulatory change and market disruption, while creating the agility and confidence to stay ahead.

David Toh is President of the Institute of Internal Auditors Singapore.