McGrathNicol

FORECAST

2025

FOREWORD —

We expect that tough economic conditions will prevail this year. Geopolitical instability, cyber threats enhanced by AI, and supply chain and trade disruption will pose challenges to the way that Australian companies do business. The rise of authoritarianism and the new Trump administration in the US will mean that governments around the world become more inward-focused. Trade-exposed businesses will likely be the most impacted.

Insolvency numbers will remain high—at levels not seen since the GFC—due to structural changes in the economy, input cost inflation, and cost-of-living pressures. While the construction sector was responsible for the highest rate of insolvency appointments in 2024, local hospitality businesses have also been tested. The energy transition continues to drive structural change in the economy. Sectors including private health and residential aged care also face structural challenges. The current macro-economic settings are more difficult now than what businesses were facing a few years ago. We expect the lingering effects of inflation will keep consumer and business sentiment weak for some time.

A challenging business environment often correlates with increased risk and questionable decision-making by both executives and employees. Businesses are encouraged to prepare for and implement appropriate risk management frameworks to mitigate increased cyberattacks, insider risk, and corporate misconduct.

Australia's private capital markets are also going through a transition, with private debt almost surpassing private equity in funds raised. Private capital is increasing financing, funding business growth, and boosting shareholder liquidity which may be an attractive option for business owners while the IPO market remains relatively subdued.

We hope you enjoy our forecast and outlook for the year ahead.

Jason Preston
Executive Chair, McGrathNicol
+61 407 236 117
jpreston@mcgrathnicol.com

CONTENTS —

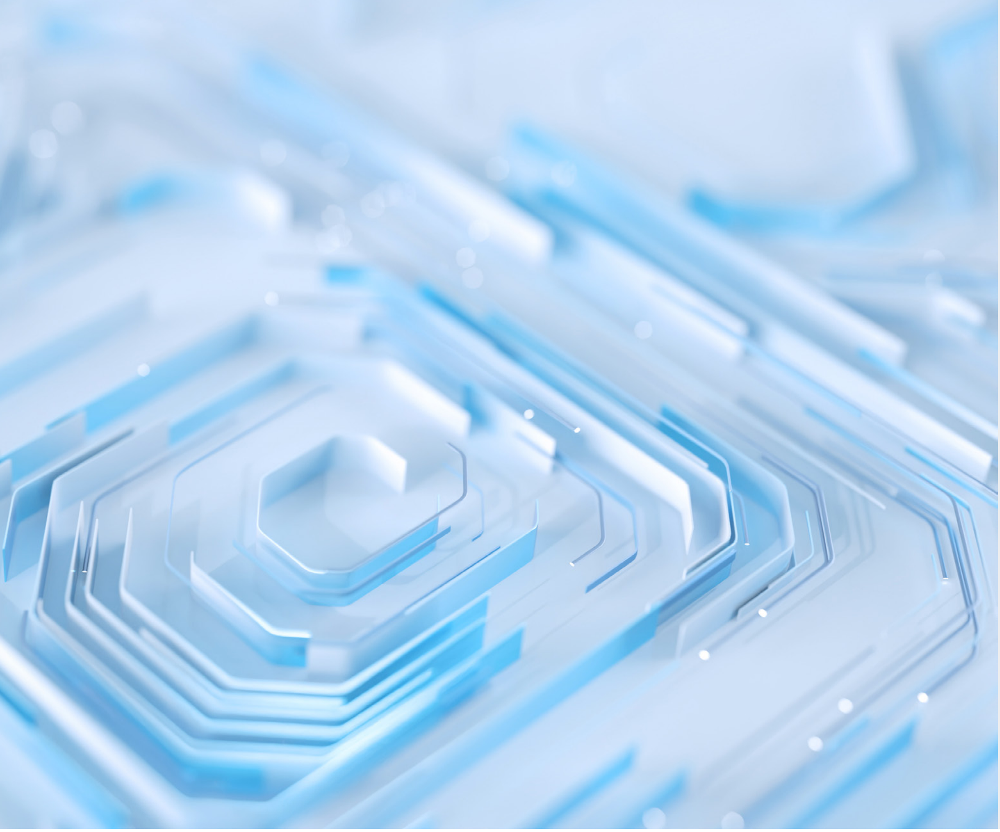
ARTICLES

AI and data governance delivers reward from risk

Data and AI governance has emerged as a critical roadblock for many enterprises, reducing their ability to address risk and seize the latest AI innovations. It has become clear that enterprises with good data governance are able to implement AI faster and take competitive advantage.

On the risk side, the rapid expansion of data-driven business operations create new vulnerabilities that require immediate attention. The exponential proliferation of data increases exposure to cyberattacks and the potential for reputational damage from misuse or breach. Enterprises must also navigate the recently amended Australian Privacy Act and global privacy standards which, if contravened, may result in substantial penalties and loss of trust.

One state government has recently imposed formal data governance compliance on all public entities and thousands of suppliers. The Western Australian Government's new Privacy and Responsible Information Sharing Act 2024 (PRIS Act) mandates privacy obligations governing data use, disclosure, sharing and security, reflecting a growing commitment to safeguarding personal information and ethical data requirements on third party government suppliers.



On the competitiveness side, organisations increasingly recognise mature data management and analytics capabilities as essential for reducing costs, growing revenue, and achieving tangible ROI from technology investments. Yet technical immaturity hampers the ability of most to leverage data strategically. This further acts as a handbrake on AI adoption, stifling innovation and slowing productivity promised by off-the-shelf AI co-pilots.

In 2025, enterprises will address this inertia by implementing data and AI governance programs that set clear policies and operational protocols for data access, usage, storage, retention and deletion. Organisations will make new investments in specialised technologies to handle discovery, classification, and compliance monitoring of the data they are processing at massive scale across sprawling technology environments.

Expert resources with the genuine experience needed to lead such programs are rare. Dedicated Chief Data Officers (CDOs) who can envision and implement governance at both the policy and technology levels, whilst aligning to business goals and managing inevitable organisational change, will be highly sought-after.

The cost of corporate misconduct

In 2024, allegations of governance failures, misconduct by senior executives, and toxic workplace cultures dominated headlines. At the same time, regulators launched investigations into large-scale price gouging, consumer exploitation, market manipulation, and breaches of Anti-Money Laundering and Counter-Terrorism Financing legislation. The damage from these scandals was far-reaching, with board and executive exits, volatile share prices and eroded public trust. Media coverage exposed systemic flaws in corporate governance structures and the challenge of balancing profit-driven goals with ethical obligations.

Looking ahead, we expect that tough economic conditions will prevail. History has shown, this often correlates with risk-taking and questionable decision-making, putting leaders in the spotlight for all the wrong reasons.

A review of the whistleblower provisions of the Corporations Act will likely enhance protections afforded to whistleblowers and we expect more social justice-driven individuals will come forward.

Mandatory climate related financial disclosures commenced on 1 January 2025. Shareholders, consumers and advocacy groups will continue to demand greater accountability, while

any misstep or violation is likely to invite significant regulatory and public scrutiny.

A High Court ruling in late 2024[1] may influence how corporate misconduct matters are pursued. The landmark ruling regarding "systemic unconscionable conduct" found that corporations think and behave through their systems, policies and practices. If those systems are found to disadvantage consumers, the corporation (and its executives) may be presumed to have acted knowingly and with intent and can be held directly responsible for such misconduct. This represents a departure in how these matters were dealt with previously.

2025 is poised to be a critical year for corporate accountability and legislative reforms. For corporate leaders, the balance between ethical obligations and business goals will remain both a challenge and imperative.

Source: [1] Productivity Partners Pty Ltd v Australian Competition and Consumer Commission Wills v Australian Competition and Consumer Commission [2024] HCA 2

Navigating cyber risks and building resilience

AI is rapidly transforming cybersecurity, offering advanced capabilities like predictive analytics and automated threat detection. However, the rise of AI-driven attacks, such as deepfake phishing and adversarial AI, underscores the need for organisations to adopt these technologies more strategically. To remain resilient and competitive, businesses must prioritise key areas that address both emerging risks and opportunities. Investments in defensive measures against malicious AI use will be as critical as leveraging AI for operational advantages.

Regulatory changes are also reshaping the cyber agenda. In Australia, this includes recent updates to the Privacy Act and the SOCI Act, as well as the introduction of mandatory ransomware reporting requirements. Robust governance and compliance strategies are essential to meet these obligations while maintaining stakeholder trust.

Critical infrastructure will remain a top target for cyberattacks, particularly ransomware and nation-state threats. Supply chain vulnerabilities will demand immediate attention as third-party breaches increasingly threaten broader ecosystems. Strengthened vendor risk

management, continuous monitoring, and targeted security improvements in procurement processes will be necessary to safeguard interconnected networks and ensure operational resilience.

Ransomware continues to evolve, with attackers employing multi-extortion tactics to maximise disruption and ensure payment. Our annual ransomware survey revealed that 84 percent of Australian businesses that have suffered an attack in the past five years paid a ransom. Further, 83 percent of businesses, including those yet to experience an attack, said they would be willing to pay a cyber ransom.

To counter these threats, organisations must implement comprehensive incident response plans, maintain robust data backup strategies, and prepare for prolonged recovery efforts.

Cybersecurity is no longer a discretionary cost; it is fundamental to building trust, ensuring business continuity, and creating competitive advantage. Organisations that adopt proactive strategies and leverage emerging technologies will be well-positioned to navigate escalating cyber threats and greater regulatory scrutiny.

Global instability driving increased security risk

Continued geopolitical instability, cyber threats enhanced by AI, and the rise of authoritarianism are pushing governments worldwide, including Australia, to strengthen their security posture. Based on President Trump's stated intent during his first year in office, we predict his administration will continue to drive for significant change in the global status quo during 2025—all of which will have a profound impact on Australia's security risk landscape.

A key driver of change will be growing tension in the Indo-Pacific region, particularly any US reaction to China's increasingly aggressive posture in the South China Sea and President Trump's follow through on his election promise to impose tariffs on all goods from China. As Australia attempts to harden itself to these external factors, organisations across sectors—especially those involved in critical infrastructure—will face heightened regulatory and compliance requirements. This will include increasing scrutiny over supply chains, the provenance of third-party suppliers, data protection, and system resilience to prevent both physical and cyberattacks. Organisations should prepare for increasingly stringent security requirements and greater scrutiny from government regulators.

The Australian Government will continue to tighten policies to safeguard critical infrastructure, with the Security of Critical Infrastructure Act expected to evolve in response to emerging cross-border threats. Expectations on businesses to demonstrate robust enterprise-wide security practices will grow and will require leaders to address the rising risk of foreign interference and intellectual property theft, particularly as geopolitical tensions fuel strategic competition.

The importance of securing sensitive data, establishing resilient communication systems, and adopting advanced cybersecurity solutions will be critical to mitigating these risks. Organisations that proactively invest in an enterprise-wide approach to security risk management and infrastructure resilience will be better positioned to navigate this complex and volatile environment, while those that fail to do so may face significant operational, financial, and reputational risks.

How CFOs can do more with less whilst remaining innovative

CFOs and finance teams have been grappling with the concept of innovation since the start of the decade. What began as a pivot to working remotely, and sustaining productivity during COVID, has evolved. We are now seeing the incremental automation of repeat activities and end-to-end redesigning of finance processes. The next tranche of investment for finance teams however, comes with dual challenges.

Broader market conditions mean that business leaders are becoming more cost conscious. CFOs are being asked to consider new technologies or capabilities while also lowering the cost of the finance function. At the same time, many CFOs have taken on new responsibilities around risk management, cybersecurity, and compliance. The Payment Times Reporting Scheme and incoming Australian Sustainability Reporting Standards are recent examples of newer obligations that are absorbing time and valuable resources.

So, in 2025, how can the finance function do more with less whilst remaining innovative?

Clear roles and prioritisation are crucial to delivering process efficiencies, as well as collaboration across the organisation to evaluate technology solutions, including AI and machine learning. Optimising finance team structures, leveraging external partnerships for transformation, outsourcing strategically, and adding specialised expertise will also enhance capabilities, mitigate risks, and help to manage costs more effectively.

Alongside cost control, effective cash flow management will remain critical for CFOs this year. Increased liquidity offers flexibility during tougher trading conditions and working capital cycles must be shortened to accelerate the conversion of earnings to cash. Proactive debtor management should begin when work starts, not when invoices fall overdue. Helpful measures may include agreed procedural steps, increased customer contact before invoice due dates, and a better understanding of customer billing cycles. Rolling 13-week cash flow forecasts should also be part of the CFO toolkit to help identify cash flow constraints or additional funding requirements early on.

Elevated corporate insolvencies set to continue

We expect elevated numbers of corporate insolvencies and challenging business conditions to continue in 2025, due to inflationary pressures, high energy costs, and poor consumer sentiment.

The slowing economy of Australia's largest trading partner, China, combined with heightened geopolitical risks, and new measures announced and potentially to be announced by the Trump administration, will likely threaten those exposed to foreign markets and trade dynamics. These factors, together with the approaching Federal Election, will pose uncertainty to Australian businesses in already challenging times.

We expect to see additional pressure being placed on businesses by the ATO, with their corporate plan 2024-25 setting out strengthening of debt collection as a key focus area, particularly in respect to the reported circa $50 billion in debt currently owed. In addition, the Federal Government has reported that, subject to the passage of legislation, from 1 July 2025 businesses will no longer be able to claim interest paid on overdue ATO debts as a tax-deductible expense.

For calendar year 2024, ASIC's insolvency data recorded a record number of insolvencies at 13,451,

with the construction and hospitality sectors accounting for 42% of all appointments. In 2025, we expect this trend to continue and the sectors impacted to widen. Economic pressures will continue to squeeze corporate margins, resulting in insolvency risk to unprepared and overleveraged businesses in the year ahead.

Insolvency rates will continue at elevated levels, with reductions in interest rates and easing of inflation the likely major catalysts to any economic recovery. This could reduce input and financing costs for businesses, improve consumer sentiment, as well as broader economic investment.

Both major catalysts are predicted to be a slow grind in 2025. The prevailing low AUD exchange will assist exporters and further erode margins of importers. There remains a wide range of capital providers interested in distressed companies. Successful outcomes are often realised through a formal restructuring process by the introduction of new capital providers.

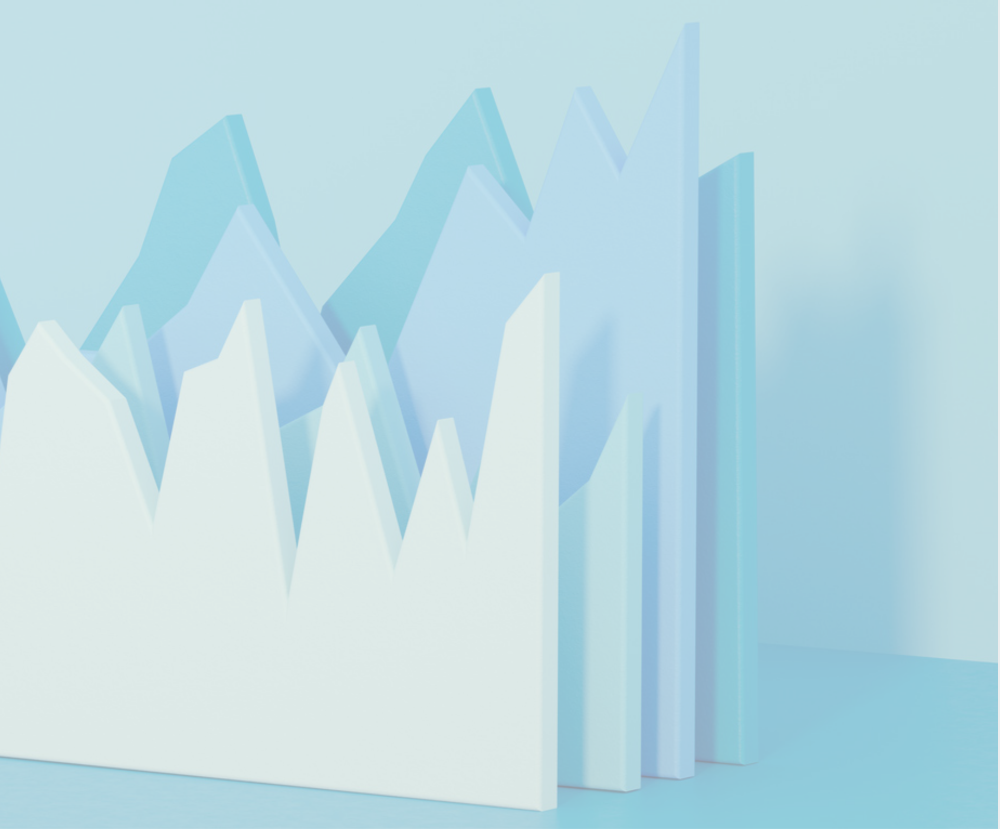
Capital markets in transition

Global markets are set for a shift in 2025, as central banks are poised to ease monetary policy. The overhang of geopolitical tension and tariff wars could push this to the second half of the year, however.

Private equity fund raising in the US declined for a third year, with 40 funds securing capital in 2024, less than half the 85 recorded five years ago. However, US PE deployment hit a record US$2.7 trillion, driven by improved financing availability. The higher rate environment has contributed to swing returns towards operational value creation, now 70% of PE returns, versus 18% only a decade ago.

Australia's private capital fund raising experienced a pivot to private debt last year. Until December, private debt fund raisings (28%) were greater than private equity (22%) for the first time.[1] Private equity fund raisings pulled ahead late in the year with a fund close by Genesis Capital and Quadrant Private Equity. Private credit and growth equity continue to be a serious alternative funding source for growth, shareholder liquidity, and for facilitating more creative solutions.

Despite the notable ASX listings of GYG and DigiCo on the ASX, these transactions were not sufficient to encourage investors to support other

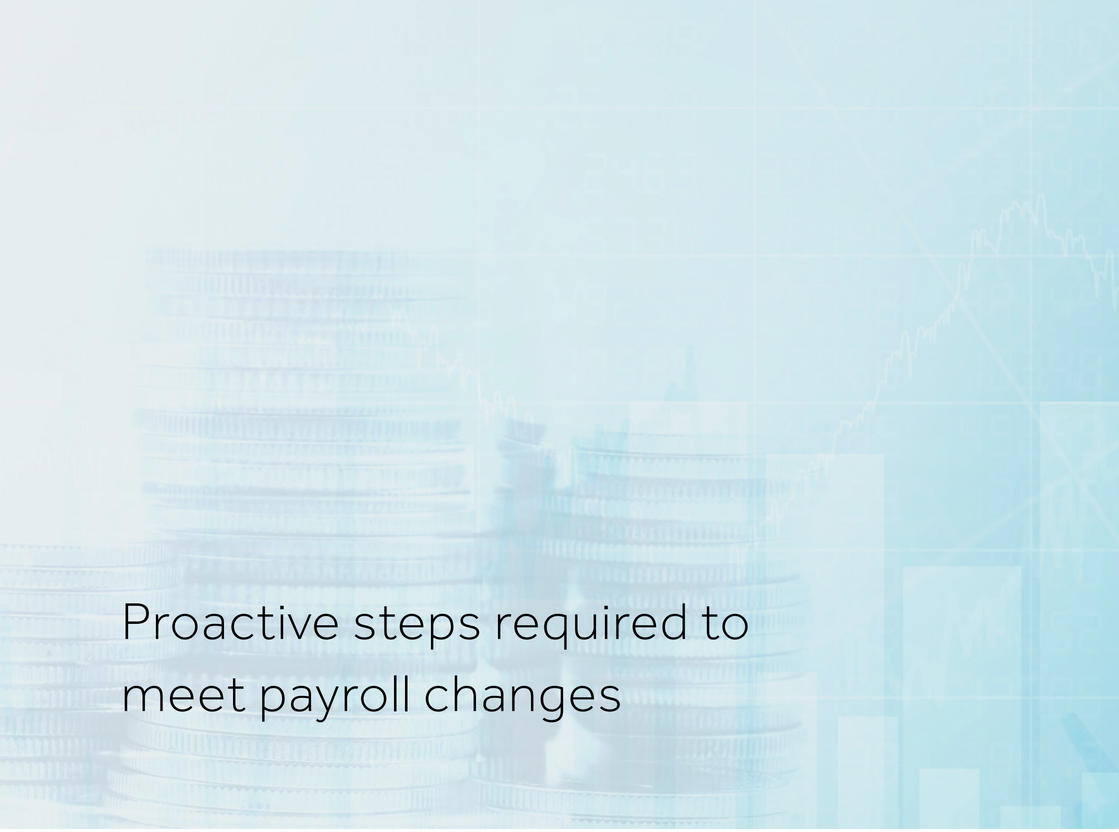


large candidates to launch IPOs, forcing financial sponsors and private owners to rely on recapitalisations, secondary exits, and stock-based mergers for liquidity. Sigma's merger with Chemist Warehouse for instance, highlighted how non-traditional deal structures provide a path to liquidity and are likely to become a more regular path to exit or liquidity.

ASX sell-side growth forecasts remain anaemic. Lagging the US, ASX200 earnings are predicted to grow only c.1% in 2025, and M&A activity may increase to fill the organic growth gap. Consumer-facing sectors may also seek to counter slowing demand, while B2B consolidation will remain focused on cost efficiencies and margin expansion.

Following several high-profile governance issues at founder-led firms, shareholder activist strategies could stage a comeback in 2025. Shareholders may become more alert and emboldened to employ activist strategies, such as pushing for board changes, asset divestitures, and improved governance to unlock value. This is counter to a backdrop of fund flows away from activist and short only funds here and abroad.

Source: [1] Preqin



Proactive steps required to meet payroll changes

Legislative changes will continue to reshape employers' payroll obligations this year. Since December 2023, the Fair Work Legislation Amendment (Closing Loopholes) Act 2023 has been introduced over several tranches, with the most recent tranche criminalising intentional wage theft from January 1. A proposed superannuation 'payday' obligation, although not yet enacted into law, is also slated for introduction from 1 July 2026.

Often, employers do not deliberately set out to underpay their staff. Many businesses are grappling with compliance due to the complexity of interpreting changes to awards, enterprise agreements, and other workplace entitlements. Common challenges include the misclassification of employees, failure to account for overtime, penalties, or allowances, and errors in calculating superannuation contributions. Outdated payroll systems, insufficient internal controls, and a lack of awareness of legislative changes compound these issues further. Underpayments can lead to significant financial and reputational risks including penalties, back payments, and loss of employee trust. Addressing these issues demands a

review of payroll practices, improved record-keeping, and ongoing investment in compliance measures to prevent future errors.

To ensure compliance with evolving payroll obligations, businesses must take proactive steps. This includes conducting regular payroll reviews to identify and rectify potential discrepancies, implementing systems to accurately track and process payment of employee entitlements, and updating payroll software systems.

Employers should provide comprehensive training to payroll staff on the latest legislation and maintain clear, up-to-date documentation of payroll records. Seeking advice from payroll advisors or legal experts can also help businesses to navigate complexity, mitigate risks, ensure compliance, and foster trust within their workforce and communities.

Restructuring activity at levels not seen since the GFC

Restructuring activity has skyrocketed to levels not seen since the GFC. The focus of recent mandates has shifted from tussles within capital structures to more substantive restructuring of fundamentally broken business models.

Over the past few years, COVID triggered the need for restructuring of many "good businesses with bad balance sheets". Lenders and sponsors could see a path to profitability and were comfortable providing support with some compromise. Many companies, sponsors and lenders acted swiftly and are now well-positioned to deal with the challenging market conditions expected in 2025.

Conversely, government stimulus and a historically low interest rate environment have hidden problems within some business models for years. Companies have woken to inflation, higher borrowing costs, and in many sectors such as gambling and healthcare, a heightened regulatory environment, creating a perfect storm for financial distress.

In circumstances where business models are broken rather than experiencing excessive debt, restructuring solutions will be more complex. This year, as the stakeholder landscape expands beyond capital

structure, more parties will need to agree to a compromise solution to avoid insolvency.

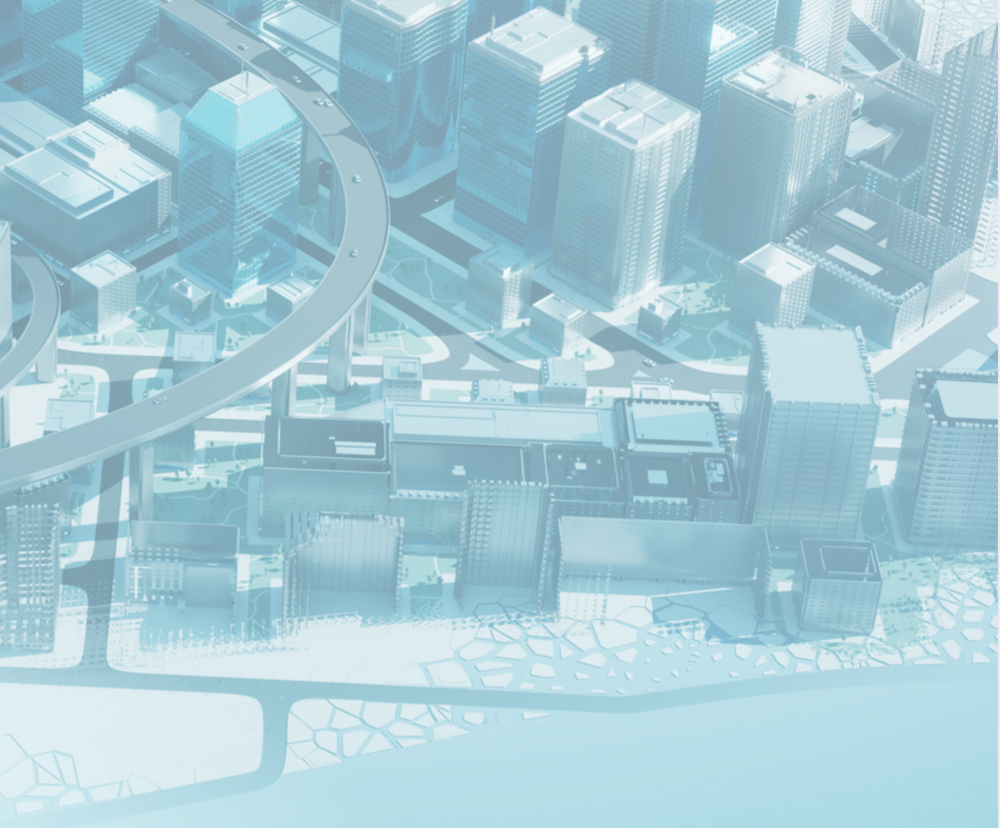
In determining who pays, restructuring will be characterised by a deep examination of legal rights and the testing of those rights against the economic leverage of the players involved in a distressed situation. We expect to see more regulators, suppliers, and customers coming to the negotiation table, as borrowers and financiers find themselves incapable of addressing broken business models on their own. The proliferation of private credit over the past decade will also introduce new faces. Negotiations will be further complicated by the existence of stakeholders with conflicting interests, particularly in heavily regulated industries where government has a major role to play. Negotiations will be tense. In 2025, more stakeholders will be asking the question, "Is the company worth saving?"

Disruption and costs driving supply chain strategies

Ongoing economic, geopolitical, financial, and regulatory changes will likely influence business decision-making and supply chain resilience. Key themes for the months ahead will include cost and inventory optimisation, ongoing industry consolidation, potential variations to major shipping lanes and sanctions, cyber threats, sustainability concerns, increased automation adoption, and upskilling.

While the need for resilience and disruption preparedness remains, supply chain leaders must also address value chain cost pressures to enhance business competitiveness.

Improved data analytics and AI will drive better cost-to-serve models as well as inventory and working capital transparency to facilitate faster decision-making. Already, operating model optimisation and service diversification is being expedited through M&A and the acquisition of emerging technologies, geographical network expansion, synergies, and market share. Meanwhile, cyber threats persist. Vulnerabilities are emerging from heavily data-driven operations, increased connectivity, data sharing with counterparties, and new technology solutions.



Regulatory and stakeholder expectations will continue to increase, with social practices and circular economy considerations now seen as a differentiator. Increased governance and related legislation in ethical sourcing and compliance tracking is likely to influence investment decisions about fleet asset electrification, alternative fuelled vessels, and technologies that can validate both internal and supplier ESG claims.

Investments in automation are expected to drive efficiencies and help in de-risking staff shortages. "Rentalising" capex into the facility lease, or securing new direct provider leasing options, will allow SMEs to access sophisticated solutions and automation. These new tools will require a trained workforce to successfully implement and reap the full benefits.

As firms prepare for disruption and bolster supply chain redundancy over the next twelve months, flexibility, proactivity and scenario planning will be critical. Strategic planning and business continuity exercises must contemplate both upstream and downstream threats across the broader supply chain partner pool, as an overreliance on a single supplier can pose increased challenges.