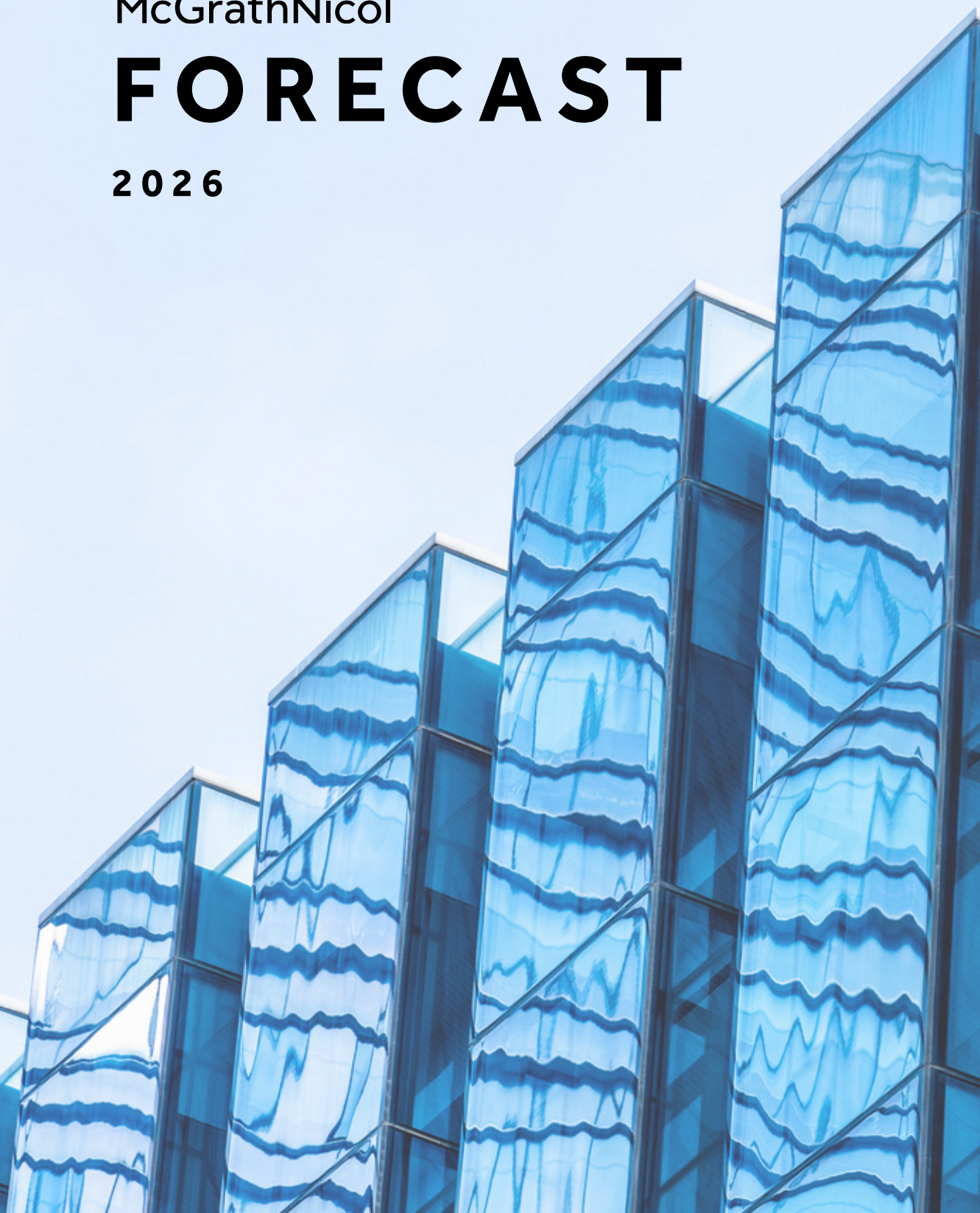
McGrathNicol

FORECAST

2026



FOREWORD —

2026 will reward organisations that recognise risk early and take action.

Global uncertainty will define the year ahead. Australian businesses are being tested by cyber and security threats, stubbornly high inflation, rising interest rates, and a constantly evolving geopolitical landscape. Add to this the accelerated pace of regulatory change, and 2026 is set to pose a major test of organisational resilience.

Gaps in supplier due diligence, data security and operational controls remain across too many organisations. These risks will only increase as legislative reform across Payday Super, anti-money laundering and counter-terrorism financing, and critical infrastructure requirements come into effect.

Threat actors are also weaponising AI to scale social engineering attacks and exploit zero-day vulnerabilities. Boards and management teams must elevate cyber resilience as a strategic priority; investing in both offensive and defensive AI tools, and embedding security measures across strategy, resourcing, and internal culture. Executives will continue to be held responsible for the actions of their critical suppliers, contractors, and service providers. Alongside these supply chain security and regulatory pressures, corporate misconduct risk is also on the rise. For boards, a failure to manage these risks may result in regulatory action, financial penalties and lasting damage to enterprise value.

Insolvency appointments are expected to increase, with input cost inflation and weak labour productivity growth creating margin pressures. We are already helping businesses manage elevated levels of distress across certain pockets of the economy. Labour-intensive industries such as construction, and sectors dependent on discretionary spending such as retail and hospitality, are likely to remain impacted. Australia's disability sector is undergoing significant structural reform, amidst funding challenges and market consolidation.

Despite this volatility, Australia remains a highly attractive and 'stable' target for global investors. Private markets continue to provide liquidity and, for good businesses that need lender support, private credit has created more restructuring options.

We hope you find our Forecast informative, and we look forward to working with you.

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

CONTENTS —

Local transactions buoyed by global demand

Growth expected, as investors seek stability

Australian M&A will increase, as global peers seek growth from stable markets and pursue unique technology, defence and resources targets. We expect accelerated demand for AI enabling infrastructure, cross border consolidation, and greater pressure on financial sponsors to deploy capital and monetise long-held assets.

The market is also bracing for regulatory complexity. As of 1 January, the ACCC's mandatory notification and merger control regime is in effect. There is also continued scrutiny of transactions involving critical industries from the Foreign Investment Review Board.

Owners and founders are exiting large, mature businesses with limited succession options. As more owners retire and look to sell successful mid-market businesses, Australia is experiencing an inter-generational shift. This will create strategic opportunities for international and domestic buyers as well as Private Equity.

Mid-market transaction activity was up approximately 40% in 2025. This trend is expected to continue, driven by continued public to private transactions. Corporate mergers and acquisitions are also off to an energetic start, with BlueScope Steel Australia recently receiving an unsolicited takeover bid.

The success of Virgin's IPO and solid post-IPO trading may also encourage sponsor-owned companies, with the market demanding well-structured, priced listings of quality businesses.

Private Credit continues to grow and is now the second largest class of open-ended funds, after Real Estate funds and overtaking Infrastructure funds.

With Private Equity and Private Credit dealmakers motivated to deploy capital and realise existing investments, we anticipate a broad range of transactions; from public to private sales, carve-outs, and leveraged buyouts. Exit transactions are likely to remain challenging. However, recapitalisations, continuation vehicles and share-based mergers can demonstrate value in 2026, if not completely realise liquidity.

Global uncertainty will define the year ahead

Strong market momentum in late 2025 and a record year for global M&A have driven surprisingly resilient corporate confidence. Global deal activity was up 40% and included several marquee US deals valued at over USD$5 billion. A resurgence in mega-mergers and undeployed private capital, combined with expectations for lower US interest rates, will drive continued momentum.

M&A activity in 2025 was helped by a 20% increase in private equity entries. The rebound in IPOs was also remarkable—up 54%—including six raises of over USD$1 billion and four initial valuations over USD$40 billion.

With over USD$2 trillion in undeployed capital, private equity players will place upward pressure on deal activity. New sources of flexible private capital across Sovereign Wealth, Infrastructure Funds and Family Offices will fuel activity and enable more complex deals with innovative financing structures.

Global private credit is set to exceed USD$2 trillion in Assets Under Management, continuing a structural expansion that includes broader asset backed finance and bespoke capital solutions. Larger deal sizes and rising participation from private wealth channels are expected, even as spread compression and increasing competition test underwriting discipline.

Despite improved availability of acquisition finance, uncertainty will remain a defining feature of 2026. Corporate acquirors will seek growth and global expansion, and dealmakers will need to respond to geopolitical manoeuvring as well as higher sovereign debt on currency and credit markets.

Key actions to take

- Prepare for deal complexity & heightened regulatory scrutiny – proactively assess the risks early and build strategies into your transaction timelines
- Unlock value upon exit – assess all available options and consider trade sales, strategic partnerships, recapitalisations or IPO options
- Engage early – build relationships with potential global buyers seeking stable markets and high quality assets

Why physical and supply chain security can't fall behind

For several years, executive attention has been focused on the digital threat landscape and the challenges of cyber crime. Investment in physical and personnel security and supply chain security is increasingly playing catchup. However, a more coordinated and integrated approach to enterprise security risk will be required in the year ahead. Organisations must understand the broader security landscape in addition to their own physical environments and actively manage supply chain exposure. Those that do will be prepared for future disruptions and regulatory scrutiny.

Reframing duty of care in a complex environment

Recent events, at home and abroad, have prompted a shift in how organisations protect their people and assets.

Physical environments, workforce related risks, and third-party exposure in complex ecosystems such as our critical infrastructure environment, will sit at the centre of this change.

Organisations are also reassessing their duty of care obligations. Boards will expect assurance that sites, events, and facilities are designed for modern threat scenarios that require rapid escalation capability, awareness of shifting crowd dynamics, and coordinated incident and crisis response. Traditional static assessments are no longer sufficient; more frequent reviews and scenario testing will become the norm.

Supply chain resilience will be tested

Organisations will be held responsible for the actions and failures of their critical suppliers, contractors, and service providers. This translates into a need for better visibility of critical suppliers and dependencies, greater contractual clarity around incident notification and response, and due diligence that extends beyond first tier relationships. McGrathNicol's third annual Risk and Security Report found 70% of organisations are failing to conduct due diligence on key suppliers and 71% are not considering their suppliers' own security as a key metric of performance and supplier evaluations.

With heightened global risk and regulatory scrutiny, there is increasing emphasis on data sovereignty, operational resilience and cross-border data risk. Prudential expectations, including under APRA standards, require regulated entities to maintain effective oversight of offshore service providers and to ensure continued access, control and auditability of critical data and systems. Similarly, amendments to the Security of Critical Infrastructure (SOCI) Act have expanded the range of entities subject to security and cyber obligations. This reinforces the need for organisations to identify where business-critical data is stored or processed, including offshore, and to assess risks associated with foreign jurisdictional access, supply chain dependencies and service disruption. Organisations that previously fell outside the definition of "critical infrastructure" may be subject to these heightened requirements.

Broadening regulatory scrutiny

Regulatory activity over the next 12 months will prioritise governance, transparency, and demonstrable control. Regulators will focus on practical risk management—including how decisions are made, how risks are owned, and how actions are recorded. Boards and executives should expect closer scrutiny of the assignment of security accountabilities and documentation of decision-making during an incident, as well as clear links between risk assessments and operational actions.

For Australian businesses in 2026, this means risk management programs must be tested to remain compliant, ensuring timely incident reporting and embedding proactive security measures across all cyber, physical, and supply chain operations.

Key actions to take

- Appoint a responsible person – nominate an experienced executive accountable for all traditional security domains
- Invest in crisis simulation training – ensure staff preparedness and implement clear command and escalation structures across your organisation
- Understand your supply chain – develop a supplier criticality framework and guidelines to better understand and maintain appropriate oversight of critical suppliers
- Consider broad SOCI requirements – regardless of whether you are captured under the SOCI Act, these standards should be applied as 'best practice' for organisational Enterprise Security Risk Management

AI-driven threats and rising regulatory demands

Cyber criminals continue to weaponise AI to scale social engineering tactics, exploit zero-day vulnerabilities faster than defenders can patch, and target the expanding attack surface created by supply chain platforms and connected devices.

Boards and management teams must treat cyber resilience as a strategic priority, invest in defensive AI and strengthen governance frameworks, uplift privacy and SOCI readiness, and establish an organisational culture that anticipates where threat actors will move next.

The next wave of cyber resilience requires business leaders to view AI as both a strategic asset and a potential vulnerability.

Threat actors are using AI to automate phishing attacks, generate deepfakes, and accelerate ransomware campaigns. In response, organisations are deploying AI tools to strengthen existing threat detection and incident response capabilities. Business leaders must continue to actively govern AI's defensive and offensive uses, ensuring ethical deployment, robust oversight, and ongoing education.

Prepare for increased enforcement action

Under the Cyber Security Act 2024, entities with $3 million+ turnover must report ransomware payments within 72 hours (effective May 2025).

In good news following the introduction of mandatory reporting requirements, fewer business leaders are paying and they are paying less. McGrathNicol research shows that the average cyber ransom paid has dropped to $711,000, from a high of $1.35 million in 2024. The pace of ransomware attacks is unrelenting however, and with 81% of Australian executives still 'willing' to pay, more work needs to be done.

The Privacy and Other Legislation Amendment Act 2024 also introduced sweeping changes, including a statutory tort for serious invasions of privacy and enhanced OAIC enforcement powers. By December 2026, organisations must comply with new transparency requirements for automated decision-making and the Children's Online Privacy Code. The Sydney Tools breach, which exposed 34 million customer records, underscores the real-world consequences of privacy failures. Regulators are expanding enforcement powers and increasing penalties under the new Act.

Similarly, ASIC has stepped up security-related enforcement actions with a clear link to directors' duties under s912A of the Corporations Act, and APRA's CPS 234 makes boards ultimately accountable for information security.

What does good cyber hygiene look like?

ASIC has taken action against organisations recently for failing to implement basic cyber hygiene controls. In doing so, they are sending a clear signal: directors are expected to own cyber risk, not delegate it. The Australian Cyber Security Centre's Essential Eight's updated guidance emphasises the need for phishing-resistant multi-factor authentication (MFA) and patching of critical vulnerabilities within 48 hours. Business leaders should also consider the applicability of other standards, including the updated SMB1001:2025 certification which complements global frameworks including ISO/IEC 27001.

Cyber risk poses a fundamental test of boardroom leadership. The pressing question is whether executive teams will take decisive ownership or wait until regulatory scrutiny or a major breach makes these decisions for them.

Key actions to take

- Embed cyber risk – set clear risk appetite and resilience objectives in governance frameworks and allocate resources.
- Uplift technical controls – align to the latest industry frameworks and upgrade your organisation's security measures to keep pace with evolving threats.
- Test and train – run cyber incident simulations involving executives and staff to identify critical weaknesses under the stress of realistic scenarios. A proactive approach will not only strengthen technical preparedness but also foster an organisation-wide culture of security awareness.
- Strengthen privacy protections – conduct a privacy gap analysis, map high-risk data processing, uplift breach response plans, and embed privacy-by-design into digital initiatives.

Converging operational, technology and compliance priorities

Regulatory change will accelerate across prudential oversight, payroll obligations, Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) reforms, and critical infrastructure requirements in the year ahead. Despite reported maturity, significant gaps remain across Australian businesses regarding supplier due diligence, third-party governance, data security, and operational controls, leaving many businesses exposed.

Organisations are encouraged to strengthen end-to-end assurance; adopting integrated governance structures and reporting across operational, cyber, and financial crime risks. Businesses must treat compliance not as a cost centre, but as a strategic long term investment in continuity and trust.

Here, we outline a number of key changes for executives to prepare for ahead of 1 July 2026.

Operational Risk and Prudential Oversight (APRA & CPS 230)

Significant for: All APRA-regulated entities

Organisations will need to extend control and assurance across their supply chain. Pressure will increase to finalise contract renewals and uplift arrangements with Material Service Providers (MSPs) to meet CPS 230's service levels, business continuity, as well as audit and monitoring rights requirements. APRA has also indicated targeted consultation on adjustments for Non-Traditional Service Providers (NTSPs), with an aim to provide a more practical and streamlined approach to market-mandated or non-negotiable arrangements. The 72-hour notification window for material cyber incidents will drive significant investment in internal reporting, triage, and forensic capabilities.

Scenario testing of critical business services will become a major focus for internal audit and external assurance, with APRA expecting greater organisational maturity in response, recovery, and communication.

Real-Time Payroll Compliance

Significant for: All employers

The commencement of "Payday Super" will fundamentally reshape payroll operations and cash flow management. The requirement for superannuation contributions to be paid at the same time as wages, and received within seven business days, will significantly increase the risk of non-compliance for organisations with fragmented payroll systems. The closure of the Small Business Superannuation Clearing House will also accelerate reliance on third party payroll platforms, particularly among small and medium sized employers.

In parallel, increased ATO funding and the expanded use of Single Touch Payroll Phase 2 data will drive a rise in automated compliance reviews. These reviews are expected to focus on superannuation guarantee shortfalls, award compliance, and employee entitlements. Payroll governance failures are likely to attract substantial penalties.

AML/CTF - Tranche 2 Reforms

Significant for: Accountants, Lawyers, Real Estate Agents, Trust and Company Service Providers

AUSTRAC's long-awaited AML/CTF reforms will mark a major regulatory uplift for the professional services sector. Newly regulated entities must rapidly implement full AML/CTF programs, including ML/TF risk assessments, Customer Due Diligence (CDD) processes, and Suspicious Matter Reporting capabilities.

The reforms will also intensify scrutiny of Ultimate Beneficial Ownership across complex corporate and trust structures, aligning AML/CTF obligations with the Government's broader focus on critical infrastructure security and foreign investment oversight under the SOCI Act and the Foreign Investment Review Board.

Key actions to take

- Integrate compliance – move away from siloed compliance functions. Treat cyber, operational risk, and payroll compliance as interconnected systems of risk that require integrated governance and reporting.
- Invest in automation – system upgrades are non-negotiable for Payday Super implementation and the accuracy required under STP Phase 2. For AML/CTF Tranche 2, automation of CDD and transaction monitoring will be essential.
- Validate your supply chain – conduct immediate, documented due diligence and contractual uplift reviews for all Material Service Providers (CPS 230) and critical technology partners.

The governance risks boards can't ignore

Corporate misconduct risk heightened in 2025, as evidenced by high-profile systemic governance failures across the Banking, Mining, Technology and Higher Education sectors. From financial crime investigations, workplace misconduct, and underpayments to alleged market manipulation, procurement fraud, insider risk, and whistleblower complaints, we expect these risks to grow. Key drivers are ongoing concerns about organisational cultures, conflict management, board transparency and accountability, and as regulatory bodies prioritise greater enforcement of directors' duties.

Trends in corporate misconduct have coincided with increased regulatory activity. ASIC has increased resources and announced its 2026 enforcement priorities including private credit and predatory credit practices, financial reporting misconduct, insurance complaints and claims handling, auditor misconduct, and strengthening the prosecution of insider trading. For boards, governance failures can result in regulatory action, major financial penalties, loss of valuable employees, and lasting damage to enterprise value and reputations.

The growing sophistication of fraud

Cost of living pressures and elevated insolvency appointments have created a challenging operating environment for lenders and corporates. At the same time, external fraud against bank and non-bank lenders is increasing, with organised groups exploiting these vulnerabilities across credit origination, asset finance, and commercial property transactions. On the law enforcement front, operations such as Elbrus and Strike Force Myddleton have highlighted the growing sophistication of criminal enterprises involved in PAYG payroll frauds and fraudulent loan schemes. We also expect a continued uptick in organised crime activities targeting the general insurance, NDIS, and construction sectors.

The reality is fraud threats will increase in both scale and frequency; organisations must be proactive in their detection and response.

Monitoring financial market integrity

ASIC continues to monitor financial markets integrity, examining market misconduct and insider trading allegations. Treasury is advancing reforms to create greater transparency in beneficial ownership and to combat corruption, tax evasion, money laundering, and terrorism financing. Meanwhile, the Australian Transaction Reports and Analytics Centre (AUSTRAC) will provide enhanced oversight under the Tranche 2 AML/CTF reforms that come into effect on 1 July 2026. ASIC is also emphasising audit quality, independence, and the extent to which management has been challenged on their assumptions. Audit committee effectiveness to ensure risks and professional judgement are prioritised over basic compliance is under the spotlight.

Following the collapse of two major Australian superannuation funds, the superannuation and insurance industries will face heightened scrutiny from the Australian Competition and Consumer Commission (ACCC) of complaints handling processes, opaque decision-making, delays, and instances of poor remediation cultures. Perceived failures will be scrutinised by regulators and the media alike.

Detecting the warning signs

Understanding these themes and the enforcement priorities of regulators like ASIC, AUSTRAC and the ACCC will help executives and their legal advisors respond decisively. To evaluate vulnerabilities and detect the early signs of corporate misconduct, executives must adopt a dynamic, evidence-based approach to monitoring and governance. This will support a strong risk culture, help to recover enterprise value, and build more resilient systems.

Key actions to take

- Map your specific threat landscape – identify where risk concentrates within your organisation and understand evolving tactics.
- Elevate insider risk management – deploy behavioural analytics, enforce least-privilege access and embed a culture of accountability across your high-risk senior roles.
- Address the human factor – invest in targeted training, simulations, and strong whistleblower programs. Reinforce ethical standards and psychological safety to reduce misconduct drivers.
- Engage independent forensic experts – ensure objectivity, avoid conflicts of interest and develop findings capable of scrutiny by regulators, boards, audit committees and the courts.

Little room for error, as conditions remain challenging

Macroeconomic conditions will remain challenging across many sectors. As input costs increase, additional interest rate rises are expected in the year ahead which will likely have a dampening effect on consumer sentiment and spending. These factors, combined with regulatory reform in certain sectors and possible geopolitical impacts on trade, will drive elevated levels of distress. Structural challenges in the economy, including the energy transition, will also contribute to increased restructuring activity.

The growth of private capital in the Australian economy, including both private equity and private credit, has led to higher levels of leverage. As a result, the room for error for business underperformance is severely limited.

In recent syndicated matters undergoing restructuring and involving a mix of traditional bank lenders and credit funds, debt has traded into the hands of credit funds that have taken a more activist role in restructuring situations. We have also seen lenders providing additional funding to support longer solvent runways and turnarounds.

Role of government in sectors of national significance

Governments are becoming more involved in large-scale restructuring matters, particularly in sectors and resources identified as being of national significance. As the machinations of government policy change, we will continue to see structural reform and resulting distress. Providers under the National Disability Insurance Scheme (NDIS) for example, are already under significant pressure. Heavily regulated sectors such as gambling, energy, healthcare, and the construction industry, will continue to raise public interest concerns that require government involvement.

Restructuring environment remains positive, if businesses are proactive

Amidst these challenges, the restructuring environment remains favourable. Since the introduction of the safe harbour regime in 2017, company directors have leveraged this personal liability defence and taken steps to negotiate with their stakeholders. In our view, this has mitigated circumstances that would otherwise have created higher levels of corporate insolvency in Australia.

The general availability of capital has meant there are more liquidity options available for 'good business, bad balance sheet' situations.

The growing presence of private capital in distressed situations will continue to impact negotiations—as providers are typically willing to deploy funds, or convert to equity-like instruments, to support favourable restructuring outcomes.

Sophisticated boards, management teams, capital providers and advisors are well-positioned to work through challenging situations in 2026 and preserve enterprise value. Companies that can recognise challenges early and develop proactive turnaround plans will be able to find support from existing lenders, or new capital if necessary.

Key actions to take

- Act early – engage with your stakeholders at the first signs of distress.
- Seek advice – lawyers, financiers and restructuring professionals can advise on Safe Harbour protections. Input from your stakeholders and advisers can preserve options and improve outcomes.

Structural challenges in economy drive elevated levels of distress

Insolvency appointments rose by 9% in 2025, and we expect this trend to continue. With input cost inflation and declining labour productivity growth putting pressure on businesses, distress will remain elevated and likely increase. While pressure will be felt across the economy, some sectors will be particularly impacted including hospitality, retail, construction and the disability sector.

Global geopolitics continues to create business uncertainty, including tariff volatility, US–China tensions and consequent flow-on impacts on supply-chains. Locally, inflation remains stubbornly high.

Australia's declining labour productivity growth rate remains a key challenge too for business leaders looking to manage rising wage costs. Unless higher wage costs can be passed on as price increases, margins will continue to be squeezed.

Industry focus

In the hospitality and retail industries, high inflation and the threat of future interest rate increases are already dampening consumer spending. Both sectors have experienced large-scale insolvencies recently. Throughout H1 2026, we anticipate a period of 'lower for longer' consumer sentiment.

Wages, operating costs, rent, utilities, and additional interest rate rises will make things challenging for businesses reliant on discretionary spend.

The construction industry experienced significant financial distress in 2025, albeit at levels consistent with the year before. Conditions will vary across states and territories, although we expect challenges around labour shortages and materials inflation to persist.

The disability sector is under strain. Over the past decade, the National Disability Insurance Scheme (NDIS) program has expanded exponentially. To remain sustainable, the Federal Government has implemented structural reform and recent changes to the sector's funding structure. Like aged care, any industry that is heavily reliant on grants or government funding will be susceptible to financial distress whenever these arrangements change. Larger operators can afford to be innovative and create efficiencies that make it difficult for smaller operators to compete. These factors will continue to drive consolidation in the sector.

Prepare for extended sales timelines

The implementation of the ACCC merger control regime may prevent transactions that otherwise could have helped a company to avoid insolvency. From 1 January 2026, it is mandatory for businesses to notify the ACCC of certain acquisitions and wait for approval to proceed. While aimed at preventing anti-competitive behaviour, this new requirement and longer approval timelines may also impact sales processes in an insolvency context.

Key actions to take

- Know your market – stay on top of trends and focus on providing your customers with value. Create efficiencies where you can without compromising on the quality of products or services
- Understand your liquidity – strengthen your cash flow forecasting and monitoring. Too many businesses monitor earnings, but not cash. Insolvency occurs when you're unable to pay debts as they fall due, i.e. when you run out of cash
- Engage expert advice early – speaking with experts early means you will have a clearer line of sight to cash flow, forewarning of distress, and likely more options to address it