



McGrathNicol

Energy, Supply Chain & Enterprise Security Risks

A resilience guide for Australian business leaders

May 2026

Business-critical vulnerabilities

Geopolitical volatility and energy market disruption are creating pressure across input costs, cash flow and supply continuity

Designed for management and leadership teams, this checklist will help you to better understand your biggest exposures, mitigate risks, test resilience, and respond proactively as conditions continue to evolve.



Supply chain vulnerabilities

Understand contracts, vendor pool, pricing and exposures

- Have you mapped where supply chain disruption is already being felt, and where it is most likely to emerge next across suppliers, geographies, routes and customers?
- Do you have a clear view of critical suppliers, their key inputs and points of failure, from raw materials to final delivery?
 - Have you assessed where suppliers are exposed to fuel availability, freight disruption, insurance, or war risk surcharges?
 - Do you have visibility beyond tier one suppliers for critical inputs?
 - Are you confident in the financial viability of your key suppliers?
- Have you modelled the potential impacts of higher input costs (COGS, labour uplifts, freight and energy) on both margin and working capital?
- Have you assessed where oil and gas is a critical upstream input (including feedstocks, plastics, packaging, fertilisers and pharmaceuticals), and the potential impact on your input costs?
- Do contracts allow for timely pass-through of disbursements or special levies?
- Are you invoicing quickly to mitigate adverse impacts on cashflow?
- Have you reviewed relevant government or industry support programs (e.g. Economic Resilience Program loans for impacted manufacturing and logistics businesses in critical sectors) and eligibility requirements?
- Are force majeure, hardship, escalation and termination clauses clearly understood and being reviewed?



Building supply chain resilience

Take practical steps to build resilience: strengthen governance, data monitoring, risk allocation, and decision cadence

- Is responsibility clearly assigned for monitoring fuel, network, freight and supply chain risks?
- Are the management team and Board receiving regular, forward-looking updates, not just backward-looking financials?
- Are there opportunities to improve resilience through supplier diversification, alternative routing, or targeted inventory buffers?
- Do you have access to the appropriate planning capability to increase flexibility and respond to demand variability?
- Do you have contingency plans for operating in a fuel-constrained or supply chain-disrupted environment?
 - Have you run war rooms or tabletop exercises for high-impact disruption scenarios?
 - Have trigger points, decision rights and thresholds been agreed so action is not delayed?
- Have you validated that your organisation could contain incidents quickly?



Cash flow management

Stress-test liquidity, working capital and margins so you can act early, rather than under pressure

- Have you updated cash flow forecasts to reflect higher input cost inflation and longer working capital cycles?
- What near-term actions could improve your working capital position (collections, inventory, payables, contract terms) and generate cash?
- What levers can you pull (pricing, surcharges, mix, cost deferral) to protect profitability?



Solvency & director risk

Know your runway, covenants and options early

- Have you stress-tested funding structures and covenants against downside scenarios and prolonged disruption?
- If short to medium-term cash flow appears challenging, have you considered funding options, including early engagement with financiers and capital providers to ensure flexibility as conditions evolve?
- Do directors understand the safe harbour regime, and has advice been sought on when and how the regime may apply?
- Are there contracts or business lines that may no longer be viable if input inflation can't be passed through, and should restructuring options be explored?

Proactively monitor second and third order risks

Beyond immediate cost and supply impacts, consider where second and third order risks may arise over time. These risks typically cut across operations, financial resilience, governance and security. While initially less visible, they can have a disproportionate impact on performance, solvency and governance if not identified early.



Growth, capital & strategic options

Balance growth, capital allocation and resilience priorities

Ongoing volatility is reshaping how organisations approach growth, funding and capital allocation to balance opportunity with resilience. Consider the following:

- Is there clarity on how growth objectives are being balanced with resilience, including implications for capital allocation?
- Do current growth initiatives need to be paused, re-scoped or re-sequenced? Should capital be preserved or redeployed?
- Are strategic growth opportunities being assessed through an appropriately risk adjusted lens, not just for strategic alignment?
- Does the Board have visibility over potential flow-on impacts of growth decisions in the current climate, including supply chain, cyber and governance risks?



Cyber resilience & enterprise security

Ensure cyber resilience supports continuity and decision making under pressure

In periods of geopolitical tension, cyber criminals are likely to focus on optionality rather than immediate disruption: establishing access, mapping dependencies and environments, and positioning to exfiltrate sensitive data or disrupt critical services at a time of strategic advantage. These campaigns are typically subtle, long-running and difficult to detect, while 'everyday' cybercrime continues in parallel.

- Have you mapped the attack surface beyond your perimeter (critical suppliers, MSPs/ SaaS, partners, and key data flows) and identified where compromise could create material operational, financial or safety impacts?
- Can you rapidly detect and investigate suspicious activity across applications, cloud, and networks?
- Do you have sufficient logging retention and monitoring coverage to support confident decisions under time pressure?
- Have you recently exercised key scenarios (credential compromise, ransomware, third-party breach, destructive attack)?
- Have you validated that you could contain incidents quickly (account lockout, network isolation, privileged access control) while preserving evidence and meeting notification obligations?
- Do you understand and have you reduced single points of failure (identity and privileged access, key person risk, and backups)? Is recovery designed to be safe (clean restore, segregation, immutable/offline options)?
- Are governance and controls keeping pace with automated threats and AI acceleration, including strong identity controls, hardening standards, and response automation with clear guardrails, segregation of duties, and forensic integrity?
- Is threat intelligence operationalised into actions (control validation, detection uplift, and threat hunting) and escalated to executives in business risk terms, with clear decision rights, escalation paths, and pre-agreed engagement with DFIR, legal, insurers, key vendors and government stakeholders?



Fraud, integrity & corruption risks

Understand and manage heightened fraud, integrity and corruption risks

Geopolitical volatility, supply chain disruption and operational pressure can increase reliance on third parties, accelerate decision making and weaken controls. Where urgency, discretion, and reduced oversight become normalised, instances of fraud, bribery and integrity risks increase. Boards and management teams should actively test where these pressures are being placed on procurement, payments and third-party relationships.

Foreign bribery risk

- Are third party agents, intermediaries and advisers subject to appropriate due diligence, oversight and ongoing monitoring?
- Are success based or contingent fee arrangements being used, and are the associated risks clearly understood and managed?
- Is there pressure to bypass controls or justify payments as unavoidable due to 'local practice' or urgency?
- Do directors understand how these scenarios could trigger liability under Australia's 'Adequate Procedures' foreign bribery offence?

Supply chain & procurement fraud

- Has urgency sourcing or exception-based procurement become routine rather than temporary?
- Are unexplained cost increases emerging, including freight surcharges, fuel premiums or retrospective price adjustments?
- Are new suppliers being onboarded without appropriate vetting, approvals or segregation of duties?
- Are contract variations increasing in frequency or being agreed after the fact?

Cyber-enabled fraud

- Are finance and procurement teams alert to phishing and business email compromise attacks using geopolitical events as a credible pretext?
- Are payment or bank detail change requests being independently verified, particularly where urgency is cited?
- Is there pressure to release funds quickly outside normal approval processes?
- Are near miss incidents being captured, analysed and used to strengthen controls before losses occur?

How we can help

McGrathNicol helps you improve performance, manage risk, and achieve stability and growth. Our teams bring deep technical expertise, commercial insight and a hands-on approach, working alongside clients to solve complex challenges and unlock opportunity. With offices across Australia and New Zealand and strong international connections, we deliver practical outcomes that help you make confident decisions and achieve lasting results.