# The Competitive Edge

A monthly operations knowledge boost

Issue #7

July 2026

By Maroubra Consulting

***Welcome to the seventh edition of The Competitive Edge: The monthly operational excellence knowledge boost from Maroubra Consulting.*** *In this edition we will look at transformation opportunities in the SMB segment, the convergence of cybersecurity and AI and organisational memory. Read on!*

# Transformation in the SMB segment: Opportunities through operational discipline

SMBs are entering a new phase. They need to grow, comply, protect customers, manage cyber and operational risk, adopt AI responsibly, and still operate with lean teams and limited investment capacity.

These pressures are not unique to companies in the SMB segment. Large institutions face similar challenges, but often struggle with their own scale, legacy complexity and slow execution. SMBs experience the same pressures differently: they are usually faster and more flexible, but often have less mature operating models, smaller teams, limited budgets and greater dependency on key individuals.

This makes transformation and operational excellence critical. SMBs need to build scalable ways of working before complexity becomes embedded.

SMB firms often face five common pressures:

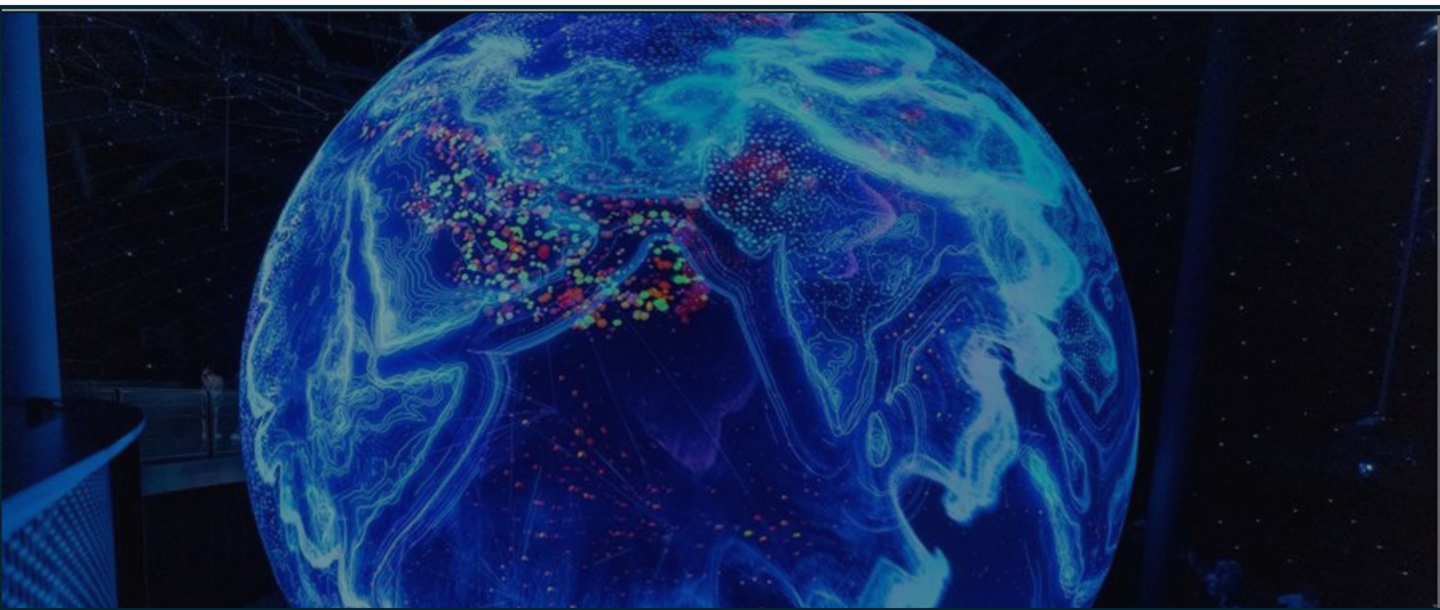
- Customers expect services to be simple, digital, fast and personalised.
- Regulators expect stronger controls around operational resilience, digital risk, AI governance, cyber security, data protection and third-party oversight.
- Investors are looking beyond customer acquisition and asking whether the business can scale efficiently.
- Technology investment must reduce complexity, strengthen controls and improve outcomes — not simply add cost.
- Fragmented manual processes and dependency on key individuals can create a gap between what the business promises customers and what it can consistently deliver

**The Opportunity: Transformation through Operational Discipline**

SMBs have an opportunity to use transformation and operational excellence to respond directly to these pressures. Their advantage is often speed, but speed alone is not enough. Transformation must be practical, structured and linked to measurable business outcomes.

There are five areas where SMBs can create value.

1. **Simplify the operating model.** As SMBs grow, informal ways of working can create unclear ownership, duplicated effort and operational drag. A simpler operating model clarifies who owns the customer journey, the process, the control and the decisions.
2. **Redesign core processes around the customer.** Core journeys such as onboarding, lending, payments, complaints and servicing should be designed around customer value. This helps remove friction, reduce rework and improve first-time-right outcomes.
3. **Embed compliance by design.** Compliance cannot remain a final checkpoint. By embedding obligations, controls, evidence and accountability into daily workflows, SMBs can scale safely and build trust with customers, regulators, partners and investors.
4. **Optimise technology, automation and AI investment.** Technology must create measurable business value. SMBs should simplify processes first, then use automation and AI selectively to reduce manual effort, improve decision-making, strengthen controls and enhance customer experience.
5. **Build a performance and continuous improvement culture.** Sustainable growth requires visibility of the right measures, including customer effort, cycle time, rework, control failures, cost to serve, productivity and risk outcomes. A strong performance rhythm helps teams solve problems early and keep transformation linked to measurable value.



**Conclusion**

For SMB firms, operational excellence is no longer a back-office improvement agenda. It is a strategic growth capability.

The firms that simplify their operating model, redesign customer journeys, embed compliance by design, invest in technology with discipline and build a continuous improvement culture will be better positioned to scale with confidence.

## 2. When Two Disciplines Become One: The Convergence of Cybersecurity and AI

Of quite different reasons, cybersecurity and AI have each become dominant forces in the modern enterprise. Both are growing fast, consuming an increasing proportion of organisational attention, budget and specialist capacity. Companies are expanding dedicated teams in both areas, and the business case for each is well established. What is becoming increasingly clear, however, is that the boundary between them is dissolving — and that organisations which continue to treat them as separate disciplines are taking a risk they may not have fully accounted for.

The convergence is not a future scenario. It is already structurally embedded in how both fields operate today. Cybersecurity teams are adopting AI to handle the scale and speed of modern threat detection — tasks that rule-based systems and human analysts alone can no longer keep pace with. At the same time, AI itself has become a cybersecurity and compliance challenge in its own right: model behaviour, data governance, access controls and audit trails are security problems as much as they are AI governance problems. The security team is, in this sense, already an AI team — whether the organisation has recognised it or not. Leading analysts at Gartner and Forrester are consistent on this point, and educational institutions are increasingly packaging the two disciplines into combined programmes, reflecting where practitioner demand is heading.

What this means for the specialist at the centre of both fields is significant. As noted in our previous edition, the automation of compliance and security monitoring is shifting team roles from execution to judgment. The same dynamic applies here, but with an additional dimension: the most capable users of AI in a cybersecurity context are not generalist AI practitioners — they are deep cybersecurity specialists who understand the domain well enough to interrogate what the AI is telling them. Four reasons the cybersecurity specialist is best placed at this intersection:

Strenght of judgement – does not come from formal IT education or skills, but rather a deeper understanding of the business process at hand.

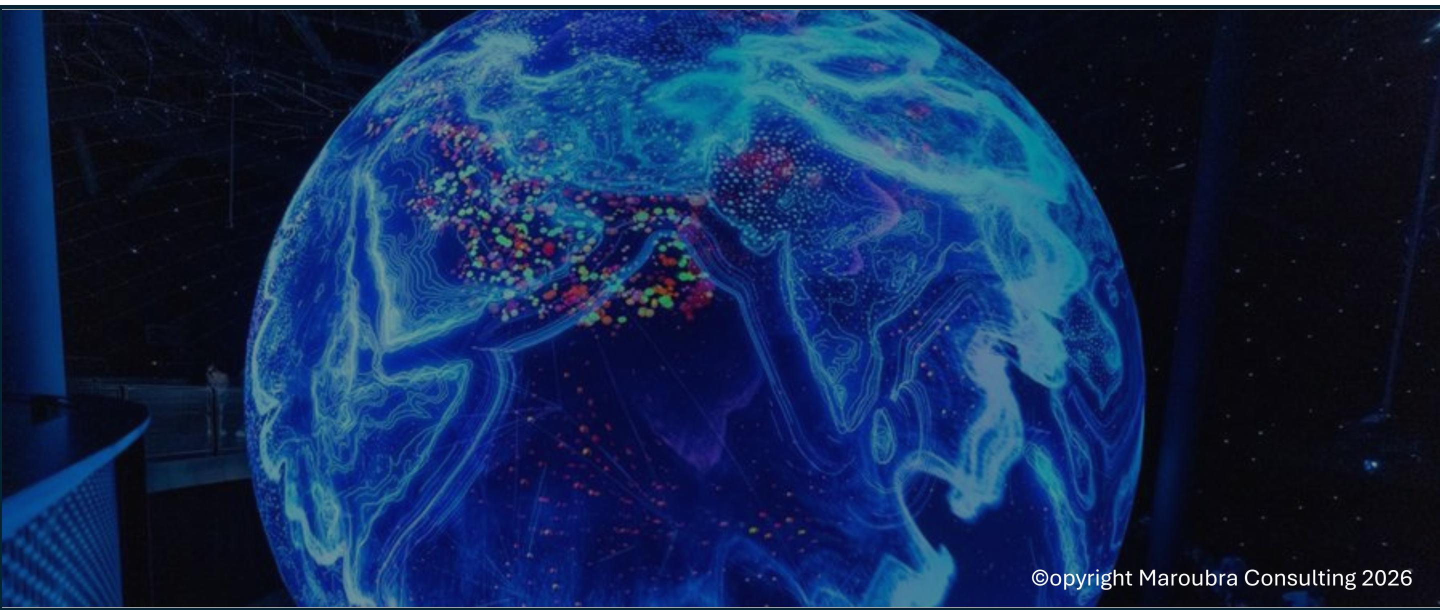
Domain knowledge to interrogate and challenge automated outputs, and to recognise where tools are missing critical context

Risk awareness to understand what failure actually means in operational and business terms — not just as a technical event, but as an organisational one

Governance and compliance experience to ensure AI operates within the regulatory and control frameworks that cybersecurity functions are already accountable for

Only staff with that background can make the judgment calls that matter when the stakes are high. AI adds capacity; domain expertise determines whether that capacity is used well.

Organisations that treat cybersecurity and AI as parallel workstreams will find the gap between them becoming a vulnerability in itself. Controls designed in isolation, teams that do not share a common language, and governance frameworks that have not caught up with the reality of AI-embedded security operations — these are the conditions in which things go wrong. The most resilient organisations will be those that deliberately converge the two disciplines: in how they design governance, how they build teams, and how they think about the competencies they need for the future.



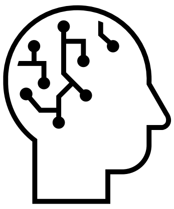
## 3. AI: Organisational memory, the new competitive advantage

For decades, organizations have invested heavily in systems designed to store data, yet far less attention has been given to preserving knowledge. Every day, valuable context is lost when employees leave, projects end, decisions go undocumented, or expertise becomes trapped within individual teams. Most businesses don't struggle because they lack information; they struggle because they can't easily access, connect, or reuse what they already know.

The growing adoption of AI is bringing this challenge into focus. While recent discussions have centered on increasingly capable models and AI agents, many organizations are discovering that the quality of AI outputs depends less on the intelligence of the technology and more on the quality of the organizational knowledge available to it. An AI system can only reason with the context it is given. If processes are poorly documented, decisions are not recorded, or knowledge is fragmented across emails, meetings, and disconnected systems, AI simply scales those limitations. In many cases, AI projects are exposing knowledge gaps that have existed for years but were previously hidden behind individual expertise and manual workarounds.

This is why organizational memory is emerging as a strategic priority. Companies are beginning to view documentation, knowledge management, process transparency, and decision history not as administrative tasks, but as business assets. The ability to capture not only what decisions were made, but why they were made, is becoming increasingly valuable as AI becomes embedded in daily operations. Organizations with strong institutional memory can onboard employees faster, reduce dependency on key individuals, and enable AI systems to operate with greater accuracy and context.

The organizations creating the greatest value from AI are often not those with access to the most advanced models, but those with the strongest foundation of institutional knowledge. As AI adoption accelerates, competitive advantage may depend less on who adopts AI first and more on who has built an organization that can remember, learn, and continuously improve from its own experience. In this sense, organizational memory is evolving from an operational concern into a strategic capability, and one that may determine how successfully companies scale AI in the years ahead.



### About Maroubra Consulting

Maroubra Consulting is an international management consulting firm, specialists in Operational Excellence. The company supports client organisations with improving competitiveness, strengthening operational resilience and achieving sustainable growth. With a 'global-first' and 'remote-first' business model, and market presence in Bergen, Barcelona, Amsterdam, San Francisco and Sydney, Maroubra Consulting combines strategic direction with digital innovation. The company proudly support the United Nations Sustainable Development Goal #1: No Poverty, partnering with NGOs to create lasting impact.