
THINKING · ENTERPRISE OPERATING SYSTEMS

The Living Organisation

Why the current executive agenda demands a system view

A reading of Australia's 2026 executive priorities, and the systems engineering principles that make it steerable.

AARON THOMAS GAICD · PRINCIPAL, SYSTEMIC ADVISORY · JULY 2026 · 18 MIN READ

Organisations are struggling with the operating system that AI has exposed, rather than with AI itself. Regulatory pressure, psychosocial safety obligations, sovereign data expectations and continuous change are entering across enterprises at a speed that a functionally designed structure was never designed to absorb. This paper positions the response as one of organisational design, not additional oversight, and offers three principles derived from systems engineering, Enterprise Traceability, Operating System Configuration and Capability Interaction Design, as the discipline that closes the gaps between functions.

Introduction

Organisational structure has followed a consistent pattern for 150 years. New technology has entered the market, been integrated as the priority, and organisational design has been treated as an afterthought. Prior to AI entering the market, this pattern

was sustainable because organisations were managed in functional groups and this was sufficient due to the slower pace of linear change. AI offers fast, deep analysis and the capacity to identify frictions across an enterprise at a scale not previously possible. That capacity is now exposing the pattern for what it is and creating an opportunity to evolve so that organisational design leads technology integration rather than follows it.

Australian boards and executives are navigating what the University of New South Wales has described as the transition from a digital transformation era to an uncertainty transformation period.¹ This new era treats trust, judgement and emotional intelligence as premium skills, providing the capacity to process the emotional weight of continuous change and embrace uncertainty as the operating condition rather than the exception. McKinsey's global research into organisational performance reaches an independent version of the same conclusion, describing transformation as a permanent condition rather than an episodic project and terming it business as change, where the operating model itself is built to absorb continuous change rather than periodically catching up to it.² Additional inputs into this era include AI integration, ongoing cybersecurity risk, evolving regulatory obligations, psychosocial workplace safety, and hybrid workforce configuration. Each of these operates on its own timeline and its own regulator.

The Australian Institute of Company Directors has captured the resulting priority pressure in the 1H 2026 Director Sentiment Index, which reports 68 per cent of directors saying regulatory requirements are limiting productivity growth in their business.³ The KPMG 2026 leader survey has independently identified AI, digital transformation, cyber risk and evolving regulation as the top four challenges facing Australian business leaders.⁴ The consistent feature across each of these priorities is that none of them sit inside a single function on the organisational chart; each is an enterprise-level impact and continuously evolving. Together, they constrain the ability of the organisation to meet requirements while sustaining and growing productivity. These challenges represent an organisational system problem.

Part 1. Historical context

The productivity paradox, a phrase coined by economic historian Paul David, has documented the pattern using electric dynamos as the anchoring case study.⁵ Electric

dynamos were commercially viable from 1882, but value was not realised until nearly 40 years later, around the 1920s. The delay was not a failure of the technology. It was that factories replaced their central steam engine with the dynamo and retained all other infrastructure. The productivity gain was only realised when factories redesigned their machinery, allowing production to be organised around material flow rather than around the constraints of power generation.

A similar pattern emerged with computers from around 1990. Computers were initially added into existing organisational designs, and productivity was not realised until they were integrated into redesigned organisations. This same pattern is now being realised across AI integration; AI has been bolted into existing processes and existing functional design. Leading research indicates that organisations which do not redesign are not expected to realise enterprise productivity gains from AI adoption.⁶

The value of AI is not in the technology itself. Like any technology, it is an input to the operating system. Like every general-purpose technology before it, the value is in the redesign the technology makes necessary.

Part 2. The evolution of organisational functions

The productivity paradox tells only part of the story. History also demonstrates that the evolution of organisational design has been reactive rather than deliberate. Each function in the modern C-suite can be traced to a specific pressure that exceeded what the existing structure could sustain.

Human resources traces to the industrial era, when Robert Owen first argued that improving factory conditions was inseparable from productivity, then to Frederick Taylor's scientific management, which needed dedicated staff to standardise and redesign work once factory floors had grown too large and too fast for an owner to organise directly.⁷ The CFO role did not emerge until the 1960s, consolidating through the 1970s as SEC and FASB reporting requirements outgrew what a financial manager or treasurer could handle without board-level standing.⁸ The CEO title appeared around

1917, when the first wave of large, merger-built corporations needed someone hired specifically to run functions and business units rather than an owner-manager doing it directly, but it did not become standard until the 1970s, when conglomerate-era firms restructured under competitive and economic pressure and needed one accountable executive separated from the board.⁹ Each position was created in reaction to a specific pressure or regulatory requirement, not designed as part of an integrated organisational architecture.

The pattern continued as new pressures emerged. The Chief Information Officer was named in a 1981 book, with an originally narrow purpose of managing data-processing procedures.¹⁰ The Chief Data Officer was created in 2002 by Capital One, driven by a compliance requirement, and remained rare until the 2008 credit crisis made data governance a regulatory necessity.¹¹ The strategic element of each role evolved over time, but each role was created in reaction to an external factor rather than as a considered part of the operating system.

The current wave is the most recent expression of the same pattern. IBM's 2026 CEO Study reports that 76 per cent of surveyed organisations have appointed a Chief AI Officer, up from 26 per cent one year earlier.¹² Predictions suggest that Chief Trust Officers, Chief AI Ethics Officers and other reactive roles are likely to emerge as AI integration continues and the technology evolves at pace.

The pattern that emerges from this history is that no executive function was ever created with an integrated design in mind. When HR was invented, it was not designed to integrate with finance, operations or technology, because those functions either did not exist or were not yet strategic. Each executive was given a functional domain of accountability, and the space between those domains was left unowned. That gap has remained unowned for over a century, one reactive addition at a time.

This pattern carries a risk that is easy to miss while reactive additions still feel like progress. Each new role adds another executive with a functional remit, and over a century the collective effect is an executive team that has come to resemble a department in its own right, with its own coordination overhead and its own boundaries to defend. A Chief AI Officer or Chief Trust Officer given a cross-functional mandate but no authority over the operating system illustrates the problem more than it solves it,

because the space that role is meant to govern was never assigned to anyone. IBM's own study found that 59 per cent of CEOs expect the Chief Human Resources Officer's influence to grow as AI matures, which raises the same question from the other direction. If AI is reshaping how work itself is organised and delivered, that sits closer to what a Chief Operating Officer already owns than to what HR was built for, and handing it to whichever function moves first is the same reactive pattern the rest of this history describes.

The systems lens points to a different response: redefining the boundaries of existing executive roles through deliberate redesign of the operating system, which is the more disciplined path than creating another position or stretching an existing one to cover ground nobody has properly assigned.

The introduction of AI has produced the first meaningful variance to this pattern. Some functional leaders are beginning to look at the connection between functions with new focus because the competing priorities landing on them cannot be resolved inside any single function.

Part 3. Three principles for enterprise practice

The paper argues that three specific disciplines close the gaps between functions. Each has been named to align with executive practice rather than technical documentation, and each is derived from a corresponding systems engineering principle used in the design and sustainment of complex technical systems.¹³ The three are Enterprise Traceability, Operating System Configuration and Capability Interaction Design. Together they form the discipline required to design, assess and sustain an organisation as a system rather than as a collection of functions.

ENTERPRISE TRACEABILITY

The capacity to follow strategic intent from the top of the organisation through to the individual and team activity that delivers on it. Derived from the systems engineering discipline of requirements traceability, it operates in the enterprise context as a live linkage between organisational purpose, functional accountability and operational execution. In many organisations, purpose is currently limited to strategic

documentation rather than embedded as a traceable design element. The executive question this principle answers is whether a particular activity, investment or decision can be explained by reference to strategic intent, or whether it exists for reasons that are no longer traceable, and whether all parts of the operating system are aligned in purpose and objectives down to individual layers.

OPERATING SYSTEM CONFIGURATION

The current state of an organisation's operating system across the capability domains that define it. Derived from the systems engineering discipline of configuration management, it operates in the enterprise context as the baseline picture of how the organisation is presently configured, rather than how it is described in strategy documents or organisational charts. The Enterprise System Health Check is designed to establish this baseline efficiently, using a common set of capability domains across every executive function to produce an evidence-based synthesis. The executive question this principle answers is what operating system the organisation actually has, distinct from the one it believes it has.

CAPABILITY INTERACTION DESIGN

The discipline of understanding and shaping how the capability domains behave when they interact. Derived from the systems engineering discipline of interface control, it operates in the enterprise context as the design of the space between functions, between the delivery system and the operating system, and between the organisation and its external environment. Most restructures and transformations fail on interactions that were not visible to the executives who authorised them. The executive question this principle answers is what else will change if a particular capability is altered, and where the flow-on effects will land.

The three principles are interdependent. Applied together, they allow the current state of the operating system to be understood, the strategic intent to be traced through it, and the interactions to be designed rather than discovered. This produces the same discipline that project delivery systems have historically provided for major investments, but applied to the operating system itself. This integrates the delivery system and operating system as a singular operating system.

Part 4. The executive priorities across the enterprise operating system

Applying the three principles to enterprise design, the operating system can be defined as a limited number of interdependent capability domains. This paper uses eight, chosen because they capture what an organisational operating system needs to be able to trace and design. The eight domains are Purpose and Objectives, Structure, Governance, People, Process, Technology, Data and Information Flow. These are offered as the minimal breakdown of an operating system under Enterprise Traceability and Capability Interaction Design.

Three of these domains have become living inputs to the organisation and highlight the continuous change environment, compounded by the speed of output AI enables. Purpose, Structure and Process are frequently evolving. Purpose and objectives shape what the organisation is designed to achieve. Structure shapes how accountability is distributed. Process shapes how the work gets done. Each of these can now be refined or expanded at speed using AI, which means the point-in-time documentation of each element is no longer able to keep pace with the change organisations are navigating. This creates a strong requirement for Operating System Configuration to be maintained deliberately, and for Capability Interaction Design to be applied when any of these three living domains is altered, so that changes are traced for flow-on impacts before implementation, rather than discovered after the fact.

The remaining five domains reflect the current executive pressures being felt across the enterprise. Australian public sector examples are drawn on frequently in what follows, because current policy and regulation in that sector are concentrated, current and public. The dynamics themselves are sector agnostic. A private equity portfolio company inheriting an under-designed operating model faces the same interface failure between value creation plan and operational reality. A mid-market business absorbing an AI-enabled workflow faces the same system impacts at smaller scale. A federated national body coordinating across independent state entities faces the same information flow challenge that a large government department faces across its own divisions. The mechanisms described here are constant across sectors.

Within the People domain, the Model Code of Practice on managing psychosocial hazards at work is now in force across every Australian jurisdiction, Victoria having completed the set in December 2025.¹⁴ Many organisations have responded through a new risk register and some online learning. Applied through a systems lens, the impact of psychosocial hazards would be considered deliberately across other interfaces, including Structure, Process and Information Flow. A specific example is the impact of AI or emerging technology capabilities on the workforce, including the potential for cognitive atrophy and its consequences for role design and structural configuration.

The Technology domain is currently centred on AI adoption. Gartner has predicted that 60 per cent of AI projects will be abandoned through 2026 because the underlying data was not ready for AI use.¹⁵ From a systems perspective, the linkage between AI and Data, Governance and Purpose is fundamental to AI integration, along with Enterprise Traceability across those domains. The current market response is largely siloed, with separate procurement for AI integration, governance and data readiness. This is producing projects with gaps that are not traceable and will not be visible until they fail.

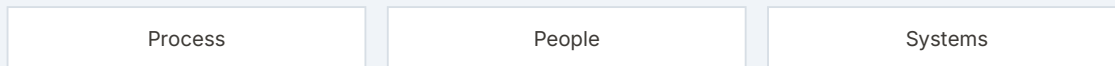
Data is often viewed as an isolated input to a specific functional need, such as customer data for operations or training data for AI, and current government practice tends to consider data in silo from other agencies. The systems approach identifies that Enterprise Traceability applied to Data, with clear Purpose and alignment to Structure, Process and the other domains, is fundamental to optimising the foundation of the enterprise operating system.

Information Flow is perhaps the least recognised domain, and yet the ability to trace how information moves internally and externally to an organisation is central to understanding the gaps between functions. Hybrid work is a topical example. Many organisations have adopted hybrid work policies with reactive, tactical workplace redesign.¹⁶ The absence of a systems approach has produced a measurable increase in shadow AI usage, which introduces significant risk to directors and executives across other domains, not least Data and Governance. The complexity of Information Flow increases in larger organisations such as government and defence, where each department is a system within a broader system. This typically produces duplicated lines of communication and accountabilities that are not consistently traceable. At the tactical level, an analysis of how many people are copied on an email chain as standard

practice, and what the productivity and decision-quality impact of that is, would itself be considered a systems input. As each of these domains is examined, the interconnectedness between them becomes evident.

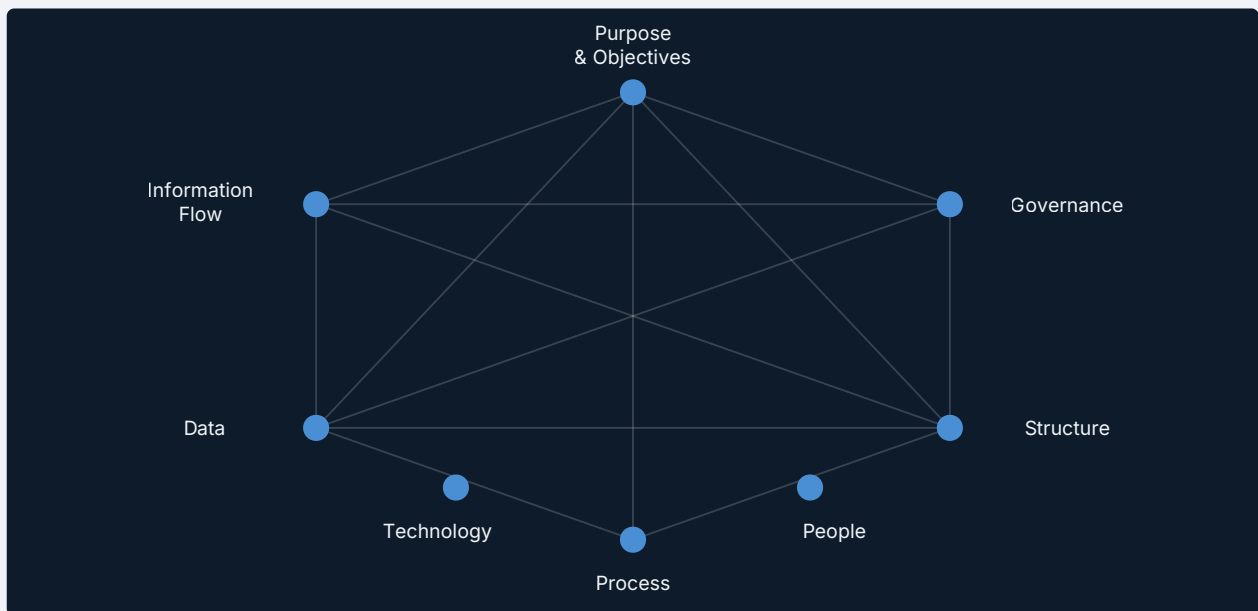
Enterprise problems rarely live in one domain. They emerge between them.

HOW MOST MODELS SEE IT · THREE SEPARATE BUCKETS



Symptoms get treated in isolation. The spaces between are nobody's job.

HOW THE ORGANISATION ACTUALLY WORKS · ONE CONNECTED SYSTEM



Assess the operating system. Not just the parts.

Figure 1. Silos versus one connected operating system. Illustrative.

Part 5. The gap in the middle

The strongest argument for applying an enterprise systems engineering lens to the organisation is that these executive priorities are more connected than they are currently being managed. Three interactions are described, each carrying material risk.

Psychosocial safety and AI adoption. The Code identifies low job control, lack of role clarity and poor organisational change management as psychosocial hazards. AI integration is a contributor to all three. Safe Work Australia has confirmed that risks

arising from artificial intelligence and digital technologies must be managed through the same risk management process as any other hazard, and that its model Codes on managing work health and safety risks and managing psychosocial hazards apply to them.¹⁷

Recognition is not measurement. There is no published Australian dataset, audit or evidence base demonstrating that psychosocial risk arising from AI adoption is being measured at any scale. Part of the reason is structural. Workers compensation claims are coded under the Type of Occurrence Classification System, which records mental stress by mechanism, including work pressure, harassment and bullying, and exposure to a traumatic event.¹⁸ A psychological injury arising from an AI-driven change to a role would most likely be recorded as work pressure, indistinguishable from a restructure or an unreasonable workload. The exposure is not absent from the national data. It is not separable within it.

The organisational consequence follows the same shape. In most organisations the AI governance arrangements and the work health and safety arrangements are held by different functions, assured separately, and reported to the board through different channels. That is a traceability failure across the Technology, People and Governance domains rather than a policy absence, and it creates legal risk, not merely productivity constraint.

Information flow and psychosocial safety. The same Code identifies poor communication and inadequate information as workplace hazards. When an organisation lacks the capacity to trace its information flow, or where flow is ambiguous, this generates efficiency risk and legal risk in the same failure point.

Data governance and director liability. Boards approving AI integration under the current governance guidance¹⁹ may not have considered the decision across all system domains, and the underlying assurance may not be traceable. Data used to support AI is drawn from the existing organisational design context, which may not be optimal and may not keep pace with continuous change. Gartner's finding that most failed AI projects trace to unready data is a board-level problem statement, not a technology one.

Part 6. The executive question

The question that matters for executives in 2026 is not how each priority is progressing in isolation. The question is whether the operating system beneath those priorities has established Enterprise Traceability, whether its current Operating System Configuration is understood, and whether Capability Interaction Design is being applied to the gaps between functions and external inputs.

Three sub-questions follow. Does the organisation have anyone responsible or accountable for the integrity of the enterprise operating system itself? When one capability domain changes materially, is there a formal approach to understanding the flow-on effects across the enterprise design? Can major investments or executive priorities be traced from organisational purpose and objectives through to the individuals delivering on that purpose, and is that managed well between the delivery and operating systems for those investments?

These are systems engineering questions being asked of executives on a regular basis. Recognising the questions is a good first step but understanding the discipline required to answer them is the second.

Conclusion

Executives and boards are navigating significant pressures that are impacting the enterprise holistically, at pace, with continuous change as the new operating condition. The next twelve months will see organisations choose between two paths. The first continues the reactive approach that history shows, and is likely to result in minimal productivity gains. The second undertakes deliberate organisational redesign and begins to manage the organisation as a living system. Australian public sector policy has already set conditions for this shift. The APS Strategic Commissioning Framework, ²⁰ now in its third year of implementation, is deliberately building that internal capability rather than outsourcing it.

Systems engineering has provided the discipline for the second path in complex, high-cost investment areas for decades. That discipline can now be offered to organisations more broadly. This paper does not describe how most organisations currently operate.

It describes what the current executive priorities are already implicitly asking for and offers a coherent way to read that request.

Executives who read their current agenda through this lens will find a structure that has been assembled for over a century, and a moment that finally asks them to design it.

Aaron Thomas GAICD

Principal, Systemic Advisory · Brisbane, Australia

SOURCES

1. Term drawn from the University of New South Wales, which frames the current period as the transition from a digital transformation era to an uncertainty transformation period.
2. McKinsey & Company, The State of Organizations 2026: Three Tectonic Forces That Are Reshaping Organizations, available at <https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-state-of-organizations>
3. AICD, Director Sentiment Index 1H 2026, available at <https://www.aicd.com.au/news-media/media-releases/2026/director-sentiment-index-1h26.html>
4. KPMG Australia, Keeping Us Up At Night 2026, available at <https://kpmg.com/au/en/insights/leadership/australian-business-leaders-top-five-challenges.html>
5. Paul A. David (1990), 'The Dynamo and the Computer: An Historical Perspective on the Modern Productivity Paradox', American Economic Review Papers and Proceedings, available at <https://gwern.net/doc/economics/automation/1990-david.pdf>
6. Erik Brynjolfsson, Daniel Rock and Chad Syverson (2021), 'The Productivity J-Curve: How Intangibles Complement General Purpose Technologies', American Economic Journal: Macroeconomics, available at <https://www.aeaweb.org/articles?id=10.1257/mac.20180386>
7. Skillscaravan, History of Human Resource Management, available at <https://www.skills caravan.com/post/what-is-the-history-of-human-resource-management-hrm>
8. Dirk M. Zorn (2004), 'Here a Chief, There a Chief: The Rise of the CFO in the American Firm', American Sociological Review, available at <https://journals.sagepub.com/doi/10.1177/000312240406900302>
9. Insigniam, A Short History of the CEO Role, available at <https://insigniam.com/a-short-history-of-the-ceo-role/>

10. William R. Synnott and William H. Gruber (1981), Information Resource Management: Opportunities and Strategies for the 1980s, summarised at <https://www.zrgpartners.com/insights/should-the-cio-be-re-titled>
11. Dataversity, The Changing Role of the Chief Data Officer, available at <https://www.dataversity.net/articles/the-changing-role-of-the-chief-data-officer/>
12. IBM 2026 CEO Study, reported via CNBC, available at <https://www.cnbc.com/2026/05/11/heres-how-artificial-intelligence-is-changing-boardrooms.html>
13. INCOSE Systems Engineering Handbook, available at <https://www.incose.org/products-and-publications/se-handbook>
14. Safe Work Australia, Model Code of Practice: Managing psychosocial hazards at work, available at <https://www.safeworkaustralia.gov.au/doc/model-code-practice-managing-psychosocial-hazards-work>
15. Gartner, Lack of AI-Ready Data Puts AI Projects at Risk, available at <https://www.gartner.com/en/newsroom/press-releases/2025-02-26-lack-of-ai-ready-data-puts-ai-projects-at-risk>
16. Croissant, 2026 Hybrid Work Predictions, available at <https://www.getcroissant.com/resources/strategies/hybrid-work-predictions-2026>
17. Safe Work Australia, Artificial intelligence (AI) and digital technologies, Managing risks, available at <https://www.safeworkaustralia.gov.au/safety-topic/hazards/digital-technologies-ai/managing-risks>
18. Safe Work Australia, Type of Occurrence Classification System (TOOCS), 3rd Edition, available at <https://data.safeworkaustralia.gov.au/about-our-datasets>
19. AICD and the Human Technology Institute, A Director's Guide to AI Governance, available at <https://www.aicd.com.au/news-media/research-and-reports/a-directors-guide-to-ai-governance.html>
20. APS Strategic Commissioning Framework, released October 2023, available at <https://www.apsc.gov.au/publication/aps-strategic-commissioning-framework>