THE **SOVEREIGN TECHNOLOGY** REPORT.

2026

FROM COMPLEXITY TO CONFIDENCE

kinetic IT

ADAPT

Kinetic IT acknowledges the Traditional Owners of the lands on which our crew, customers and communities live and work across Australia. We acknowledge the enduring connections Aboriginal and Torres Strait Islander people have with land, sea, and community, as the oldest continuous culture in the world. We pay our respects to the Elders past and present and commit to ensuring that we operate in a fair and ethical manner that respects Aboriginal and Torres Strait Islander peoples' rights.

This artwork was created by Gamilaroi and Wiradjuri artist Sean Kinchela for Kinetic IT's Innovate Reconciliation Action Plan (RAP). Learn more about our reconciliation journey online.

kinetic IT

DEAN LANGENBACH

CHIEF EXECUTIVE OFFICER
KINETIC IT

FOREWORD

Australian government and critical infrastructure no longer lack the ambition nor need persuasion to modernise.

The hard part is doing it well.

Sovereignty sits at the centre of this – not as a concept or policy, but as an operational capability: knowing who responds when something breaks, where accountability lies and how quickly an organisation can recover and get back on its feet.

In my first months as CEO of Kinetic IT, I have heard the same thing from customers and partners across government, defence, and critical infrastructure. Leaders are being asked to modernise faster while improving resilience, cyber maturity, and service continuity in environments with little tolerance for failure.

AI sharpens this pressure. The opportunity is real, particularly in sectors where Australia possesses deep operational expertise and world-class capability. But scaling beyond pilots raises challenges around governance, assurance, and accountability. The question unique to AI is who is answerable when an AI-enabled decision goes wrong.

None of this is an argument against global platforms – they remain essential. The risk is integrating them in ways that strengthen resilience and accountability, rather than hollow it out.

Australia has genuine advantages: strong institutions, world-class research, a highly skilled workforce, and hard-won expertise in large-scale, high-consequence environments. Turning those into durable capabilities that strengthens our resilience as a nation is the work ahead.

To explore how leaders are navigating this, Kinetic IT partnered with ADAPT to analyse survey data and executive insights across Australia's public sector, defence, and critical infrastructure. The finding is clear: the greatest challenge is no longer recognising the need to transform — it's executing transformation consistently, securely, and sustainably.

As one of Australia's largest privately owned technology services providers, Kinetic IT has spent more than 26 years in exactly these environments. This report is our contribution to that conversation.

> *Fiscal constraint translates into an incredibly immature decisioning environment in terms of acknowledgement of the realistic nature of technical debt.*
>
> **DIGITAL LEADER**
> *AUSTRALIAN STATE GOVERNMENT*

1.

EXECUTIVE SUMMARY

SOVEREIGN EXECUTION UNDER SUSTAINED PRESSURE

A clear signal from research gathered for this Sovereign Technology Report is that Australia's public sector technology agenda has moved decisively beyond strategy and ambition. Success now depends on the ability to execute under sustained pressure.

The research reveals strong momentum behind technology modernisation, cyber resilience and AI adoption, with all firmly positioned as executive priorities. Yet execution is increasingly constrained by operational reality, with 73 per cent of Australian public sector leaders identifying funding and resourcing pressures as the primary barrier to transformation.

Today's leaders are being asked to modernise faster, strengthen resilience, and accelerate AI adoption while continuing to deliver uninterrupted services in increasingly complex environments, without greater tolerance for failure or additional resources to support delivery.

WHAT IS SOVEREIGN EXECUTION?

Sovereign execution is the operational discipline of maintaining control, accountability, resilience, and evidence across modern technology environments, regardless of which platforms, vendors, or partners are involved.

Data residency matters, but it is not enough. Sovereignty is now tested well beyond where data is stored: who holds privileged access, who can act in the first hour of an incident, and who remains accountable when platform, personnel or partners change.

Sovereign execution is proven in moments of disruption and demonstrated in practice.

FIVE SHIFTS DEFINING THE NEW OPERATING REALITY

AI IS AMPLIFYING FOUNDATIONAL WEAKNESSES

AI adoption is advancing across government; however, governance foundations are the limiting factor. The Australian Government's mandatory AI guardrails and Essential Eight cyber security baseline set the foundation for safe AI deployment.

EXECUTION RISK IS LIMITING TRANSFORMATION SCALE

Operating model mismatch, skills shortages, and diffused accountability slow modernisation more reliably than technology constraints or investment levels.

DELIVERY CONFIDENCE NOW DEFINES PROGRESS

Delivery confidence is displacing delivery speed as the primary measure of transformation progress. What constrains progress now is the ability to operate, govern, and sustain modern platforms under pressure.

HYBRID IS THE NORM

Cloud migration remains incomplete across most agencies, creating a prolonged hybrid operating reality. On average, agencies report around 50 per cent of migrations complete; larger and more complex organisations are significantly further behind. Hybrid working practices extend the same pressures into home networks and personal devices.

PARTNER EXPECTATIONS ARE SHIFTING

Agencies are shifting what they value in delivery relationships: away from innovation speed, toward operational continuity and visible accountability.

WHAT THIS MEANS FOR LEADERS

Modernisation has become a sustained operating condition that requires sovereign execution embedded in governance, architecture, and operating models. Sovereignty functions as a practical decision filter: not just which platforms are adopted, but who controls them, who can respond in the first hour of an incident, and how accountability is maintained across partners, providers, and regulators.

Leaders are shifting how they evaluate and structure delivery relationships. Operational continuity, visible accountability, and responsiveness under pressure emerged as the most valued attributes, ahead of innovation capacity and cost efficiency. These are qualities that formal procurement frameworks have traditionally struggled to prioritise.

The chapters that follow examine what facilitates sovereign execution, and what separates environments that maintain control from those that lose it.

ABOUT THIS RESEARCH

METHODOLOGY

This report draws on two primary evidence sources: quantitative survey data collected by ADAPT, and qualitative executive interviews conducted in partnership with Kinetic IT.

ADAPT's research program covers Australia's technology leadership community across public sector, critical infrastructure, and regulated industries. The survey data referenced in this report draws primarily from ADAPT's 2025 Government Edge research series. Supplementary data is drawn from ADAPT's broader CIO Edge program where noted.

Executive interviews were conducted with senior technology, digital, cyber, and operational leaders across Australian federal and state government agencies, critical infrastructure operators, and defence organisations. Interviews took place under Chatham House Rules; all quotes are attributed by role and sector only, unless the individual has given specific permission. Kinetic IT executives are identified by name and role where quoted and are clearly distinguished from client and agency voices throughout.

Survey data was gathered in late 2025 and early 2026, and reflects the positions and priorities of respondents at the time of collection.

FINDINGS THAT CHALLENGED EXPECTATIONS

Six counterintuitive findings from the research

> *We're always trading something for something.*

CHIEF INFORMATION OFFICER (CIO)
NATIONAL MARITIME SAFETY AGENCY

FINDING ONE

THE REINVESTMENT RATE IS ZERO

Other long-lived government assets typically have ongoing funding set aside for maintenance, upgrades and renewal. Information technology (IT) often does not. Across executive interviews, no agency described having a formal annual reinvestment approach tied to the value of its technology environment.

0%

The proportion of IT asset value agency leaders described as being formally reinvested each year to keep assets current.

SOURCE: ADAPT EXECUTIVE INTERVIEWS CONDUCTED IN PARTNERSHIP WITH KINETIC IT, 2025 - 26

FINDING TWO

AGENTIC AI AMBITION IS OUTPACING READINESS

Agentic artificial intelligence (AI) sits on the investment priority list for 60 per cent of agencies. The share assessed as having the governance, data maturity and assurance mechanisms to deploy it safely is significantly smaller.

2%

Australian public sector agencies positioned to support autonomous AI safely under current governance and data conditions.

SOURCE: ADAPT GOVERNMENT EDGE AND CIO EDGE RESEARCH, 2025.

FINDING THREE

THE WIDEST CAPABILITY GAP IS IN DATA, NOT CYBER

Cyber security receives the most consistent attention in budget submissions and public commentary. In the survey data gathered for this report, the widest self-reported capability gap sits in a different domain.

74%

Government leaders report a severe or significant capability gap in data, analytics and artificial intelligence (AI).

SOURCE: ADAPT GOVERNMENT EDGE SURVEY, OCT 2025, N=87.

FINDING FOUR

MORE THAN A DECADE IN, CLOUD CAPABILITY REMAINS A CONSTRAINT

Cloud has been a stated Australian government IT priority since the first Australian Government Cloud Computing Strategy in 2014. The Foreword observes that cloud migration is progressing alongside cyber uplift, AI adoption and service digitisation simultaneously; the survey data indicates the capability foundations are still maturing.

64%

Government leaders report a severe or significant capability gap in cloud and infrastructure operations.

SOURCE: ADAPT GOVERNMENT EDGE SURVEY, OCT 2025, N=87.

FINDING FIVE

ERP MODERNISATION IS LESS ADVANCED THAN INVESTMENT SUGGESTS

Enterprise resource planning (ERP) modernisation is a top-three initiative. Nearly half of agencies have not moved beyond the planning phase; fewer than one in five are live and optimising.

45%

Still in planning mode

18%

Live and optimising

SOURCE: ADAPT GOVERNMENT EDGE SURVEY, OCT 2025, N=85.

FINDING SIX

THE SOURCING MODEL IS SHIFTING AWAY FROM HEADCOUNT

Agencies have historically scaled delivery capacity through individual contractor and staff augmentation arrangements. Survey data gathered for this report shows that pattern reversing, with comparable proportions of agencies reducing reliance on staff augmentation and increasing their use of specialist capability arrangements.

36%

Cutting staff augmentation

32%

Increasing specialist capability bursts

SOURCE: ADAPT GOVERNMENT EDGE SURVEY, OCT 2025, N=83.

2.

In critical infrastructure, the test of sovereignty is not compliance documentation. It is what happens in the first hour of an outage. Authority during an incident, clarity of escalation pathways, and proximity of response determine whether control is maintained or lost. Under the Security of Critical Infrastructure Act 2018 (SOCI Act), this is not a governance aspiration; it is an operational obligation with enforceable consequences.

DRAWN FROM INTERVIEWS WITH
CRITICAL INFRASTRUCTURE LEADERS

THE OPERATING REALITY: PRESSURE, CONSTRAINT, COMPLEXITY

Australia's public sector is operating under sustained structural pressure rather than episodic disruption. Transformation cannot be staged or deferred. Technology agendas are now defined by multiple simultaneous mandates: modernising core platforms, strengthening cyber resilience, preparing for AI, and improving citizen outcomes, while maintaining continuity of essential services.

Audits, regulators, and public accountability sharpen this pressure on government agencies. For critical infrastructure operators, the stakes are higher: service interruptions can have immediate safety-of-life, economic, and societal consequences. Under the SOCI Act reforms, cyber maturity, incident response capabilities, and risk management programs are operational obligations.

These pressures sit within a broader national policy architecture setting explicit expectations for how the Australian Public Sector (APS) designs, delivers, and governs technology, including the Data and Digital Government Strategy, the Australian Public Sector (APS) AI Plan 2025, and the Australian Public Sector (APS) Experience Design Principles alongside the Australian Cyber Security Strategy 2023-2030 and mandatory AI guardrails. Incident reporting thresholds, risk management obligations, and government assistance powers mean sovereignty extends beyond policy or data residency to the ability to act with authority during disruption.

In consequence-based environments, assurance must be continuous.

Modernisation is unfolding within increasingly complex environments. Hybrid cloud, shared platforms, and expanding partner ecosystems with hyperscalers and managed service providers are intersecting with legacy estates, and in critical infrastructure settings, with operational technologies (OT) and industrial control systems. The convergence of IT and OT adds complexity: the challenge is to transform without eroding control under stress.

Executives describe today's reality as one of sustained constraint. Budget pressure, legacy platforms, regulatory obligations, skills shortages, and low tolerance for disruption are enduring features of public sector technology and service delivery.

> ***"Service continuity is our function. That is what the public expects from us. Modernisation matters, but we cannot compromise on security or reliability just to move faster."***
> ***- Senior Technology Leader, Australian Public Sector***

$158.8 M

Average Australian government IT budget over the past 12 months, compared with $106 million for CIOs across all sectors.

> *What percentage of the total value of your IT assets should you invest every year to keep those assets current? The current percentage is zero*

DIGITAL LEADER
AUSTRALIAN STATE GOVERMENT AGENCY

THE BUDGET REALITY

ADAPT's research indicates the average Australian government IT budget over the past 12 months is $158.8 million, compared with $106 million for CIOs across all sectors. Yet despite these substantial budgets, funding and resourcing remain the top-cited barrier to transformation progress, suggesting the issue is not simply the size of the budget, but where and how that budget can be applied.

Viewed as a proportion of total agency expenditure or asset base, government IT budgets are broadly comparable to other sectors, reinforcing that the constraint is structural, not absolute. The problem is not how much is available, but the near-total absence of protected sustaining investment within those budgets.

ORGANISATIONAL GOALS FOR FY25-26 ACCORDING TO GOVERNMENT LEADERS

SOURCE: ADAPT GOVERNMENT EDGE SURVEY IN OCT 2025. SAMPLE SIZE: 138 AUSTRALIAN GOVERNMENT LEADERS

1. Developing the AI strategy and roadmap
2. Tech modernisation and simplification
3. Key capability delivery
4. Improving operational effectiveness
5. Optimising costs
6. Building a secure and trusted organisation
7. Pursuing broad-based digital transformation
8. Improved citizen experience and measurable societal outcomes
9. Ensuring governance and compliance
10. Creating a data-driven organisation

THE BUDGET PARADOX

The problem is not the total available; it is how budgets are structured and what they can be applied to. Annual budget cycles favour new investment over sustaining what already exists. Funding for transformation is competed for and approved; funding to maintain, refresh, and secure the existing technology estate is structurally absent from most planning frameworks.

> ***"What percentage of the total value of your IT assets should you invest every year to keep those assets current? The current percentage is zero."***
>
> ***— Digital leader at an Australian state government agency***

Technical debt accumulates not because leaders are unaware of it, but because the budget mechanism provides no natural vehicle for addressing it. Agencies then build transformation programs on top of an estate that is simultaneously modernising and degrading; every dollar of new investment carries a hidden overhead.

Public sector agencies face additional cost pressures with no private-sector equivalent: complex procurement frameworks, heightened governance and compliance obligations, and legacy estates that consume the majority of available budget before transformation begins. One leader managing a $1.4 billion ICT portfolio noted 70 per cent was absorbed by operations alone - a ratio that reflects structural reality across the APS, not poor management.

For agencies with Public Governance, Performance and Accountability Act 2013 (PGPA Act) obligations, this creates a specific accountability exposure: the requirement to maintain proper use and management of public resources does not distinguish between transformation spend and sustaining spend; however, the budget structures that govern most agencies effectively do.

STRUCTURAL CONSTRAINTS SHAPE WHAT'S POSSIBLE

However, this challenge extends beyond funding availability to a deeper structural tension: leaders must operate more complex environments, absorb new mandates, and modernise faster, yet tolerance for delivery failure has not shifted accordingly. ADAPT's data shows this creates a situation where ambition routinely outpaces what funding and capacity can actually deliver, with 73 per cent of leaders still constrained by limited funding with the full extent of technical debt rarely acknowledged.

While strategic expectations continue to rise, the barriers to delivery remain largely unchanged. Skills gaps are now among the most persistent inhibitors, with 31 per cent citing insufficient capability in their existing workforce and another 20 per cent reporting shortages in critical cloud, cyber, data, and AI roles. These pressures sit alongside competing priorities (32 per cent), which dilute focus and slow progress, even as leaders attempt to advance multiple transformation agendas simultaneously.

Legacy and organisational constraints further compound the challenge. Technical debt remains a drag on momentum for 15 per cent of leaders, while cultural and readiness factors also hold progress back. User resistance affects 16 per cent of leaders, low digital literacy 8 per cent, and outdated processes another 8 per cent. Regulatory and assurance requirements add another layer of complexity, with 7 per cent noting stringent or unclear obligations that reduce tolerance for disruption and reinforce the operational need for sovereign, resilient environments.

Leaders described these constraints as cumulative, driving a shift away from large, fixed roadmaps toward more controlled, iterative progress that protects stability while enabling incremental innovation.

ORGANISATIONAL BARRIERS ACCORDING TO GOVERNMENT LEADERS FOR FY25-26

1. Lack of funding/resources
2. Competing business priorities
3. Insufficient skills in the existing workforce
4. Insufficient staff in key roles
5. Adverse culture and user resistance
6. Legacy systems and technical debt
7. Data security issues
8. Insufficient digital literacy
9. Outdated processes
10. Stringent or unclear regulatory requirements

SOURCE: ADAPT GOVERNMENT EDGE SURVEY IN OCT 2025. SAMPLE SIZE: 132 AUSTRALIAN GOVERNMENT LEADERS

Sometimes I can see things that are dated, it's the way we used to write projects 10 years ago, but nowadays it doesn't work like that. I don't see who's going to make a budget on a tech investment for the year 2031... It doesn't make sense anymore. As a result, long-term transformation roadmaps are increasingly giving way to more cautious, iterative approaches.

SENIOR DATA SCIENCE LEADER
AT AN AUSTRALIAN FEDERAL
GOVERNMENT ORGANISATION

FOUNDATIONAL WORK DOMINATES THE NEAR-TERM AGENDA

As ADAPT's 2025 Government Edge survey data shows, investment is currently heavily skewed toward foundational work. Cyber uplift, infrastructure refresh, and ERP or core system modernisation feature among top priorities, while fewer agencies focus on end-to-end transformation programs.

Interviews for this report surfaced a recurring pattern: loss of delivery confidence forces agencies back to basics, stabilising what exists rather than building what is next. Leaders are therefore prioritising operational reliability and reputational security over accelerating change.

Loss of accountability or resilience during transition can carry consequences that outweigh the benefits of faster progress.

INVESTMENT PRIORITIES OF GOVERNMENT LEADERS IN THE NEXT 12 MONTHS

SOURCE: ADAPT GOVERNMENT EDGE SURVEY IN OCT 2025. SAMPLE SIZE: 139 AUSTRALIAN GOVERNMENT LEADERS

60% AI Agents

59% Enterprise Architecture

59% Application Development

57% DevOps / DevSecOps

59%	Governance, risk and compliance	**53%**	Cloud security (includes SaaS security)
56%	Cyber security skills, awareness and engagement	**53%**	Organisational Change Management - Design and implementation
54%	Application security	**53%**	Organisational Change Management

> *It is worse to deliver something that puts us at a risk of breaching our service or reputation... than keeping what is existing, even if we don't modernise it.*

DATA AND ANALYTICS LEADER
AT AN AUSTRALIAN FEDERAL GOVERNMENT ORGANISATION

EXECUTION NOW MATTERS MORE THAN AMBITION

Across Australia's public sector, constraints now extend beyond the strategic realm and into the operational domain.

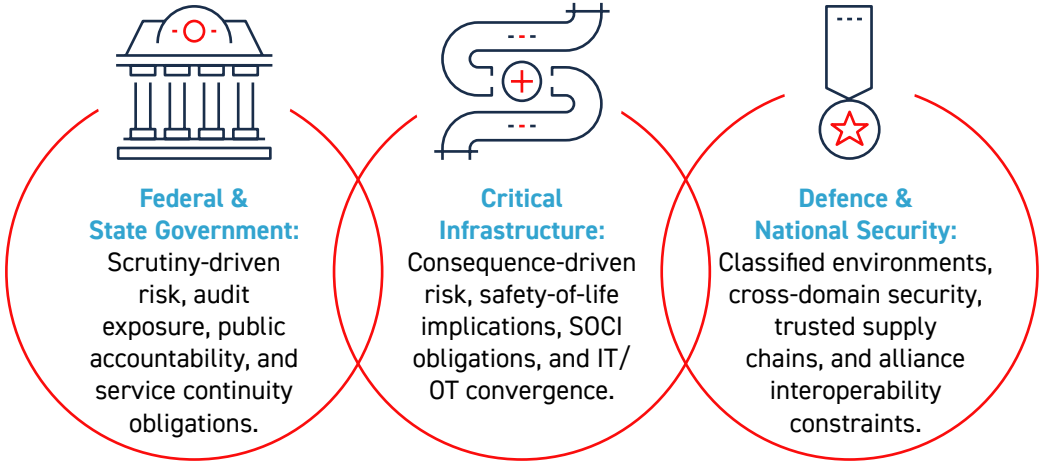
Research indicates delivery confidence, operational maturity, and assurance now carry as much weight as cost and capability in technology decisions. Ambition alone is insufficient. Success depends on the ability to operate, govern, and maintain modern platforms under pressure. Leaders are now evaluating technology choices through questions of control, accountability, resilience, and evidence before making technology investment decisions.

SECTOR OPERATING REALITIES

Agencies operate under ministerial oversight, audit scrutiny, and public accountability frameworks that require decisions to be defensible at any point in time. Under the PGPA Act, accountable authorities carry personal responsibility for the proper use and management of public resources, including technology assets. Sovereignty risk emerges most clearly in multi-vendor environments, where accountability fragments during transformation.

For critical infrastructure operators, IT and OT convergence extends sovereignty into physical systems where minutes matter. Incident response must be local, immediate, and authoritative.

In defence environments, sovereignty must be resolved at every layer of the stack. The Australian Signals Directorate (ASD) Information Security Manual (ISM), classified architectures and coalition interoperability frameworks such as AUKUS impose constraints on platform choice, workforce, and supply chain. Sovereignty is inseparable from national capability. If the pressure is this well understood, why do so many programs still stall?



3.

WHY TRANSFORMATION STALLS: THE EXECUTION GAP

Across Australia's public sector, the intent to modernise is clear. Cloud strategies are mature, ERP reform programs are underway, and digital roadmaps consistently prioritise consolidation, shared services, and data-led service delivery. Yet progress remains uneven.

ADAPT's research shows the primary constraint lies in the operating models, governance structures, and delivery capacity required to sustain modern environments. As platforms modernise, complexity increases, and the challenge shifts from whether to modernise to how to operate, govern, and scale transformation under public sector constraints.

Leaders indicated that execution is now the primary limiting factor.

> *"It's not the tech that holds us back... You can't just modernise a system. You need to modernise the people, the process, the way of working."*

EXECUTIVE DIRECTOR
AT AN AUSTRALIAN
STATE GOVERNMENT
EDUCATION ORGANISATION

CLOUD PROGRESS, GOVERNANCE LAG

Cloud adoption across government is well underway, but the transition remains uneven and ongoing. Agencies report an average around 50 per cent of migration complete, with larger organisations significantly below that average. ADAPT's longitudinal data shows in-house workloads declining from 61 per cent in 2020 to 48 per cent in 2025, with public cloud growing from 19 per cent to 24 per cent over the same period. The trajectory is clear; however, the pace is uneven and the governance overhead of extended hybrid environments is a material operating cost.

Most government agencies are operating in extended hybrid environments, with workloads spread across on-premise, private, and public cloud platforms. Rather than being a temporary stage, hybrid now represents a structural reality for government IT. This shift brings governance and operational complexity into focus: agencies face challenges such as unclear fiscal responsibility, distributed cost and usage data, limited visibility over legacy IT investments, and architectural constraints that drive unexpected costs.

> ***"Hybrid is no longer a stepping stone. It is the environment we have to run reliably for the foreseeable future."***
>
> ***— Digital Leader at an Australian State Government Agency***

In critical infrastructure environments, IT and OT convergence further complicates modernisation. Legacy supervisory control and data acquisition (SCADA) and industrial control systems were not designed for cloud-native governance, extending sovereignty and control questions into real-time operational domains.

ERP MODERNISATION AMPLIFIES RISK WITHOUT OPERATING MODEL CHANGE

Sovereignty in ERP reform remains one of the largest and highest-risk transformation initiatives across government. Survey data shows wide variation in ERP maturity, with many agencies still in planning or early implementation phases, and only a small cohort reaching stabilisation or optimisation.

Leaders emphasised that ERP programs amplify operational risk when legacy governance and delivery models are applied to modern platforms. During transition, agencies must operate parallel systems, manage data integrity, retrain users, and maintain compliance, without disrupting core financial, workforce, and procurement functions.

> ***"ERP programs do not fail because of technology. They fail when operating models, governance, and accountability do not keep pace."***
>
> ***— Chief Information and Digital Officer at an Australian Defence Agency***

Without enough delivery capacity, clear ownership, and operating model change, ERP initiatives risk becoming extended stabilisation exercises rather than platforms for broader transformation.

In light of new Australian public sector ERP approach, where is your agency today on its ERP modernisation journey?

SOURCE: ADAPT GOVERNMENT EDGE SURVEY IN OCT 2025.
SAMPLE SIZE: 85 AUSTRALIAN GOVERNMENT LEADERS

14% LEGACY / NO ROADMAP

Still operating an on-premise or heavily customised ERP with no endorsed modernisation plan

48% PLANNING PHASE

Discovery and business case work underway (including options analysis and risk assessment)

6% PROCUREMENT PHASE

Funding approved and active market engagement via BuyICT / Software Marketplace or other sourcing channel

18% IMPLEMENTATION PHASE

Preferred solution selected (e.g SAP S/4HANA Cloud Oracle Fusion, TechnologyOne SaaS) and build / configuration or pilot deployment in progress

18% LIVE & OPTIMISE

New ERP is in production and the agency is focusing on stabilisation, increased improvement and benefits realisation

THREE PERSISTENT EXECUTION FAILURE MODES

Three failure modes consistently emerge where modernisation efforts stall, regardless of technology platform or investment level.

OPERATING MODEL MISMATCH

Modern platforms demand new ways of working, including cloud operations, DevSecOps, platform ownership, and service-based accountability. Many agencies continue to apply legacy governance and delivery models to modern environments, creating friction, delays, and risk.

SKILLS AND CAPACITY CONSTRAINTS

Skills shortages remain a persistent barrier. Leaders cited material capability gaps across cloud operations, cyber security, data, and AI, limiting the pace and confidence of transformation. The public sector's low tolerance for failure compounds these constraints. In environments where disruption can carry legal, safety, or reputational consequences, experimentation without assurance or evidence is rarely acceptable.

DIFFUSED ACCOUNTABILITY

As environments become more distributed across internal teams, vendors, and shared services, ownership is often fragmented. Where accountability is unclear, risk tolerance drops and decision-making slows, particularly in high-stakes public sector contexts.

A SOVEREIGN EXECUTION LENS ON MODERNISATION

Programs that maintained progress under pressure tended to be anchored by a common set of operational questions. These focused on authority, accountability, and response: who controls privileged access and can act on it without delay; who is accountable for outcomes when something goes wrong; whether incident response capability is local and rehearsed; and whether compliance can be evidenced on demand rather than reconstructed after the fact. The final question is particularly significant for agencies with PGPA Act obligations, where governance must be evidenced on demand.

1. Do we retain operational control across hybrid and legacy environments throughout transition — not just at go-live?
2. Is accountability for platform performance and risk explicit, local, and enforceable?
3. Can we evidence assurance during transition — not just at steady state?
4. Are operating models designed for long-term continuity, not just delivery success?
5. Who is at the table in the first hour of an incident — and can they act?

One CIO called it the 80 per cent solution: deliberately aiming for good enough rather than ideal, because constrained budgets and low tolerance for disruption make iterative progress more sustainable than comprehensive transformation.

This pattern appeared across sectors and organisation types. A national maritime safety agency described targeting the 80 per cent solution explicitly to maintain delivery momentum under financial pressure. An energy utility operating under a government-subsidised tariff model described the same trade-off: scope and pace is continuously adjusted to match what funding and change appetite will support. A state law enforcement agency described it as a structural consequence of year-by-year funding cycles that make multi-year capability planning effectively impossible.

This reflects a rational response to a structural constraint, but also raises an important question: where does the remaining 20 per cent accumulate?

The research suggests residual risk is not evenly distributed. In the organisations studied, sovereign gaps, including fragmented privileged access, untested incident response, and diffused accountability across multi-vendor environments, were often concentrated in the areas iterative delivery had not yet reached. For agencies operating under SOCI Act obligations or PGPA Act accountability requirements, those gaps carry material operational and governance risk.

> *We've really focused on delivering the bare minimum capability... target the 80% solution. That's the trade-off - you're not getting everything you want, but you actually end up getting something.*

CHIEF INFORMATION OFFICER
AT AN AUSTRALIAN FEDERAL GOVERNMENT AGENCY

THE EXECUTION GAP IS STRUCTURAL

Public sector organisations must operate two systems at once: a legacy estate that must remain stable, secure, and continuously available, and a modern environment that must evolve, integrate, and scale under constant change. These systems are governed, funded, and operated differently. They move at different speeds. They are owned by different parts of the organisation and, increasingly, by different external partners.

The execution gap sits between them.

This gap surfaces during platform transitions when accountability is shared, access is distributed, and no single party can act with authority in the first hour of an incident.

The research suggests that most transformation programs do not fail at the point of design. They degrade in this gap, where modern capability is layered onto environments that were not funded, structured or governed to sustain it.

This creates a condition that is difficult to measure but easy to recognise: environments that are modernising and destabilising at the same time.

The organisations that maintain progress identify this gap, contain it, and design their operating models around it.

4.

SOVEREIGNTY REDEFINED: FROM POLICY TO EXECUTION

Sovereignty is measured in practice by three things: clarity of accountability, speed and proximity of response, and reliability of recovery. As technology environments grow more interconnected, operating models, privileged access arrangements, partner structures, and escalation pathways shape sovereignty far more than procurement frameworks do.

> *You only really find out how 'sovereign' you are when something breaks. That is when contracts matter less than who is actually at the table.*
>
> **TECHNOLOGY LEADER**
> IN THE CRITICAL INFRASTRUCTURE SECTOR

If you're going to offshore data, you're beholden to other nations' statutes. If you were to offshore information to the US, for example, any piece of data can be seconded then by Congress. That changes the risk profile.

MURRAY THOMPSON
CHIEF STRATEGY OFFICER, KINETIC IT

kinetic IT

THE SHIFT IN SOVEREIGN RISK

In defence and national security environments, sovereignty extends into classified and air-gapped domains, cross-domain architectures, and trusted supply chains. Data sovereignty across classification tiers, cleared workforce constraints, and alliance interoperability materially shape platform and partner decisions. Here, sovereignty is inseparable from national capability and coalition requirements.

In interviews for this report, leaders also expressed growing concern about overseas third-party dependencies, global platform concentration, and extra-territorial legal exposure.

Australian sovereignty obligations require agencies to assess where data is stored, and which jurisdictions can compel access to it. The Australian Signals Directorate's cloud security guidance, the Hosting Certification Framework, and SOCI Act risk management obligations all require explicit assessment of legal control over data and systems.

This risk is practical and immediate. Under the United States Clarifying Lawful Overseas Use of Data Act 2018 (US CLOUD Act), US authorities can compel US-incorporated providers to disclose data regardless of where it is physically hosted. For Australian agencies operating under the Privacy Act 1988 and the Australian Privacy Principles, this creates a direct intersection between foreign jurisdiction exposure and domestic accountability obligations.

"There is this capability gap that exists... we've got some great organisations, some great resources, but compared to what I can access elsewhere, there's still a way to go."

— Digital leader at an Australian critical infrastructure sector organisation

SOVEREIGNTY AS A DECISION FILTER

What has changed in practice is when and how sovereignty enters the decision process. The insights gathered for this report indicate that sovereignty is increasingly shaping technology decisions alongside cost, capability, and time to value. Leaders are applying sovereignty earlier in the process and with greater precision, recognising that operational authority determines whether a service or platform can be trusted.

> ***"The whole sovereignty debate is a little bit naive... unless you're credibly able to say that both the software and its hosting arrangements are sovereign."***
>
> ***— Chief Digital Officer at an Australian State Government Agency***

Across discussions, leaders described a shift in priority. Speed and innovation remain important; however, they are now counterbalanced by delivery confidence, risk tolerance, and assurance requirements. This means sovereignty enters the discussion earlier, and narrows what is acceptable, particularly around privileged access, incident response capability, and extra-territorial legal exposure.

SOVEREIGNTY IS A TRADE-OFF, NOT A STATE

A consistent tension runs through the research. Sovereignty is often discussed as a condition that can be achieved and maintained.

In practice, leaders describe a more dynamic reality of continuous negotiation between control and dependency, sustained over time.

Every decision redistributes control, accountability, and risk across the system. Global platforms provide scale but introduce jurisdictional exposure. Distributed delivery models increase flexibility, but fragment accountability. Rapid modernisation accelerates capability but extends hybrid complexity. There is no configuration in which these tensions disappear.

What changes is how consciously they are managed. The organisations that maintain sovereign execution understand where dependencies sit, how they behave under stress, and who retains authority when conditions deteriorate.

This is why sovereignty is applied as a decision filter early in the process. Not to eliminate trade-offs, but to make them explicit before they are embedded in platforms, contracts, and operating models.

The research suggests that this requires continuous management, and highlights a tension agency leaders are actively navigating: demand for local accountability, operationally capable delivery partners continuously growing, but supply struggling to keep pace.

For leaders, that creates a real sequencing problem: how to close the gap now while the market catches up. This pressure reflects a long-standing, technology-centred structural challenge for the public sector, identified in successive Australian Government capability reviews including the 2023 Australian Public Service (APS) Reform Agenda.

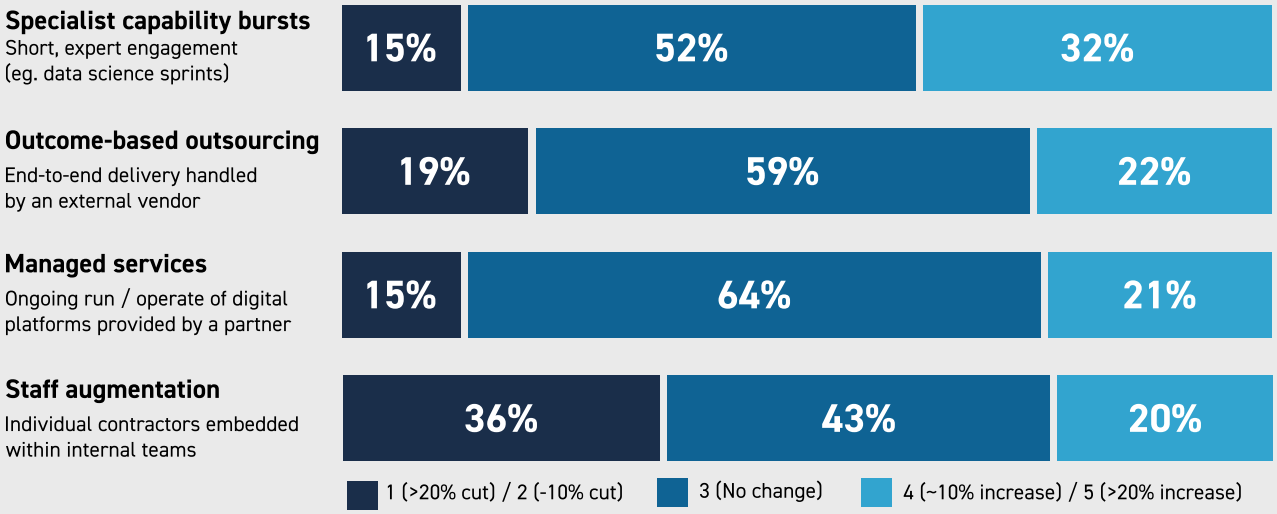
> *"There has to be a balance. It's going to be very difficult to claw away – the hyperscalers have invested heavily. Often that's been in partnership with government. The question isn't whether they play a role. It's how you retain authority and accountability across that ecosystem."*

JEREMY O'DONOHUE
MANAGING DIRECTOR

STATE GOVERNMENT AND CRITICAL INFRASTRUCTURE, KINETIC IT

In light of new Australian public sector focus on sovereign capability, how was your agency's reliance on each engagement model changed over the past 12-18 months?

SOURCE: ADAPT GOVERNMENT EDGE SURVEY IN OCT 2025. SAMPLE SIZE: 83 AUSTRALIAN GOVERNMENT LEADERS



ADAPT's 2025 Government Edge research reinforces this shift. In the context of the APS' increasing focus on sovereign capability, 21 per cent of agencies reported greater reliance on managed services and long-term operational partnerships over the past 12-18 months, especially for mission-critical systems. Crucially, leaders are prioritising partners who can provide onshore control, accountable operations, and assured incident response.

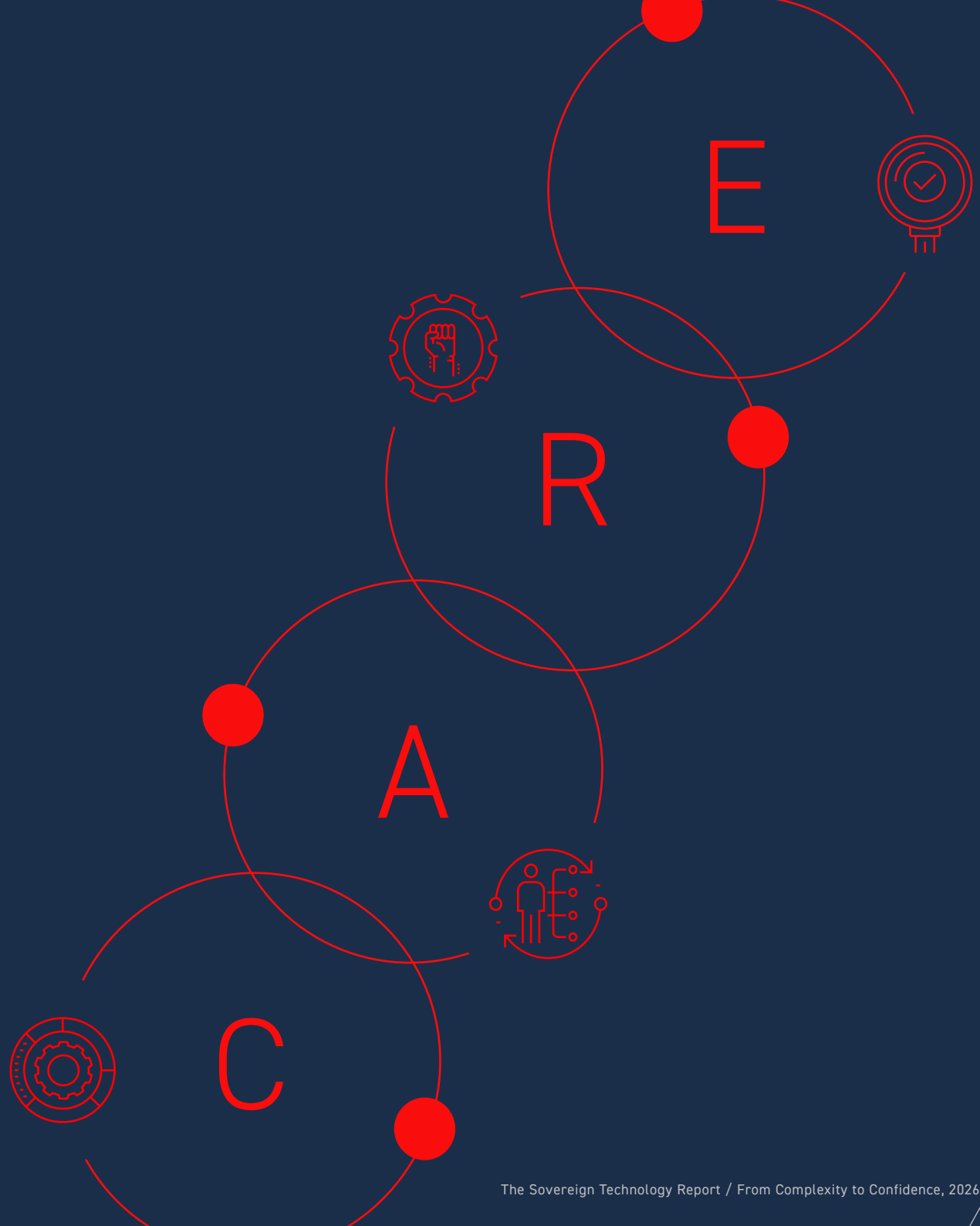
Leaders increasingly treat sovereignty-driven decision-making as a more mature response to risk, enabling modernisation that can be defended to boards and regulators. The focus shifts from policy alignment to operational defensibility: whether a platform can be operated and governed under pressure.

Knowing what sovereignty demands is one thing. Knowing where your organisation actually stands is another.

5.

THE FOUR DIMENSIONS OF SOVEREIGNTY: A FRAMEWORK

Four dimensions stand out as the points where sovereign execution is tested and most likely to come under strain. These are operational priorities that leaders in high-consequence environments return to when assessing their own readiness and evaluating the platforms and partners they work with.



Accountability is key... clarity and ownership, and the decision rights, help determine the responses.

DIGITAL LEADER
AT AN AUSTRALIAN
DEFENCE ORGANISATION

THE FOUR DIMENSIONS

The four dimensions are control, accountability, resilience, and evidence. Each maps to an obligation or risk recognised in Australian governance frameworks already discussed: PGPA, SOCI, and the ASD's Information Security Manual. Together, these dimensions enable operational sovereignty while strengthening citizen trust in the continuity, security, and accountability of government services.

DIMENSION	WHAT IT MEANS	KEY QUESTIONS TO ASK	WHAT GOOD LOOKS LIKE
 CONTROL	Retaining direct authority over systems, data, and operational decisions — with the ability to intervene without relying on opaque escalation paths or distant third parties.	Do we retain operational authority during incidents and change? Who holds privileged access — and can we revoke or act on it without delay?	Clear ownership, local escalation pathways, real-time platform visibility, no dependency on offshore response for critical actions.
 ACCOUNTABILITY	Clear, explicit ownership of outcomes across platforms, partners, and delivery models — with named decision rights and enforceable escalation authority.	Is responsibility for outcomes explicit across every partner and platform? Is there a named owner who can be held accountable — not just a contract clause?	Named owners with decision rights and escalation authority across internal and external delivery. Accountability survives change of personnel, platform, or partner.
 RESILIENCE	The ability to maintain operations, recover rapidly, and retain decision-making authority through cyber incidents, supply chain disruptions, or geopolitical volatility.	Can we operate through disruption and transition without compromising sovereignty? Do we understand our third- and fourth-party risk exposure?	Demonstrated continuity during incidents, migrations, and operating model change. Recovery is local, transparent, and rehearsed.
 EVIDENCE	Demonstrable confidence that systems are secure, compliant, and operating as intended - extending beyond certifications to continuous control testing and auditability.	Can we evidence security and compliance in practice, not just in documentation? Can we adapt global platforms to Australian regulatory and operational conditions?	Controls tested continuously and enforced operationally. Auditability is built in. Assurance can be demonstrated to boards, auditors, and regulators on demand.

THE CARE FRAMEWORK WAS DEVELOPED BY KINETIC IT AND ADAPT THROUGH SYNTHESIS OF THE QUALITATIVE EXECUTIVE INTERVIEW PROGRAM AND ADAPT'S 2025 GOVERNMENT EDGE SURVEY DATA. IT REFLECTS THE OPERATIONAL LANGUAGE AND PRIORITIES EXPRESSED CONSISTENTLY BY SENIOR LEADERS ACROSS GOVERNMENT, DEFENCE AND CRITICAL INFRASTRUCTURE AND IS GROUNDED IN APS GOVERNANCE OBLIGATIONS

APPLYING THE FRAMEWORK: SECTOR BY SECTOR

FEDERAL AND STATE GOVERNMENT

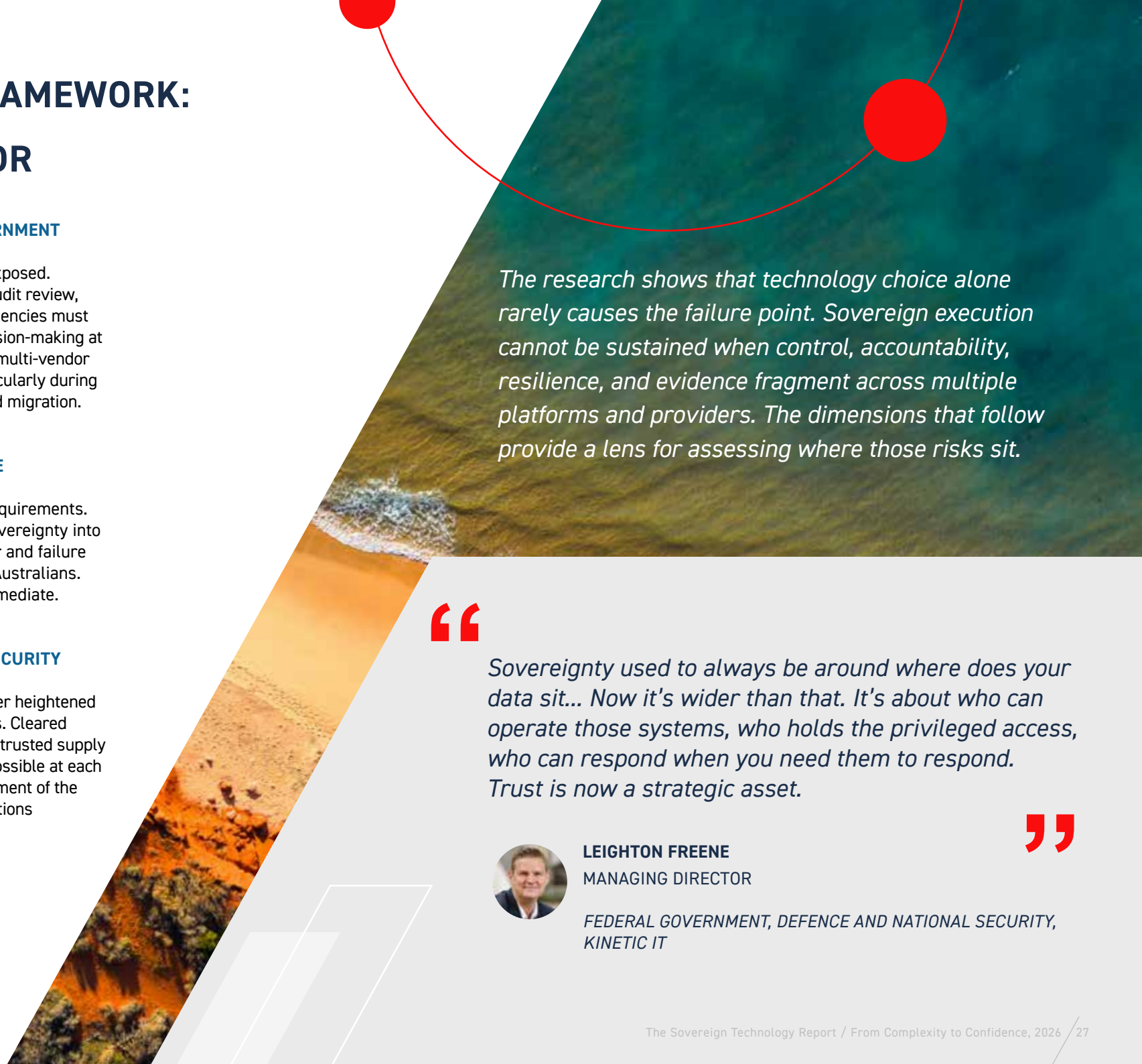
Accountability and evidence are most exposed. Operating under ministerial oversight, audit review, and public accountability frameworks, agencies must be able to evidence compliance and decision-making at any time. Diffused accountability across multi-vendor delivery models is a recurring risk, particularly during major programs like ERP reform or cloud migration.

CRITICAL INFRASTRUCTURE

Resilience and control are existential requirements. IT and OT convergence has extended sovereignty into physical domains where minutes matter and failure carries safety-of-life consequences for Australians. Incident response must be local and immediate.

DEFENCE AND NATIONAL SECURITY

Operates under all four dimensions, under heightened constraints'under heightened constraints. Cleared workforce, coalition interoperability, and trusted supply chain requirements determine what is possible at each layer of the stack, and shape any assessment of the partners against national security obligations



The research shows that technology choice alone rarely causes the failure point. Sovereign execution cannot be sustained when control, accountability, resilience, and evidence fragment across multiple platforms and providers. The dimensions that follow provide a lens for assessing where those risks sit.

> *Sovereignty used to always be around where does your data sit... Now it's wider than that. It's about who can operate those systems, who holds the privileged access, who can respond when you need them to respond. Trust is now a strategic asset.*

LEIGHTON FREENE
MANAGING DIRECTOR

FEDERAL GOVERNMENT, DEFENCE AND NATIONAL SECURITY, KINETIC IT

6.

SECURITY, DATA AND AI: THE FOUNDATIONS OF SOVEREIGN EXECUTION

Interest in AI and advanced automation across Australia's public sector continues to grow. Leaders recognise the potential to improve productivity, enhance decision-making, and deliver more responsive services. However, ADAPT's research shows that AI adoption is advancing carefully, held back by risk and readiness rather than a lack of appetite.

Security maturity, data governance, and responsible AI adoption are the foundations that make sovereign execution possible. Leaders were consistent on this point: where these foundations are strong, agencies can move further and faster with confidence. Where they are weak, every step forward carries compounding risk. The question isn't whether to invest in these areas, but how to build them in a way that actively enables the digital and AI ambitions the APS is being asked to pursue

> ***"AI raises the stakes... At the end of the day, accountability still sits with us. If we cannot explain how a decision was made, we cannot delegate that responsibility to a system."***
>
> ***— Senior Data Leader at an Australian Federal Government Organisation***

In environments where failure carries real consequences, these foundations determine how far organisations can move beyond experimentation.

ESSENTIAL EIGHT MATURITY - AUSTRALIAN GOVERNMENT AGENCIES

Cyber security maturity sets the ceiling for digital progress

Operating at Level 1 or 2 (baseline-developing)

Compliant and structured - but not yet optimised for distribution, AI-augmented or API heavy environments.

~70% of agencies remain at Level 1-2 across critical controls including MFA, patching access, and app hardening.

Achieved Level 3 (highest maturity)

Varies by control - highest for disabling untrusted macros (23%), lowest for patching apps regularly (16%).

16-23% reach Level 3 depending on the control - a wide spread that reflects uneven, not absent, investment.

SOURCE: ADAPT SECURITY AND GOVERNMENT EDGE SURVEY, APRIL AND OCTOBER 2025. SAMPLE: 255 AUSTRALIAN CISOS AND GOVERNMENT LEADERS.

CYBER MATURITY SETS THE CEILING FOR DIGITAL PROGRESS

Cyber security has become a defining constraint on digital ambition across government. While awareness and investment are high, maturity remains uneven.

ADAPT's 2025 Government Edge survey shows that Essential Eight maturity is broadly embedded at baseline but only 16-23 per cent of agencies report achieving the highest (Level 3) maturity. The majority continue to operate at Level 1 or 2 for critical controls such as multi-factor authentication, patching, privileged access restriction, and application hardening. In practice, this means many agencies are compliant and structurally disciplined, but not yet uniformly optimised for distributed, API-heavy, or AI-augmented environments. Hybrid working practices broaden this exposure further, extending cyber security boundaries beyond organisational control into home networks and personal devices.

This uneven maturity effectively sets a ceiling on how far automation and AI-driven decision-making can safely scale.

For organisations captured under the SOCI Act reforms, enhanced obligations around incident reporting, risk management, and governance elevate cyber maturity to a licence-to-operate requirement.

> ***"If the security aspect of the digital product you're offering is not good enough, it's going to be a deal breaker... AI raises the stakes. If you do not already trust your data and controls, automation just magnifies the risk."***
>
> ***— Data and Analytics Leader at an Australian Federal Government Organisation***

DATA INTEROPERABILITY STILL A STRUCTURAL BOTTLENECK

Beyond cyber security, data continues to constrain digital transformation across government. ADAPT's Government Edge Survey shows most agencies operate in partially integrated environments. Between 45 and 56 per cent report low maturity throughout cross-jurisdiction data exchanges, shared vocabularies, and data quality, while only 10 to 18 per cent demonstrate strong capability.

These barriers are largely governance-related rather than technical. Leaders cite gaps in resourcing and incentives, coordination, culture, legal clarity, and risk management as key obstacles.

The legislative environment is moving. The Data Availability and Transparency Act 2022 (DATA Act) established a framework for sharing Commonwealth data with accredited users, administered by the National Data Commissioner. However, the research points to persistent gaps: 32 per cent of agencies cite resources and budget as the primary barrier to DATA Act scheme participation, and 19 per cent cite data quality and metadata standards that do not meet accreditation requirements.

Who owns the data? Who is accountable for its quality? Who carries liability when shared data informs decisions that affect citizens or public safety?

> ***"The technology is rarely the blocker. The harder question is who owns the data, who is accountable for it... We have ideas, we have capability, but we don't want to take the liability."***
>
> ***— Senior Data Leader at an Australian Federal Government Organisation***

AI ADOPTION IS ADVANCING, BUT DELIBERATELY

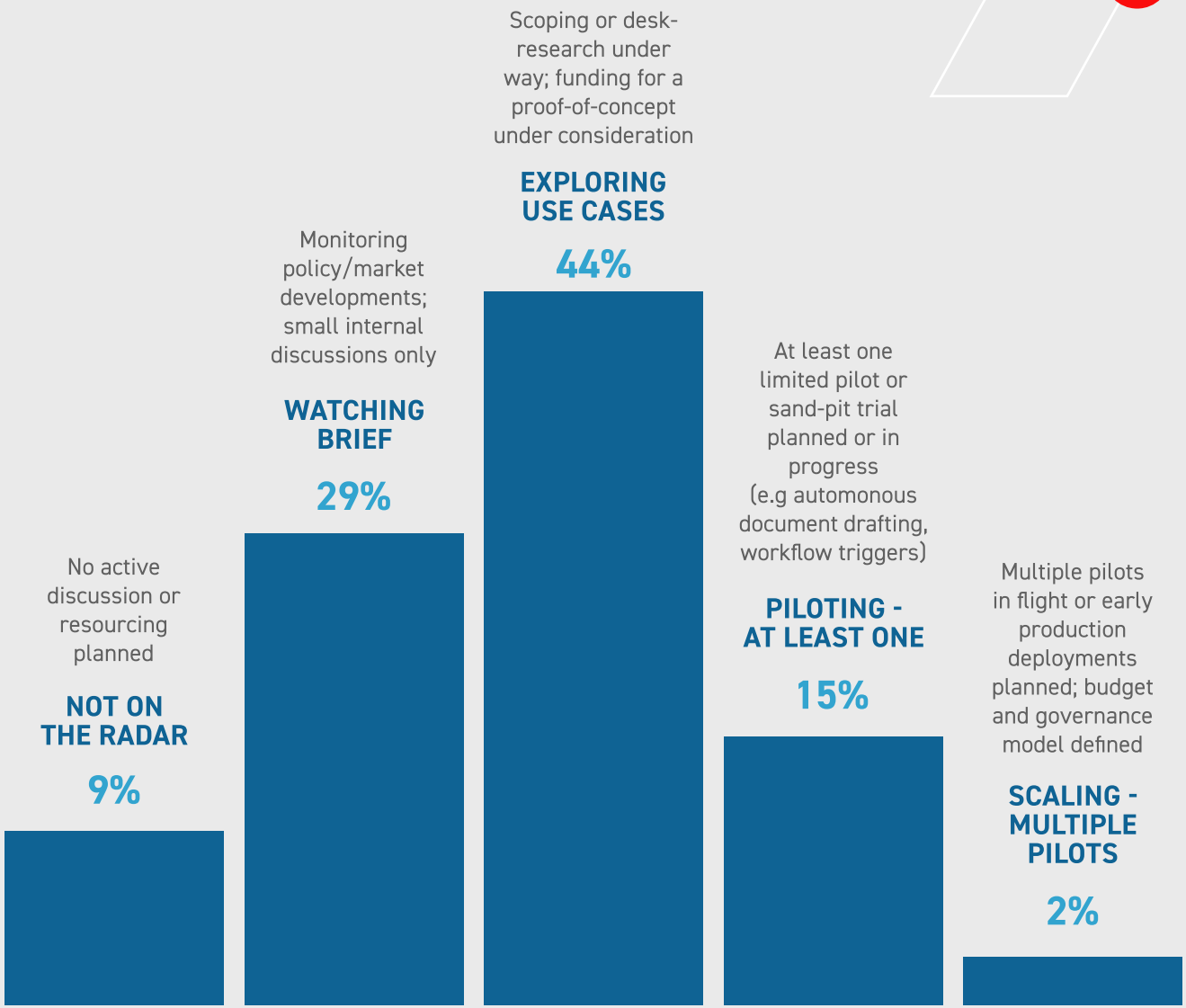
Against this backdrop, AI adoption across government remains measured. ADAPT's research characterises AI expansion as cautious and accountability-driven, constrained by factors such as complex data ownership, integration gaps, and the need for explainability under ministerial and public scrutiny. While AI experimentation is widespread, activity remains focused on early-stage applications including copilots, decision-support tools, and sandbox testing.

In OT environments, automation carries additional constraints. AI systems influencing grid management, transport coordination, or essential service delivery must meet higher thresholds for determinism, explainability, and fail-safe control. Human-in-the-loop governance is both foundational and essential.

Agentic AI remains a medium- to longer-term consideration rather than an operational reality. Only two per cent of Australian public sector agencies believe they currently have the governance, data maturity, and assurance mechanisms required to support autonomous AI safely.

In defence environments, AI adoption is further constrained by classification tiers, coalition interoperability requirements, and data sovereignty obligations, reinforcing the need for sovereign execution within multi-level security architectures.

How are Australian agencies responding to agentic AI?



SOURCE: ADAPT GOVERNMENT EDGE SURVEY IN OCT 2025. SAMPLE SIZE: 95 AUSTRALIAN GOVERNMENT LEADERS

AI AS A SOVEREIGNTY STRESS TEST

AI accelerates and exposes weaknesses that already exist. Systems manageable under traditional operating models become significantly harder to govern once automation and real-time decision-making are introduced at scale.

The research suggests AI adoption will increasingly be shaped by the ability to evidence control, resilience, and governance in live operational conditions.

> *I'm a bit of a sceptic at the moment on [agentic AI]... Rather than doing a scattergun of pilots, we're being very specific on the use cases and the business benefit.*

CHIEF INFORMATION AND DIGITAL OFFICER AT AN AUSTRALIAN DEFENCE AGENCY

When leaders start asking different questions, markets eventually have to provide different answers. ***Is the market there yet?***

7.

> *We need partners who stay accountable when things get difficult, not just when things are going well.*
>
> **TECHNOLOGY LEADER**
> IN THE CRITICAL INFRASTRUCTURE SECTOR

THE MARKET SHIFT: FROM PROJECT DELIVERY TO OPERATIONAL STEWARDSHIP

Leaders interviewed for this report described a clear shift in how they evaluate technology partnerships. Technical capability remains important but is no longer sufficient on its own.

Increasingly, agencies are prioritising partners that can operate alongside them over time, maintain continuity through disruption and retain accountability in complex operational environments.

This reflects the realities of public sector and critical infrastructure operations, where statutory and regulatory obligations elevate operational failure beyond a delivery issue into legal, governance, and reputational risk.

Viewed collectively, these findings point to a broader market shift away from discrete project delivery and toward long-term operational stewardship.

WHAT LEADERS NOW EXPECT FROM DELIVERY PARTNERS

Leaders expressed a growing preference for partners that remain engaged beyond projects, evolving environments in line with operational pressures and regulatory scrutiny. This translates into concrete contractual expectations: service level agreements anchored to incident response and recovery times rather than project milestones; named accountable executives onshore; and clearly defined obligations to coordinate across multi-vendor ecosystems during disruption.

OPERATING ACROSS COMPLEX ENVIRONMENTS

As technology environments become increasingly interconnected, delivery responsibility is also becoming more distributed. Leaders highlighted the growing importance of providers who can operate effectively across multi-vendor ecosystems while maintaining clear coordination, operational visibility, and continuity of service. This is particularly important where critical services, compliance obligations, and incident response activities span multiple suppliers, platforms and operational domains.

THE NEW DIFFERENTIATOR IS OPERATIONAL TRUST

The survey findings suggest the basis of competitive differentiation is changing. Technical capability is increasingly viewed as the baseline expectation. What distinguishes providers is the ability to sustain operational trust over time through transparency, responsiveness, continuity, and accountable delivery under pressure. Long-term stewardship, hybrid nvironment operations, and continuity through transformation are becoming foundational expectations for providers operating in high-consequence environments.

> *If we move faster than our controls allow, we create more problems than we solve*

SENIOR EXECUTIVE
IN THE AUSTRALIAN PUBLIC SECTOR

STRATEGIC IMPLICATIONS, EMERGING OPERATING PRINCIPLES

1. Modernisation is increasingly being treated as a continuous operating discipline rather than a series of discrete transformation programs.
2. Sovereignty considerations are moving earlier into platform, procurement, and operating model decisions.
3. Accountability structures are becoming a critical design consideration in multi-vendor environments.
4. AI adoption is increasingly constrained by cyber maturity, data governance, and operational readiness rather than ambition alone.
5. Execution risk is most concentrated where accountability, resilience, and operational control are fragmented across complex ecosystems.

8.

CONCLUSION: FROM INTENT TO CONTROL

Across Australia's public sector and critical infrastructure environments, the intent to modernise is clear. What this report puts into question is whether execution can keep pace with the conditions in which these organisations must now operate.

The research points to a shift that is still emerging in practice. Sovereignty is moving from policy to operation, aspiration to test, and is ultimately defined by what happens when systems are under pressure.

The primary risks sit in operating models, funding structures, and how accountability is distributed, not in technology choice. Procurement and architecture cannot control these variables on their own.

Across the organisations studied, three patterns distinguish those that maintain control from those that lose it.

1. **First, visibility.** Leaders have a clear view of where authority sits, how access is structured, and how systems behave under stress, including across third-party environments.
2. **Second, accountability**. Ownership is explicit, local, and enforceable, particularly during incidents and transition states, where risk is highest.
3. **Third, response.** Capability exists to act immediately, without dependency on distant escalation pathways or fragmented delivery chains.

Hybrid architectures, multi-provider ecosystems, and increasing regulatory obligations mean these conditions must now hold under far more complex circumstances than before.

As such, sovereign execution should be regarded as a continuous operating condition in complex, high-consequence environments.

The demand for locally accountable, operationally mature sovereign execution capability is real and growing. It is reflected in legislation: in the SOCI Act's enforceable operational obligations, in the PGPA Act's accountability requirements, in the Australian Signals Directorate's ISM controls, and in the Australian Government's mandatory AI guardrails. The policy direction is clear.

The supply side is more complex. Onshore capability is still developing, governance frameworks across the market are maturing, and the ability to operate hybrid and OT environments at scale under sustained pressure is improving. However, they are not yet uniformly available at the standard the relevant regulatory and operational environments demand.

In that gap, transformation programs continue. Agencies modernise platforms, adopt AI, and restructure delivery models, often before the sovereign execution foundations are fully in place. The research collated for this Sovereign Technology Report suggests that this is where risk concentrates: not in ambition, not in technology selection, but in the operating model decisions made during transition.

If the standards for sovereign execution are increasing, and the structural constraints on delivery remain, how will organisations bridge the gap between what is required and what is currently possible?

kinetic IT

ADAPT

ABOUT THIS RESEARCH

SURVEY DATA
drawn from ADAPT's 2025 Government Edge research series. 147 Australian government leaders; 30 per cent CIO/CTO; 85 per cent federal. Supplementary data from ADAPT's CIO Edge program *(236 respondents; 71 per cent CIO/CTO).*

EXECUTIVE INTERVIEWS
Conducted with senior technology, digital, cyber, and operational leaders across Australian federal and state government agencies, critical infrastructure operators, and defence organisations. All interviews conducted under Chatham House Rules. Quotes attributed by role and sector only unless explicit permission to identify was given. Kinetic IT executives are identified by name and role throughout and are clearly distinguished from agency and practitioner voices.

DATA COLLECTION PERIOD
Survey data gathered October to November 2025. Qualitative interviews conducted 2025-26.

APPENDIX

RESEARCH METHODOLOGY AND EVIDENCE BASE

Prepared for inclusion in The Sovereign Technology Report 2026: From Complexity to Confidence

This appendix outlines the research basis, methodology, respondent qualification and analysis approach behind the report. It distinguishes ADAPT's proprietary survey research from the executive interviews conducted specifically for this project, while summarising how the evidence base was gathered and reviewed.

RESEARCH BASIS

The Sovereign Technology Report 2026 was developed by Kinetic IT in partnership with ADAPT to examine how sovereign technology considerations are being understood and operationalised across Australia's public sector, defence, critical infrastructure and regulated environments.

The report combines ADAPT's proprietary survey research with a dedicated executive interview program undertaken specifically for this project. ADAPT's survey research provided the quantitative evidence base, drawing on established research programs that track technology priorities, investment intentions, maturity and operating challenges across senior Australian and New Zealand technology leaders.

The interview program added first-hand perspective from leaders operating in high-consequence environments, as well as from Kinetic IT executives with direct experience supporting government, defence, national security and critical infrastructure organisations. These interviews were used to deepen the interpretation of the survey evidence and ground the report in practical operating realities.

METHODOLOGY

ADAPT's proprietary survey research was the primary quantitative input for the report. The survey evidence drew mainly from ADAPT's 2025 Government Edge research program, with supplementary context from ADAPT's broader CIO Edge and Edge programs where relevant. These research streams capture the priorities, investment intentions, capability maturity and operating challenges of senior leaders across government, enterprise, critical infrastructure and regulated sectors.

Alongside this survey base, ADAPT and Kinetic IT conducted a dedicated qualitative interview program for this report. Interviews were designed to explore the practical realities behind the research themes, including how leaders think about sovereignty, accountability, operational control, partner models and delivery confidence in complex technology environments.

Participants included senior technology, digital, cyber, operational and transformation leaders across Australian federal and state government, defence, critical infrastructure and adjacent regulated sectors. The program also included Kinetic IT executives with relevant operational experience. External interviews were conducted under Chatham House principles; quotes are attributed by role and sector only unless explicit permission has been provided. Kinetic IT executives are identified by name and role where quoted and are clearly distinguished from external participant perspectives.

The survey and interview evidence was reviewed by ADAPT's research and analyst team as part of the report development process. Findings were interpreted against prior-wave research, adjacent ADAPT research programs and broader market engagement to ensure the final narrative reflected both market-level data and grounded executive perspective.

SURVEY RESPONDENT QUALIFICATION

ADAPT qualifies all survey respondents as senior technology leaders actively involved in key decisions about which technologies their organisation adopts, how those technologies are implemented and how value is leveraged from technology investments.

Respondents include:

- C-suite executives with direct accountability for technology strategy and outcomes
- Senior leaders with significant budget authority and vendor selection responsibility.
- Decision-makers who shape how technology is embedded across business functions.

Participation is by invitation only. Respondents primarily come from leaders who attend ADAPT Edge events, which are closed, peer-only forums for senior technology and business leaders from Australia and New Zealand's largest organisations.

SURVEY DESIGN AND ADMINISTRATION

Surveys are administered digitally to registered attendees in the lead-up to each ADAPT Edge event. Question development is led by ADAPT's internal survey committee: a dedicated group of analysts who work in collaboration with industry experts and ADAPT's broader advisory community to design the right set of questions for each executive persona.

The committee's focus is on understanding where organisations are trying to go strategically: how technologies are anchored to key initiatives, what investments are being prioritised and what barriers are preventing organisations from realising value.

This ensures each survey instrument captures the decisions and dynamics that matter most to senior leaders, rather than surface-level adoption metrics

Each survey instrument includes a combination of:
- Single and multi-select questions capturing technology priorities, investment intentions and adoption maturity.
- Scaled questions assessing confidence, readiness and importance across key dimensions.
- Open-text questions providing qualitative depth on barriers, opportunities and strategic intent.

Surveys are fielded annually or bi-annually per persona, enabling longitudinal tracking of sentiment and behaviour over time.

ANALYSIS AND REPORTING

All analysis is conducted by ADAPT's in-house research and analyst team. Findings are validated against prior-wave data and cross-referenced with qualitative intelligence gathered through ADAPT's broader research program, including executive interviews and roundtable discussions.

For this report, the analysis was further strengthened by the dedicated interview program conducted with senior leaders and Kinetic IT executives. This helped ensure the report reflected not only the direction of the market, but the practical context in which sovereign technology decisions are being made.

Outputs are designed to highlight not just what the market is doing on average, but what higher-performing or more mature organisations do differently, giving technology vendors, partners and leaders a clearer view of the behaviours and conditions associated with stronger technology outcomes.

ABOUT ADAPT

ADAPT is a specialist Research & Advisory firm providing local market insights and benchmarking data to Australia and New Zealand's senior technology and business community.

Since 2011, ADAPT has worked with the region's leading enterprise and government executives through proprietary surveys, executive research programs, industry conferences, private roundtables and custom research engagements. Its research is grounded in direct engagement with the leaders who set strategy, control budgets, shape technology adoption and are accountable for business and operational outcomes.

Through this research, ADAPT helps senior leaders make informed strategic decisions, benchmark their priorities against peers and extract greater value from technology investments. ADAPT's research programs span key executive communities, including CIOs, CISOs, Chief Data and AI Officers, Cloud and Infrastructure leaders, Digital leaders, CFOs and Government technology leaders.

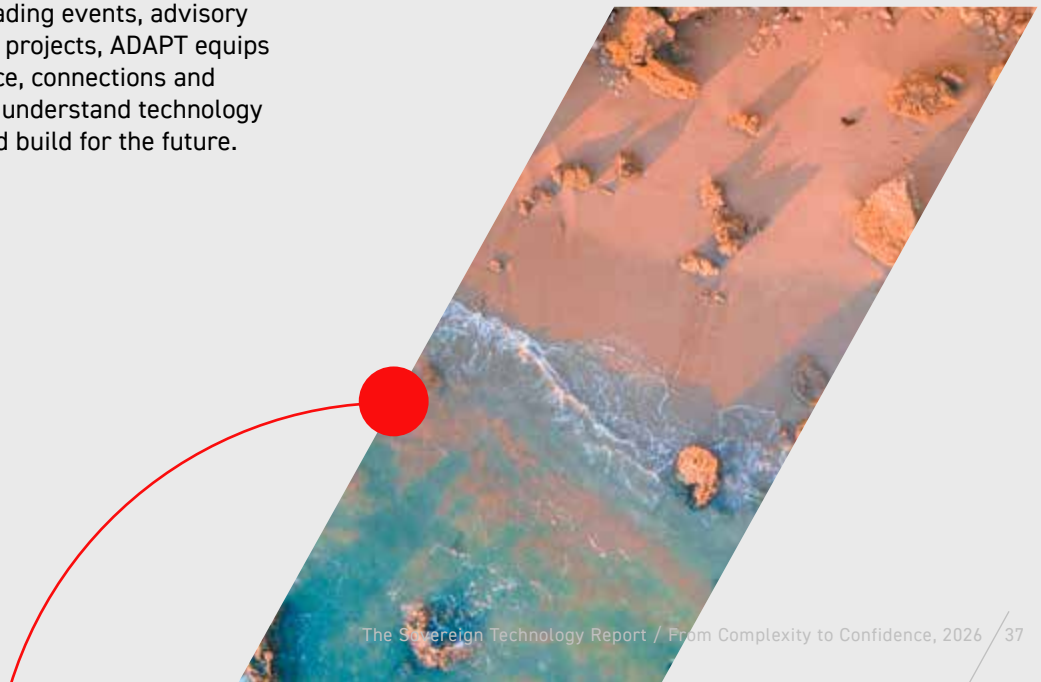
Combined with its industry-leading events, advisory services and custom research projects, ADAPT equips organisations with the evidence, connections and market intelligence needed to understand technology shifts, navigate complexity and build for the future.

RESEARCH INDEPENDENCE AND DISCLAIMER

ADAPT's research reports are based on proprietary survey insights, qualitative research and expert analyst interpretation, curated to inform strategic decision-making. Findings represent independent analysis and should not be considered definitive statements of fact, formal legal guidance or a substitute for organisation-specific risk, compliance, procurement or technology advice.

ADAPT does not endorse any vendor, product or service. References to vendors, partners, technology categories or market models are included for research and analysis purposes only.

All research is provided "as is" without warranties, including warranties of merchantability, fitness for a particular purpose or completeness. Organisations should assess the findings in the context of their own operating environment, regulatory obligations, risk profile and strategic priorities.



WHAT GOVERNMENT LEADERS WANT IN FY26

MODERNISATION, SOVEREIGNTY, ACCOUNTABILITY

> *The challenge is balancing business outcomes with what we're trying to achieve from a security standpoint.*

ANONYMOUS MARITIME SAFETY TECHNOLOGY LEADER

Organisational goals for FY 25-26	
1 Developing the AI strategy and roadmap	6 Building a secure and trusted organisation
2 Tech modernisation and simplification	6 Pursuing broad-based digital transformation
3 Key capability delivery	8 Improved citizen experience and measurable societal outcomes
3 Improving operational effectiveness	9 Ensuring governance and compliance
5 Optimising costs	10 Creating a data-driven organisation

Organisational barriers for FY 25-26	
1 Lack of funding/resources	6 Legacy systems and technical debt
2 Competing business priorities	7 Data security issues
3 Insufficient skills in the existing workforce	8 Insufficient digital literacy
4 Insufficient staff in key roles	8 Outdated processes
5 Adverse culture and user resistance	10 Stringent or unclear regulatory requirements

Initiatives for FY 25-26	
1 Pilot and adopt generative AI	6 Embed automation and foundational AI
2 Bolster overall cyber security	6 Multi-cloud migration and unification
3 Back-office systems modernisation (ERP, CRM or HCM)	8 Device management, modernisation and refresh
4 Infrastructure modernisation	8 Streamline and enable processes
5 Application modernisation and integration	10 Collaboration and productivity tools

Investment priorities of government leaders in the next 12 months

60%

AI agents (digital assistants that execute roles or tasks)

59%

Application development

59%

Enterprise architecture

57%

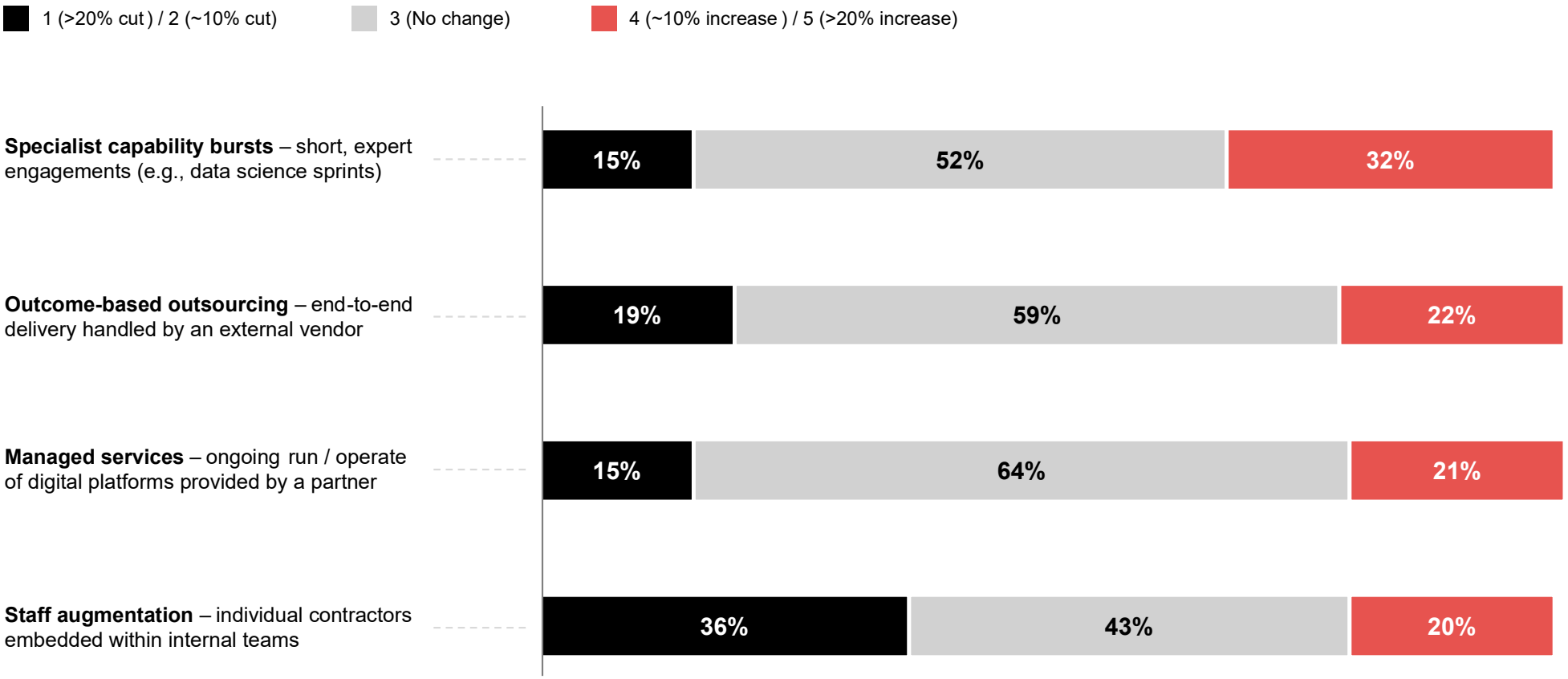
DevOps / DevSecOps

57%	Governance, risk and compliance
56%	Cyber security skills, awareness, and engagement
55%	Application security
54%	Cloud security (includes SaaS security)
53%	Organisational change management – design and implementation
53%	Data governance

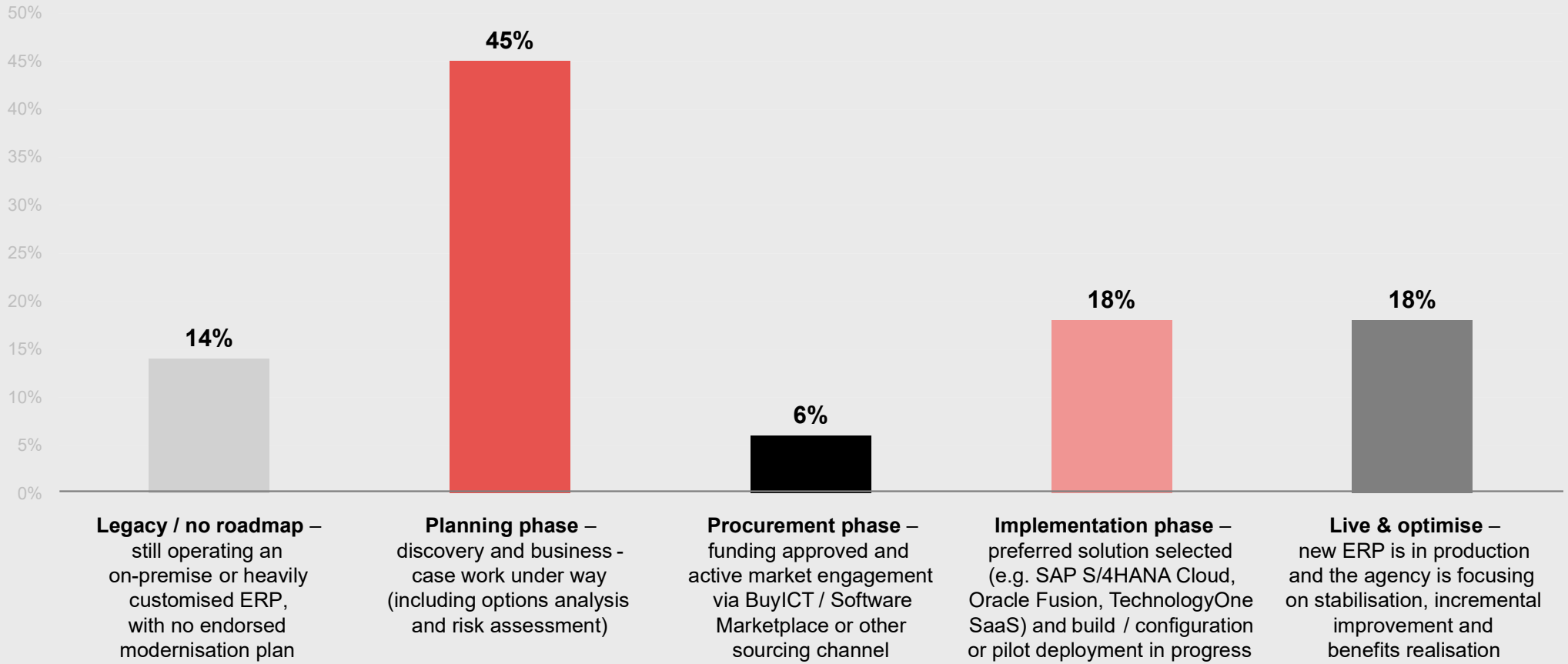
WHAT GOVERNMENT LEADERS WANT IN FY26

SOVEREIGN CAPABILITY IS RESHAPING GOVERNMENT SOURCING

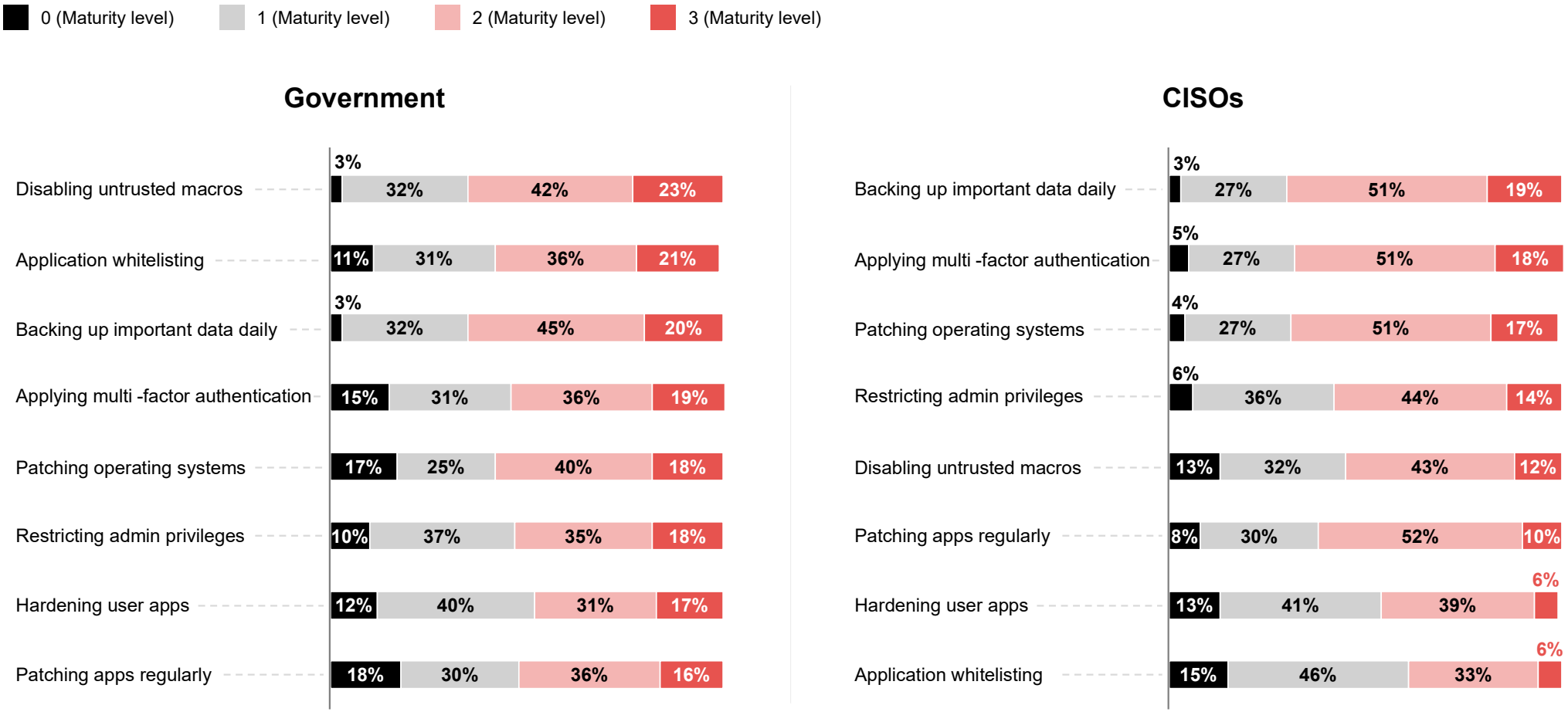
In light of the APS's focus on sovereign capability, how has your agency's reliance on each engagement model changed over the past 12–18 months?



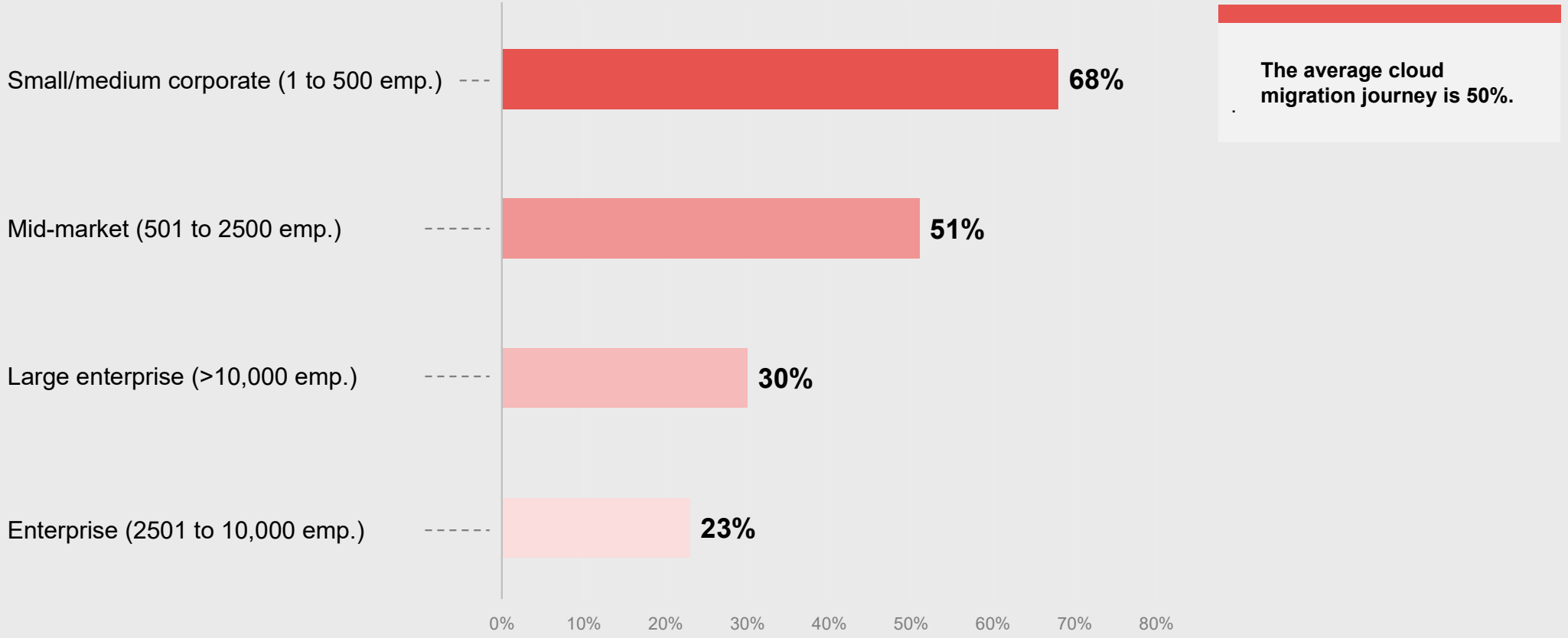
In light of the new APS ERP approach (replacing the earlier GovERP shared-services program), where is your agency today on its ERP modernisation journey?



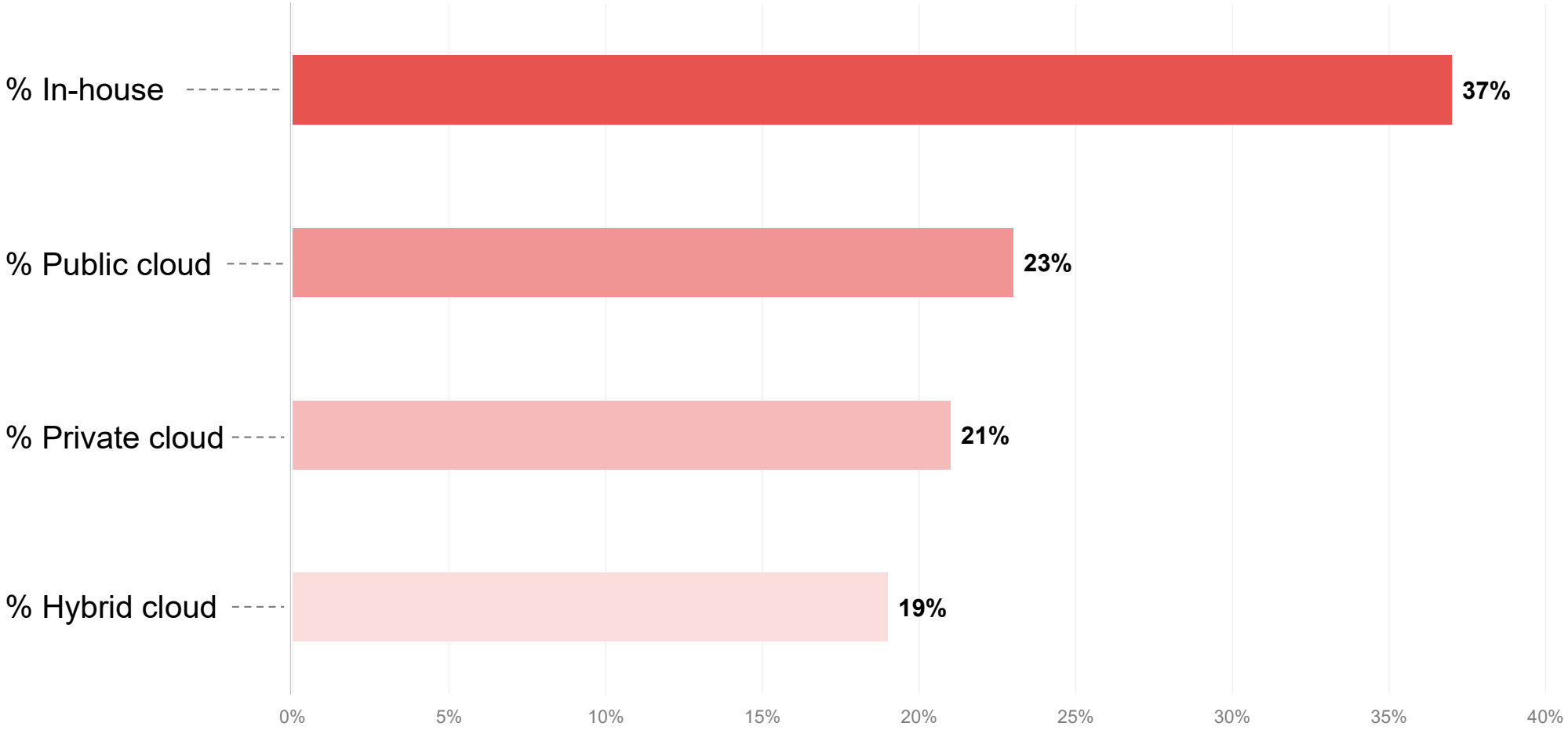
Please rate your department's cyber security maturity across the 'Essential Eight', based on the ASD 0-3 maturity definitions



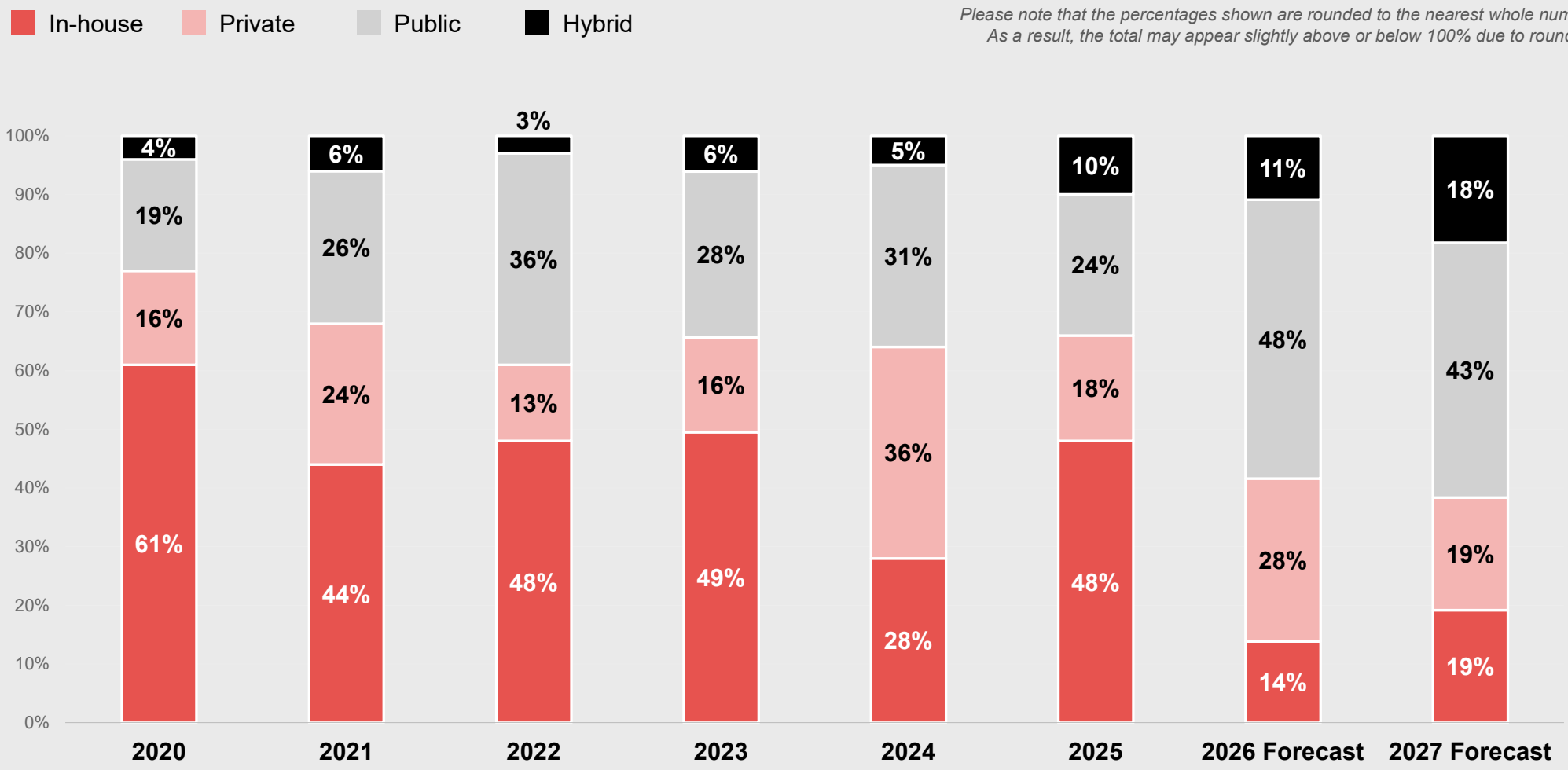
On a scale from 0% to 100%, roughly what percentage of your cloud-migration journey is complete?



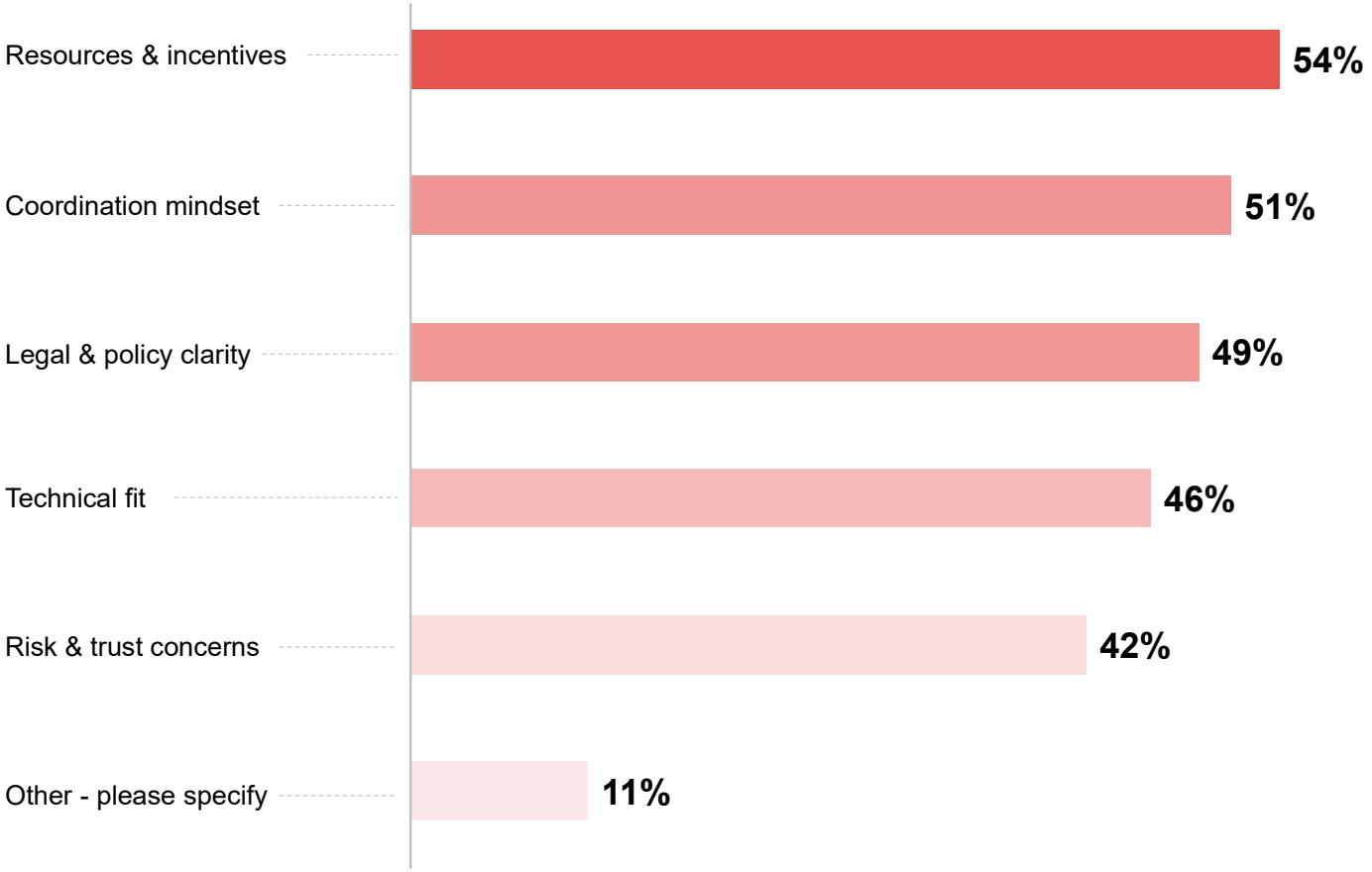
Based on that, roughly what % of your workloads are in each of these environments today?



Government: Cloud migration trends 2020 – 2027

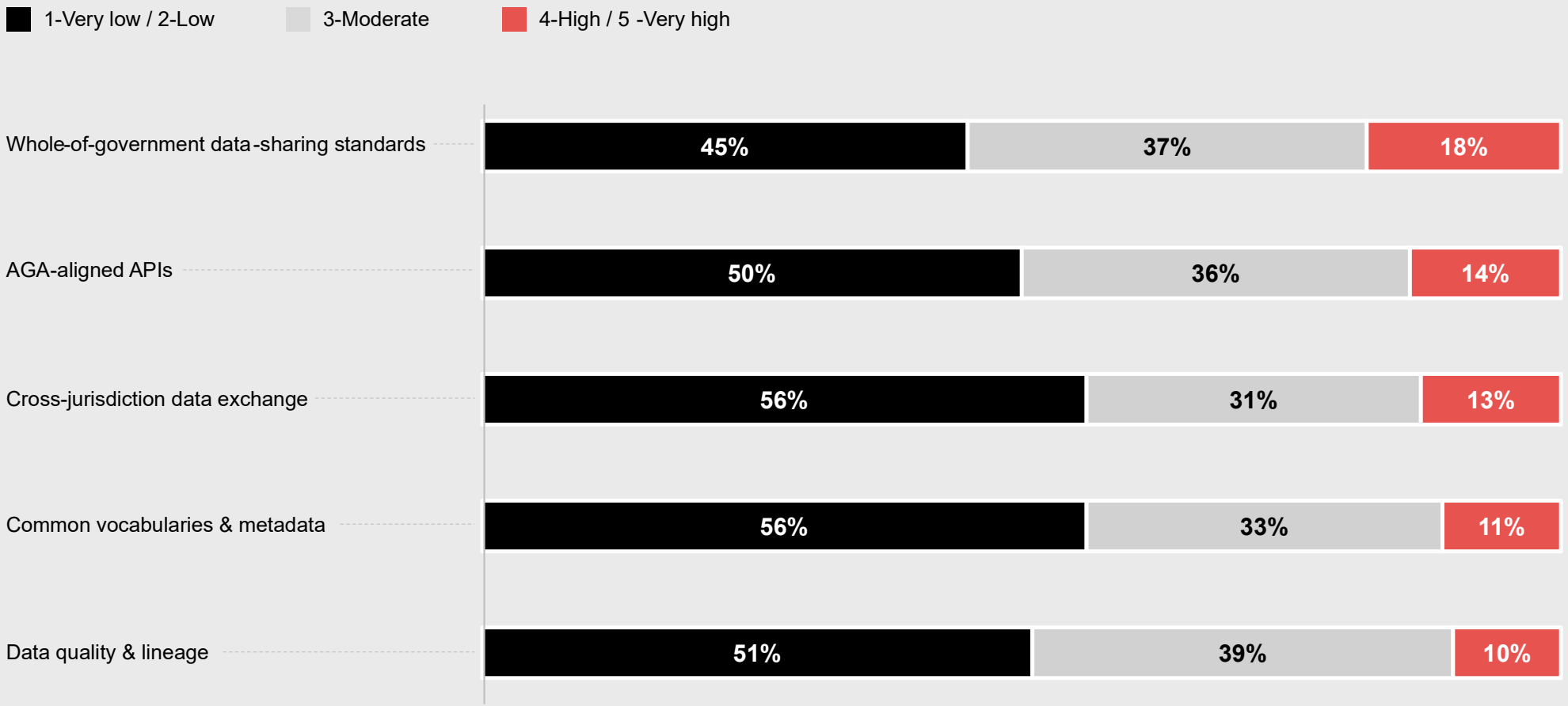


What limits your ability to work with other agencies to deliver a seamless service experience for citizens across different life events (e.g., birth, job loss, moving house)?

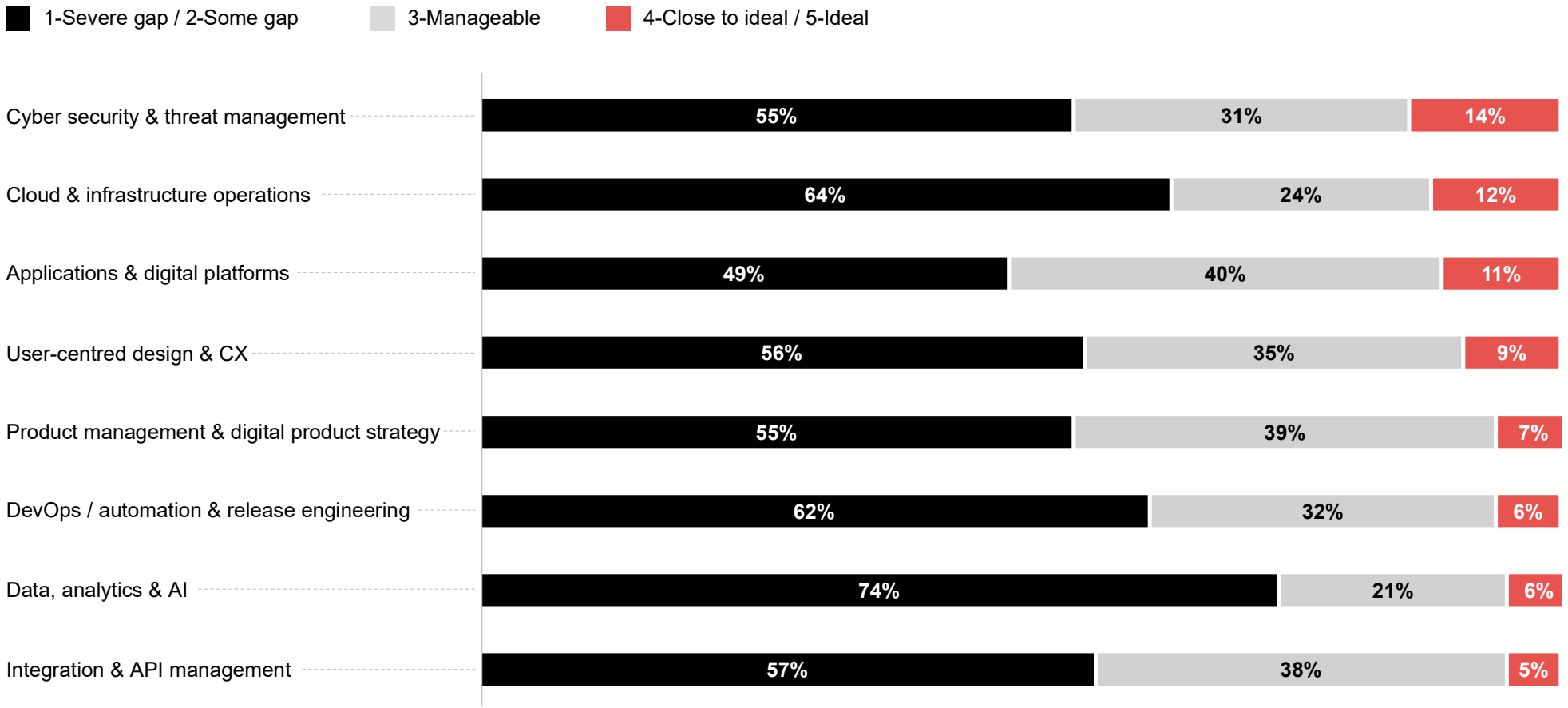


Others category	%
Not applicable	44%
Classification	11%
Security permissions	11%
Legislation	11%
Legal limitations	11%
Networking	11%

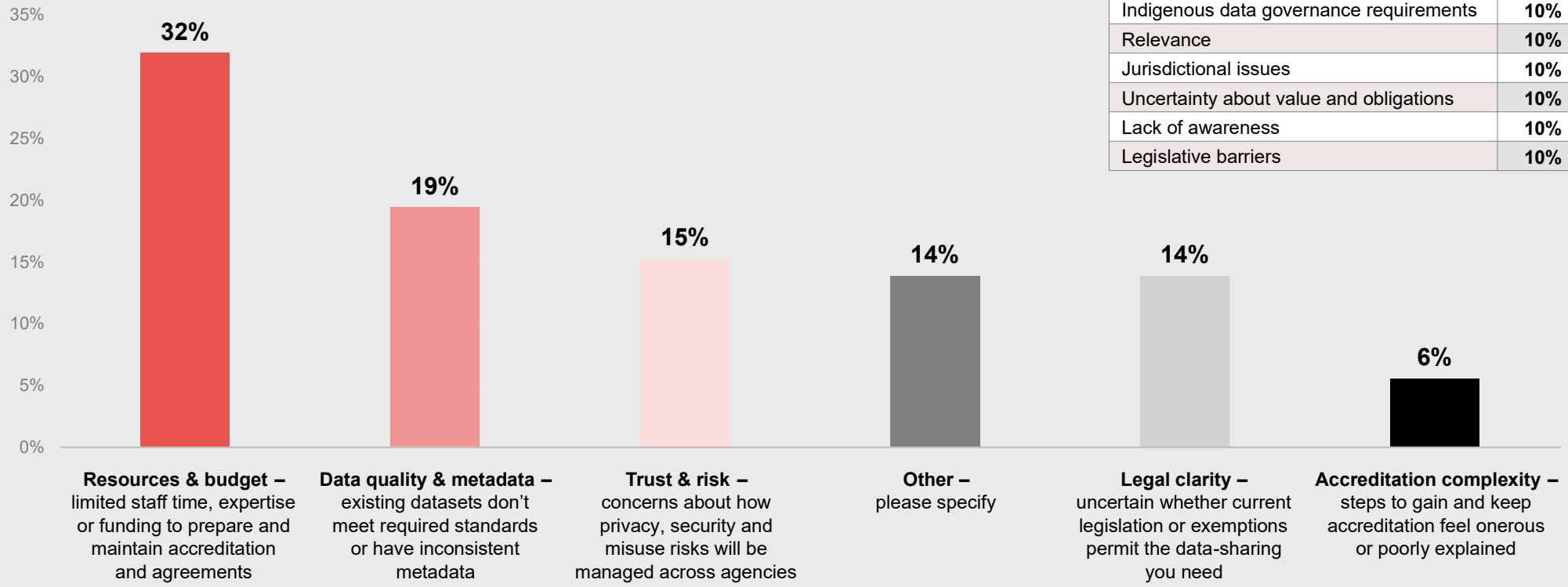
How would you rate your agency's maturity in each area of data interoperability?



What is the biggest barrier to your agency's full participation in the Data Availability and Transparency (DATA) scheme?

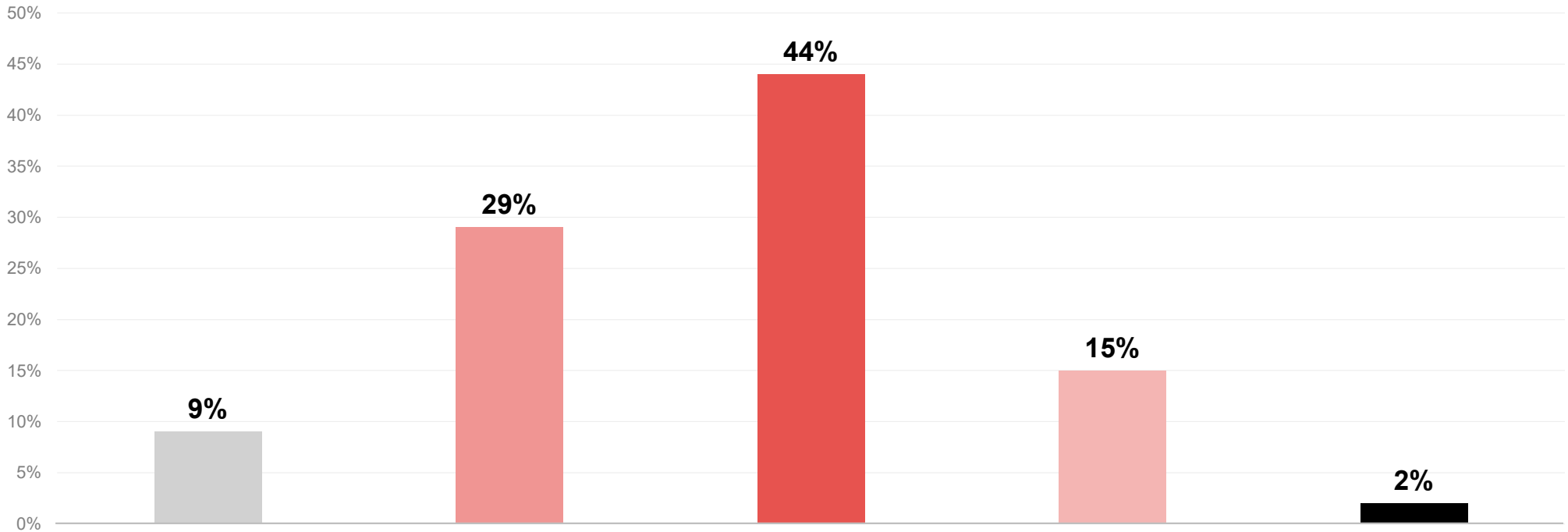


What is the biggest barrier to your agency's full participation in the Data Availability and Transparency (DATA) scheme?



Others category	%
Security concerns	20%
Organisational constraints	10%
Data classification issues	10%
Indigenous data governance requirements	10%
Relevance	10%
Jurisdictional issues	10%
Uncertainty about value and obligations	10%
Lack of awareness	10%
Legislative barriers	10%

Which statement best describes your agency's current appetite & capability to leverage agentic AI over the next 18 months?



Not on the radar – no active discussion or resourcing planned

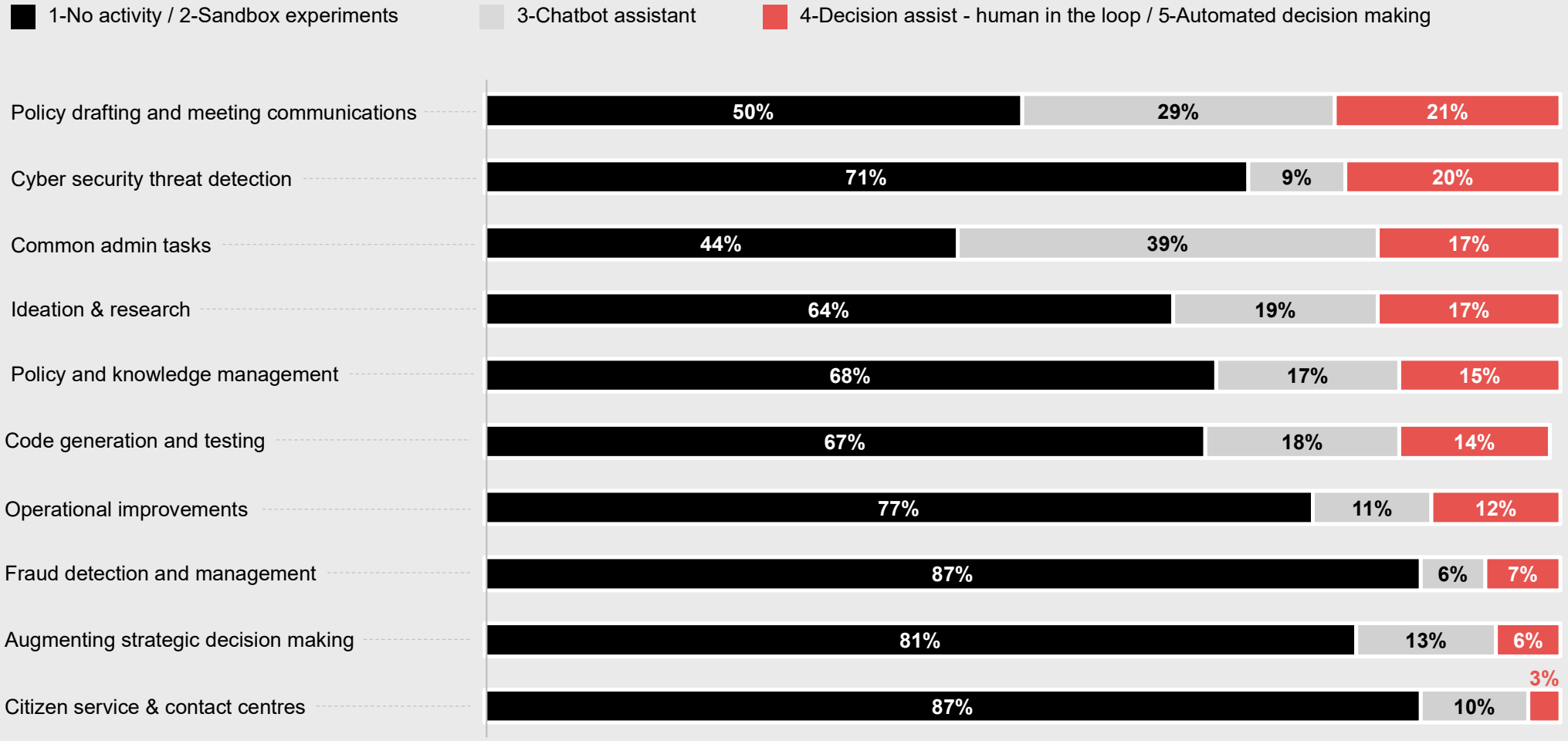
Watching brief – monitoring policy/market developments; small internal discussions only

Exploring use-cases – scoping or desk-research under way; funding for a proof-of-concept under consideration

Piloting – at least one limited pilot or sand-pit trial planned or in progress (e.g., autonomous document drafting, workflow triggers)

Scaling – multiple pilots in flight or early production deployments planned; budget and governance model defined

What are your primary generative AI use cases so far and the maturity of their deployment?



Sovereign execution is proven in moments of disruption, not documented in policy.

SAY G'DAY

Hi@KineticIT.com.au

1300 782 072

www.KineticIT.com.au