Closing the digital blind spot: managing third-party risk

May 2026

CLAYTON UTZ

About this report

Closing the digital blind spot: managing third-party risk is written by Clayton Utz in partnership with The Action Exchange, a strategic communications and business intelligence agency.

Digital third-party risk has become a resilience issue. Our analysis shows that Australian organisations need to act quickly. In this practical guide, our partners explain that accountability can't be outsourced, why procurement is a critical control point, and how to build resilience by understanding hidden digital dependencies before disruption hits. Get in touch with our technology, risk, cyber, and procurement experts if you'd like to learn more about how we can help you navigate digital risk.

Our easy-to-use toolkit to sets out a simple framework for enterprise-wide digital third-party risk management.

We acknowledge the Traditional Owners of Country throughout Australia and recognise their continuing connection to land, waters, and culture. We pay our respects to their Elders, past and present.

Meet the contributors

Simon Newcomb
Head of AI
Brisbane
0412 686 454
snewcomb@claytonutz.com

Angie Freeman
Co-Head of Digital
Canberra
0413 581 756
afreeman@claytonutz.com

Doug Nixon
Head of Risk Advisory
Sydney
0499 036 395
dnixon@claytonutz.com

Brenton Steenkamp
Head of Cyber
Sydney
0408 258 573
bsteenkamp@claytonutz.com

Robert Dearn
Partner, Public Sector
Canberra
0401 084 101
rdearn@claytonutz.com

John Dieckmann
Partner, Projects & Technology
Melbourne
0411 646 764
jdieckmann@claytonutz.com

Michelle Dawson
Director, Risk Advisory
Sydney
0481 056 389
michelledawson@claytonutz.com

Monique Azzopardi
Special Counsel, Technology and Privacy
Sydney
0401 694 371
mazzopardi@claytonutz.com

Executive summary

Australian organisations are more digitally dependent than ever. Most rely on third-party technology providers for critical business functions including cloud hosting, cybersecurity, customer platforms, and data processing. These dependencies extend to enterprise applications such as payroll, finance, and human resources as well as to digital payments and third-party artificial intelligence providers.

Third-party providers in turn depend on a web of their own digital suppliers. The result is a supply chain that few executives can confidently map until a failure forces them to do so. When failures occur they rarely stay contained. Operational disruption, regulatory exposure, and reputational damage can quickly follow.

The risk is real and increasing, yet many executives view digital third-party risk as a compliance or vendor-management task. IT, risk, procurement, and legal often have overlapping responsibilities, with oversight mainly based on policies, contracts, and vendors' self-assessments. This reactive approach creates a gap between how risk is managed on paper and how digital services actually perform under pressure. Boards and executives can remain unaware of how much dependence on third-party providers they have already accepted or what will happen if a key provider fails.

Digital third-party risk is a cross-disciplinary challenge, spanning cybersecurity, procurement, legal, and operational resilience. These functions are increasingly affected by emerging technologies, such as artificial intelligence, which introduce new vulnerabilities. Managing these risks effectively requires shifting from isolated controls to an enterprise-wide approach focused on resilience, with a clearly defined risk appetite and stress-tested scenario plans.

Drawing on the real-world experience and insights of Clayton Utz's leading technology, risk, cyber, and procurement partners, this report identifies the critical lessons emerging from the front lines of the Australian business community in managing digital third-party risk. By cutting through technical complexity, this paper offers a practical guide for boards, executives, and in-house counsel to move beyond fragmented controls and compliance checklists, providing a clear roadmap for a genuinely resilient operating model.

Key takeaways:

Digital third-party risk is a broader risk management and resilience issue, not a narrow compliance problem. Failures cascade across technical, operational, legal, and reputational domains.

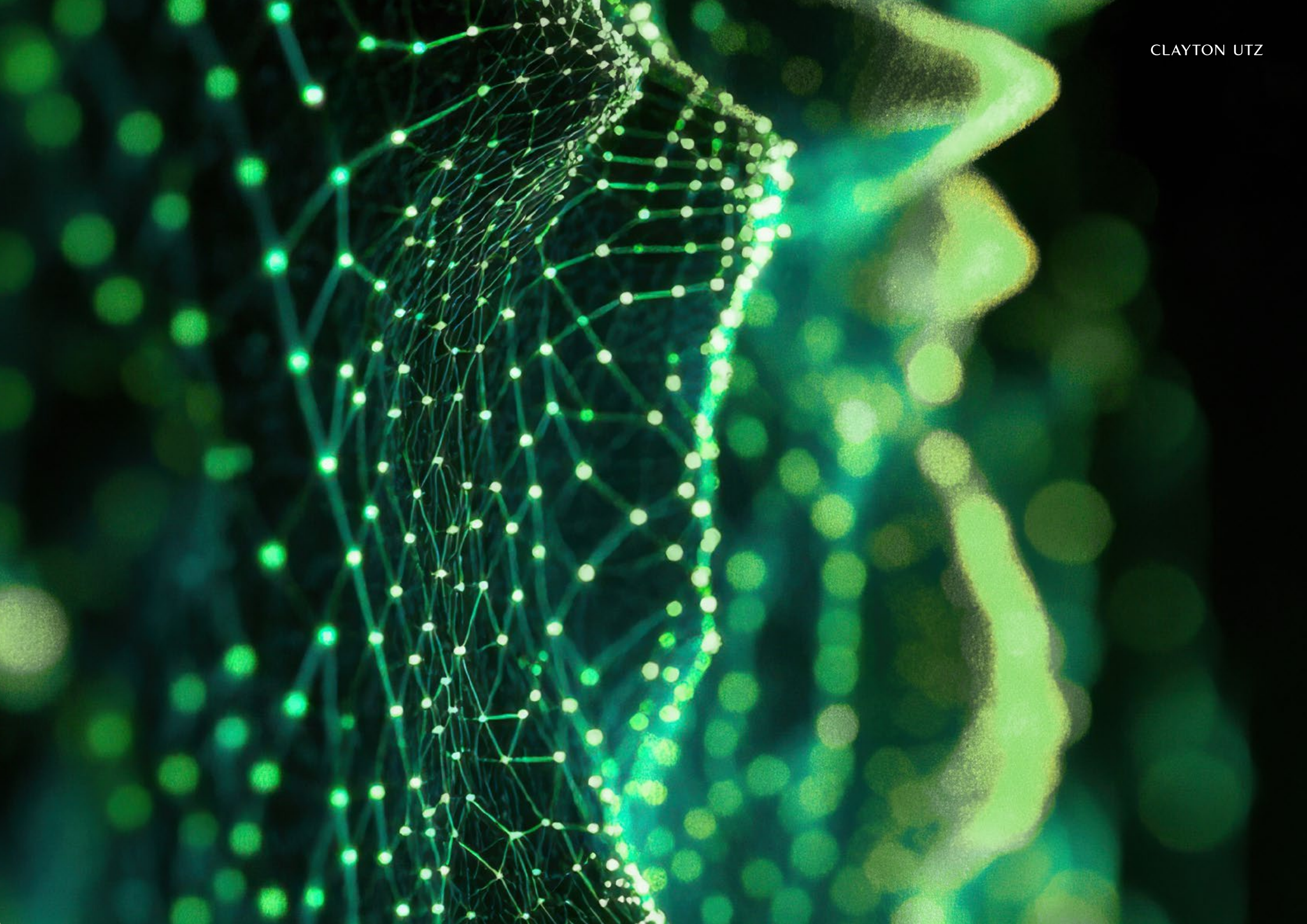
Many organisations underestimate their exposure because they focus on suppliers rather than on the digital services they actually depend on, including those from fourth- and fifth-party providers.

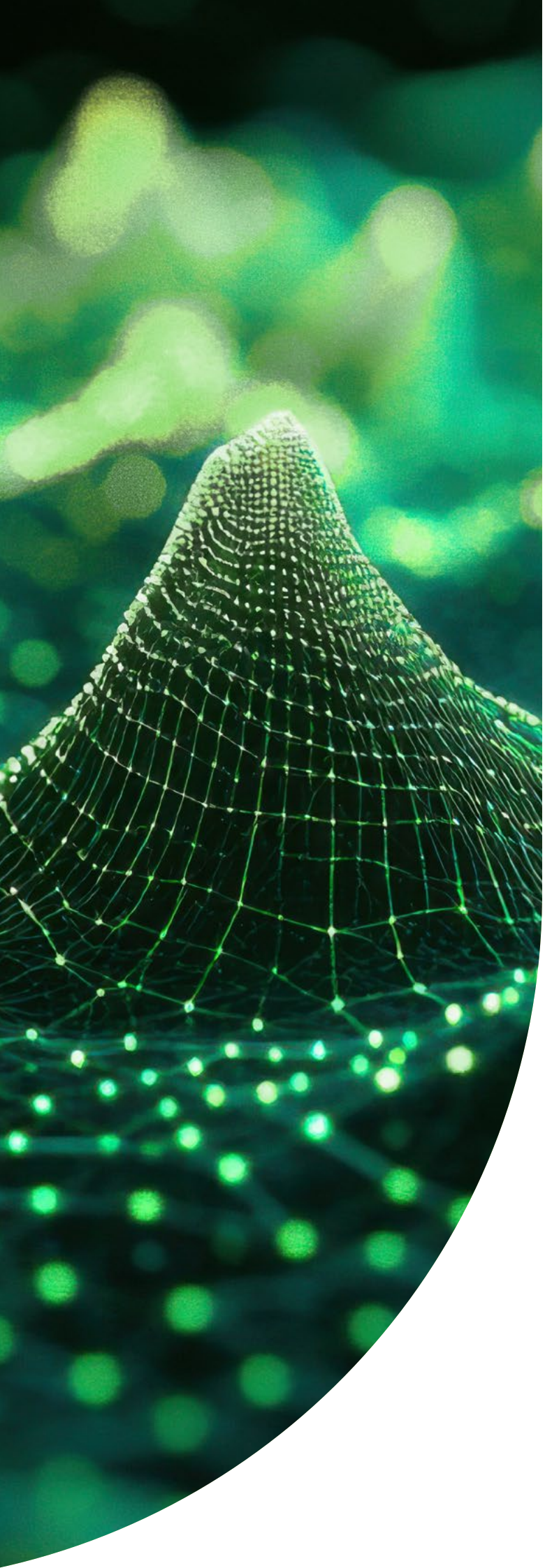
Procurement requires early collaboration between legal and technical teams to ensure that rigorous stress testing informs, rather than follows, contract negotiations.

Regulatory regimes, such as CPS 230 and the SOCI Act, sharpen expectations. However, non-regulated entities face similar risks and cannot take comfort from the absence of specific regulatory obligations. Instead, these organisations should look to such standards as useful frameworks for their own resilience.

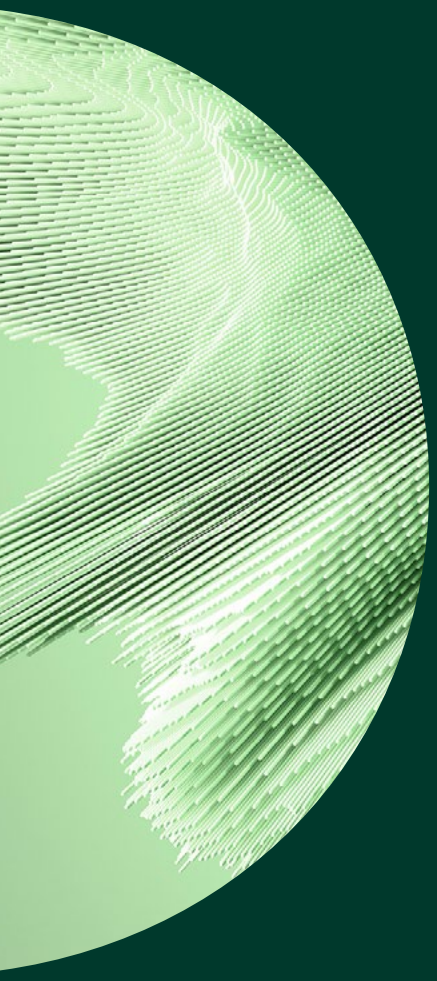
A clear, board-approved risk appetite, expressed in operational terms, is the foundation for effective governance and investment decisions.

Organisations that integrate digital third-party risk into enterprise risk management, procurement and continuity planning are better placed to absorb disruption and recover quickly.


CLAYTON UTZ



Contents



Introduction

If 2025 was the year that Australian organisations rushed to adopt productivity-enhancing AI tools, 2026 is likely to be the year they must reckon with the risks of such a rapid rollout. In the financial services sector, for example, the Australian Securities and Investments Commission (ASIC) has indicated that operational failures, cyber resilience, and decision risks associated with agentic AI will be firmly in the regulators' sights,[1] calling for an urgent capability uplift. The Australian Prudential Regulation Authority (APRA) has also reiterated their expectation that organisations will strengthen AI-related risk management.

The risk of rapidly adopting digital technologies is not confined to financial institutions. Government departments, critical infrastructure providers, and large companies increasingly depend on complex networks of third-party technology to run their core operations. Customer interactions, payments, data analysis, and decision-making all pass through highly interconnected digital systems.

This makes digital resilience - the ability to keep systems operational during shocks such as cyberattacks or system failures - mission-critical. When a government department or major infrastructure operator cannot function, the consequences extend well beyond the organisation itself.

Digital third-party risk is often managed as a set of discrete problems, spanning cybersecurity, operational risk, outsourcing, and procurement, rather than as an interconnected system. In reality these risks are horizontal, affecting multiple suppliers simultaneously, and vertical, extending down the supply chain to fourth parties and beyond. A cyber incident at a fourth-party provider, for instance, can trigger operational outages, regulatory breaches, and reputational harm.

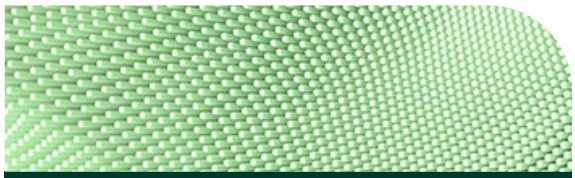
Drawing on the experience of Clayton Utz's partners across its risk, technology, cyber, and procurement practices, this report sets out a practical guide to building digital third-party resilience for chief risk officers, legal counsel, executives, and directors of large Australian entities. It makes the case for an integrated resilience-led approach that goes well beyond a narrow focus on compliance. While the challenge is universal, effective responses must reflect each organisation's sector, operating model, risk appetite, and maturity, anchored in consistent governance principles. The overarching goal, says Brenton Steenkamp, lead partner in Clayton Utz's cyber security practice, is to proactively build digital resilience: "A reactive posture is not going to be good enough to mitigate what might happen in the future."

Digital risk often lies below the headline supplier, in the layered dependencies that keep services running.

Simon Newcomb
Head of AI
Clayton Utz

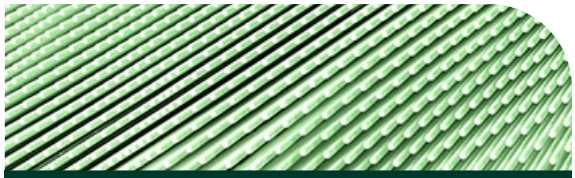
Mapping the terrain: Types of third-party digital risk

Cybersecurity risk
Unauthorised access, malware, vulnerability management, and the frequency and reliability with which a provider updates software to fix security flaws.



Data privacy and sovereignty risk
Cross-border data transfers, foreign government access powers, as well as compliance with the 'Australian Privacy Principles' and any jurisdictional privacy regimes.

Operational and availability risk
Service disruption, business continuity, disaster recovery capability, and infrastructure reliability.



Concentration risk
Over-reliance on a single provider or geography.

Fourth-party risk
The provider's own supply chain.

Compliance and regulatory risk
Whether the provider's activities could cause the licensee to breach its own obligations.

Access and identity management risk
The governance of user permissions, 'privilege escalation' (where a user gains higher levels of access than intended), and the monitoring of user activity.

Incident detection and response risk
The ability to identify, escalate, and remediate a breach when the function sits offshore and outside your direct operational environment.

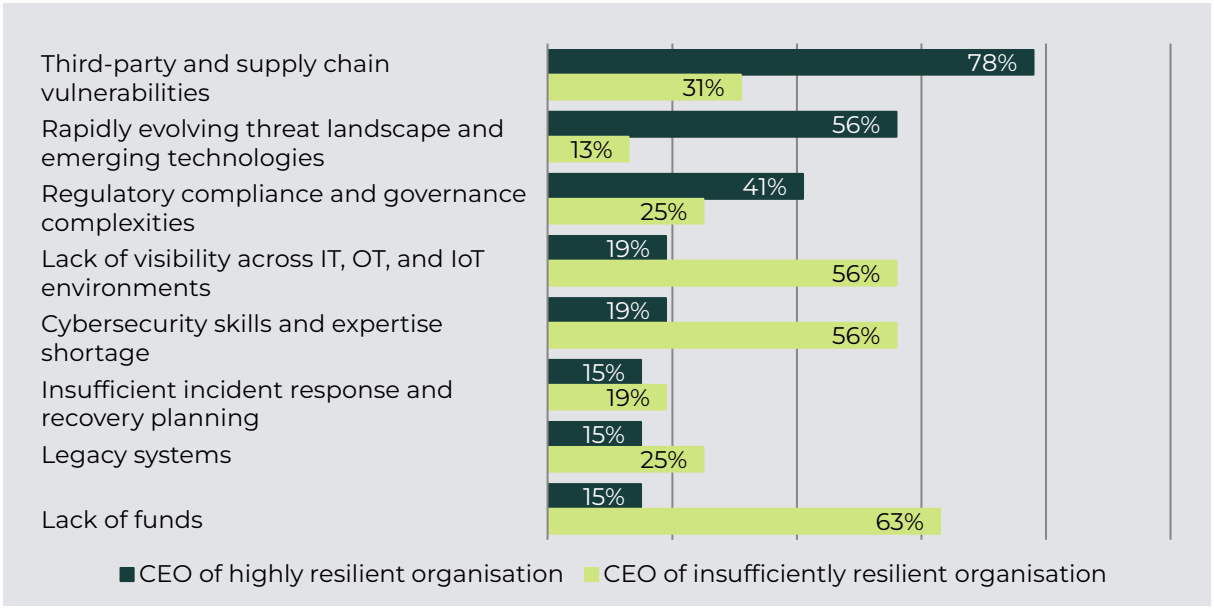
The dependency dilemma: Do you know your digital third-party risk exposure?

Effectively managing digital third-party risk is an increasingly ubiquitous challenge. More than two-thirds of organisations report an increase in digital supply chain disruptions in 2026, according to the World Economic Forum's Global Cybersecurity Outlook. Among CEOs of highly resilient firms, 78% identify third-party dependencies as the primary barrier to digital resilience.[2]

78%

of CEOS in highly resilient firms identify third-party dependencies as the primary barrier to digital resilience.

What is your organisation's greatest challenge to becoming cyber resilient?



Source: World Economic Forum[3]

The digital domino effect

Cyber, operational, or compliance failures can trigger a cascading crisis in another area. Cybersecurity firm CrowdStrike's 2024 software defect, which caused Microsoft systems worldwide to crash, is perhaps the most notorious example of this 'digital domino' effect.[4] Australian Microsoft customers, many of whom did not even know they were exposed to the risk of a failure of this fourth-party provider, experienced an estimated $1 billion of financial losses from the incident.[5]

"This lack of visibility is the biggest challenge," explains Angie Freeman, a partner at Clayton Utz specialising in large-scale technology procurement. "If you don't know who's in your supply chain, you can't manage the risk. And most organisations, if you ask them who their fourth- or fifth-party providers are, simply don't know. Where is the data sitting? Where is the code being written? It's that level you don't even know exists."

"Previously, many organisations dealt with risk by contracting certain obligations out to third-party providers, using commercial arrangements to agree where the line of liability was," explains Michelle Dawson, a director in Clayton Utz's Risk Advisory practice. "That's not the world we live in anymore. It doesn't align with community or regulatory expectations for where responsibility for customer outcomes lies."

Global executives' ranking of top supply chain cyber risks	
1	**Inheritance risk:** Unable to assure integrity of third-party software, hardware, and services
2	**Visibility:** Lack of visibility into extended supply chain
3	**Concentration risk:** Too great dependence on critical third-party suppliers
4	**Procurement risk:** Unable to apply security controls to third-party suppliers
5	**External factors:** Uncertainty of impact of external factors

Source: World Economic Forum[6]

Winning over decision-makers

Yet even as expectations grow, chief legal and risk officers can still struggle to make the case to boards and executives for greater investment in proactive digital resilience. Part of the challenge is that many of the most material risks sit beneath the immediate contractual relationship. Organisations typically deal with the supplier they appoint and rely on that provider to manage the broader delivery model. This is often commercially appropriate, but it can also make underlying dependencies harder to see, test, and explain, says Simon Newcomb, head of AI at Clayton Utz. As a result, boards and executives can misread resilience measures as unnecessary process or cost rather than as a practical response to existing risk.

"The issue is not just who an organisation contracts with, but how the service is actually put together and delivered," says Mr Newcomb. "If boards and executives do not have a clear view of those dependencies, the cost of discovering them in the middle of a disruption can be far greater than the cost of coordinated oversight."

Organisations don't often appreciate and effectively manage the myriad of exposures they are subject to when engaging a third party.

Doug Nixon
Head of Risk Advisory
Clayton Utz

Digital resilience across regulated and non-regulated sectors

- **The APRA CPS 230 (Operational Risk Management)** requires APRA-regulated institutions, including banks, insurers, and superannuation trustees, to comprehensively manage operational risk, including third-party risks. Additionally, CPS 230 requires institutions to ensure essential operations can continue during disruptions and makes boards explicitly accountable for operational resilience.[7]
- **The Security of Critical Infrastructure (SOCI) Act 2018** is a national framework for managing risks to Australia's critical infrastructure assets, including energy, communications, data storage and processing, water, healthcare, transport, and parts of the financial system. SOCI requires organisations that own, operate, or directly manage critical infrastructure assets to maintain risk management programs and report significant cyber incidents.[8]

There is a wide range of maturity across sectors, even those regulated under CPS 230 or SOCI. Yet each sector also faces its own particular challenges.

Government entities typically manage large, multi-vendor programs. Failure by one prime contractor can halt an entire public service. Disruption at a single **SOCI-regulated entity** can disrupt interconnected infrastructure sectors such as energy, water, or transport, elevating what might otherwise be a organisational risk into a broader national issue.

Most large **financial services** firms regulated under CPS 230 have formal third-party risk management frameworks. Yet many struggle to identify all the services that support critical operations, particularly downstream technology services that have become embedded over time but are not always stress-tested. Other small and mid-size financial services firms lack the sophistication of their larger competitors. Meanwhile, non-regulated entities often operate within the same digital ecosystems as banks but lack regulatory scrutiny, which can create a false sense of security.

AI: A new dependency in the digital supply chain

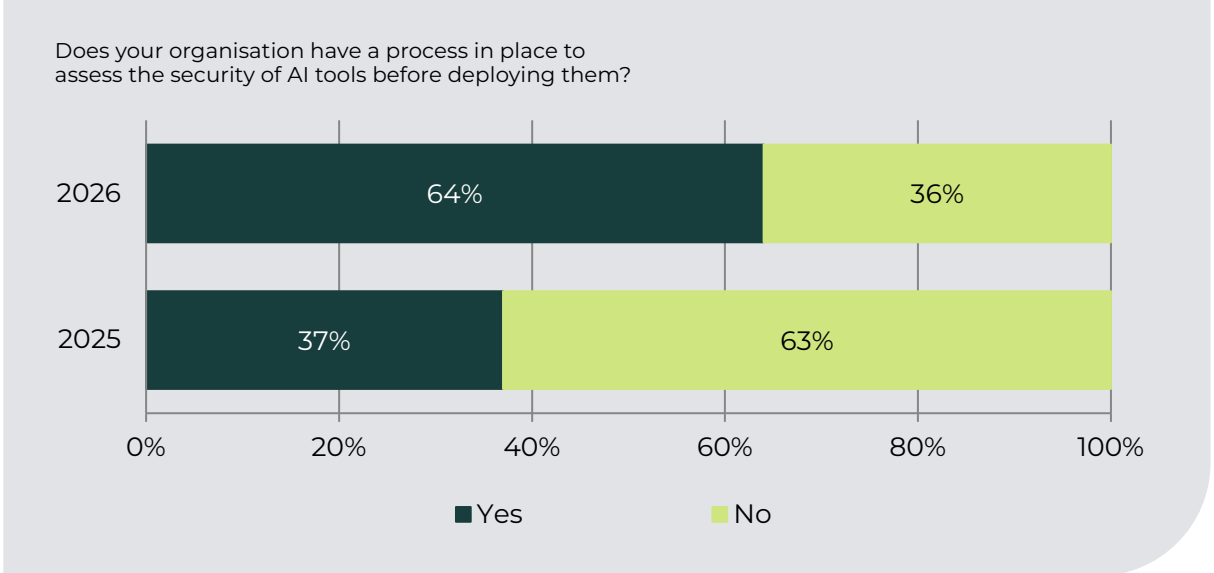
Many organisations are quickly adopting third-party AI tools to manage customer service, support decision-making, detect fraud, and enhance productivity. In 2024, 78% of organisations reported using AI, up from 55% in 2023.[9] Very few of these organisations are developing their own AI tools in-house; most are buying off-the-shelf or custom-built tools from third-party vendors. As with traditional digital services, these vendors themselves rely on a web of providers. It is common for large organisations to use multiple AI tools for different purposes.

AI tools are often technically complex, and their algorithmic decision-making processes are typically opaque. This 'black box' nature introduces the risk that organisations are unable to understand or account for decisions or outcomes for which they are legally responsible. There are ongoing concerns that AI models may make biased or flawed decisions or compromise the privacy and security of organisational data, exposing users to reputational damage and even litigation.[11]

Market concentration is a risk, too. As the AI industry matures, it is becoming increasingly concentrated among a few large global players. In February 2026, specialist software providers worldwide saw their share prices plummet amid concerns that they would be disrupted by AI giants. Indeed, the European Central Bank has warned that this market concentration, coming at the same time as organisations substitute human resources with AI in core processes, poses a risk not just to individual firms but to financial stability as well.[12]

A handful of major players, principally OpenAI, Google, and Anthropic, whose foundation models underpin a myriad of enterprise applications, dominate the AI ecosystem.

Percentage of organisations with processes in place to assess AI security



Source: World Economic Forum[10]

This market dynamic resembles hyperscale cloud infrastructure, says Mr Newcomb: organisations may think they are procuring a distinct AI application, but much of its capability depends on a downstream provider over which they have limited visibility or influence. “This creates familiar third-party risks around market concentration, limited transparency over the underlying model, and reduced visibility into how changes at that upstream layer may affect performance,” he says.

Yet Mr Newcomb also points to a more encouraging feature of the current market: many AI applications are now being built on a model-agnostic basis, allowing organisations to switch more readily between providers such as ChatGPT, Gemini, and Claude. This reduces lock-in risk, creates leverage over price and performance, and gives customers a practical way to diversify exposure at the model layer, he says. The capability is not perfectly interchangeable in every case, but it is often sufficiently substitutable to reduce dependence on any single provider. In that respect, competition in the AI market is helping to soften third-party concentration risk.

AI and cybersecurity

Another dimension of AI-related third-party risk that is often overlooked is the cybersecurity implications of connecting third-party AI tools to an organisation’s systems and data. “When you grant a third-party AI provider access to your data, whether for analytics, customer service, or decision support, you are creating a new attack surface,” says Mr Steenkamp. “The integration itself becomes a pathway for risk. How is data transmitted to the provider? Where is it processed and stored? What visibility do you have over who accesses it within the provider’s environment? These are the practical questions that sit behind every AI-related risk decision.”

These risks are compounded when employees adopt AI tools without formal approval, a practice known as ‘shadow AI,’ which can mean organisations unknowingly expose sensitive data to third-party providers without any contractual protections, security assessments, or oversight mechanisms in place. “You cannot manage a third-party relationship that you do not know exists,” Mr Steenkamp says. “Shadow AI is not just a governance gap; it is an unmanaged third-party risk.”

Directors need to ask, if this AI vendor goes offline tomorrow, do we still have the human expertise to step in?

Michelle Dawson
Director, Risk Advisory
Clayton Utz

AI: The new key person risk?

Another emerging challenge is that as organisations use AI to deliver a wider range of tasks, the skills and capacity of their human workforce will inevitably decline. Already, in Australia, there have been high-profile examples of large organisations reducing their headcount in response to AI-driven productivity gains.

This offers a financial dividend but increases operational risk: if an AI platform becomes unavailable due to an outage, cyber incident, or contractual dispute, these organisations may find they lack the capacity to function in the old-fashioned way. Reverting to manual processes and rebuilding human capability can be slow and expensive, potentially wiping out the commercial gain. In this sense, AI may become the new 'key person' risk, says Ms Dawson.

Governance and the upside of competition

In Australia, liability and accountability for AI-related risk are complex. ASIC has called for stronger governance frameworks to protect consumers and clarify organisations' responsibility for third-party issues, noting in a 2024 review that nearly 50% of AI licensees lacked policies addressing consumer fairness or bias, and even fewer disclosed their use of AI to customers.[13] Yet directors cannot wait for the still-evolving regulatory landscape to catch up: they are already subject to AI-related liability through existing consumer law, human rights charters, and anti-discrimination frameworks.[14] "This means the organisation should extend existing governance mechanisms to include AI-related risk, rather than creating new ones," says Doug Nixon, leader of Clayton Utz's Risk Advisory practice. Where organisations struggle with AI governance, it is often because they lack a strong, holistic risk management framework, rather than because AI introduces an entirely new category of risk, he says.

A framework for managing AI-related third-party risks

1	Establish accountability	• **Objective:** Embed AI risk management into existing oversight structures. • **Actions:** Assign clear responsibility; integrate legal obligations and transparency requirements. • **Third-party risk lens:** Upstream providers have contractual responsibility for visibility over downstream providers.
2	Define risk tolerance	• **Objective:** Clarify intended use cases and define acceptable risk thresholds for each use case before deployment. • **Actions:** Identify foreseeable misuse and set explicit thresholds for ceasing operations. • **Third-party risk lens:** Due diligence must move beyond vendor questionnaires to assess how and where a tool is used. Risk tolerance will vary depending on the sensitivity of the use case and the organisation.
3	Identify systemic risks	• **Objective:** Test for large-scale or catastrophic failure modes. • **Actions:** Assess the potential for severe impacts, such as widespread bias or security threats. • **Third-party risk lens:** Over-reliance on a provider creates risk; a failure could cripple the entire organisation. Stress tests to determine how a provider holds up under extreme pressure are critical.
4	Measure trustworthiness	• **Objective:** Regularly test systems to find and fix their weaknesses. • **Actions:** Use simulated attacks to expose dangerous weaknesses; track risks even where they are difficult to measure. • **Third-party risk lens:** Conduct independent checks and ask for evidence of a vendor's own testing, including reports from simulated attacks.
5	Implement proportionate controls	• **Objective:** Identify and manage the most serious risks at each stage of deploying a tool. • **Actions:** Make explicit 'go or no-go' decisions at each stage of development; ensure you can switch off systems if risks become too high. • **Third-party risk lens:** Controls should be stronger for higher-risk systems. Specify the level of access to tools at the procurement stage.
6	Document and disclose	• **Objective:** Ensure accountability by maintaining clear records and engaging regularly with vendors. • **Actions:** Document risk assessments of both individual tools and the overall system and and communicate the conclusions clearly. • **Third-party risk lens:** Transparency is the foundation of trust. Clear, organised disclosures allow firms to compare vendors and meet regulatory obligations.

Source: Adapted from UC Berkeley Center for Long-Term Cybersecurity [15]

The contract is only one part of your data protection strategy. Assess that your vendors can, in fact, protect your data. Due diligence of both your vendor and their products is key.

Monique Azzopardi
Special Counsel, Technology and Privacy
Clayton Utz

Embedding digital third-party risk management in procurement and contracting

Organisations typically spend the most time examining digital third-party risk during procurement and contracting. The procurement process offers a good opportunity to adopt and embed a strong digital third-party risk management framework, but many organisations miss out by getting the timing and sequencing wrong, says John Dieckmann, a Clayton Utz partner specialising in technology procurement and the protection of digital assets.

Treating procurement as a linear process, where an organisation defines its requirements, selects a vendor, and only then engages a legal team to negotiate the contract, leaves little room to meaningfully manage risk. This is particularly true for third-party risk, as a rushed process often fails to interrogate the supply chain and examine which fourth-party vendors are providing the underlying service.

A more effective approach is for legal, IT, risk, and commercial teams to work collaboratively at the earliest stages of procurement to consider how a proposed solution or service will operate in practice, and to understand and devise a plan for managing third-party risk.

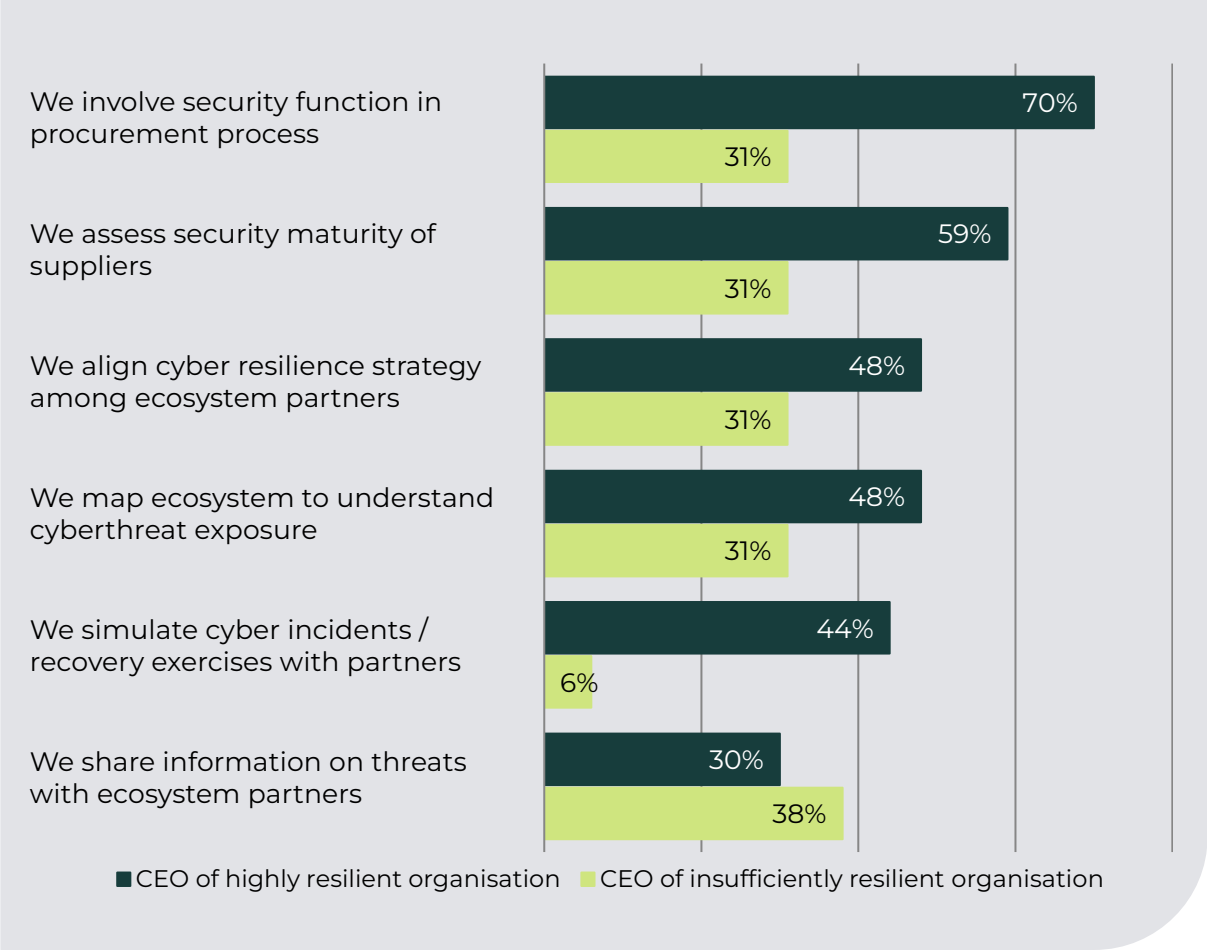
This means working through scenarios such as vendors' service outages or data breaches, as well as failures within the supplier's own supply chain, to determine how the organisation and vendor should respond. It involves understanding how the solution will interface with other parts of the organisation's digital environment, the supplier's dependencies on third parties, and how to deal with any associated risks. When this work occurs alongside the development of go-to-market documents and vendor selection, rather than after it, it can shape the commercial model and risk allocation in ways that are much more difficult to achieve later.

This approach also allows procurement teams to clearly specify the organisation's requirements, taking proper account of those factors, so they can establish a solid foundation for the procurement. "Over 90% of disputes that I see in relation to technology projects stem from poorly drafted or inaccurate specifications. These are simple things like you didn't say what you want, or what you said was ambiguous or lacked the right amount of detail," says Mr Dieckmann.

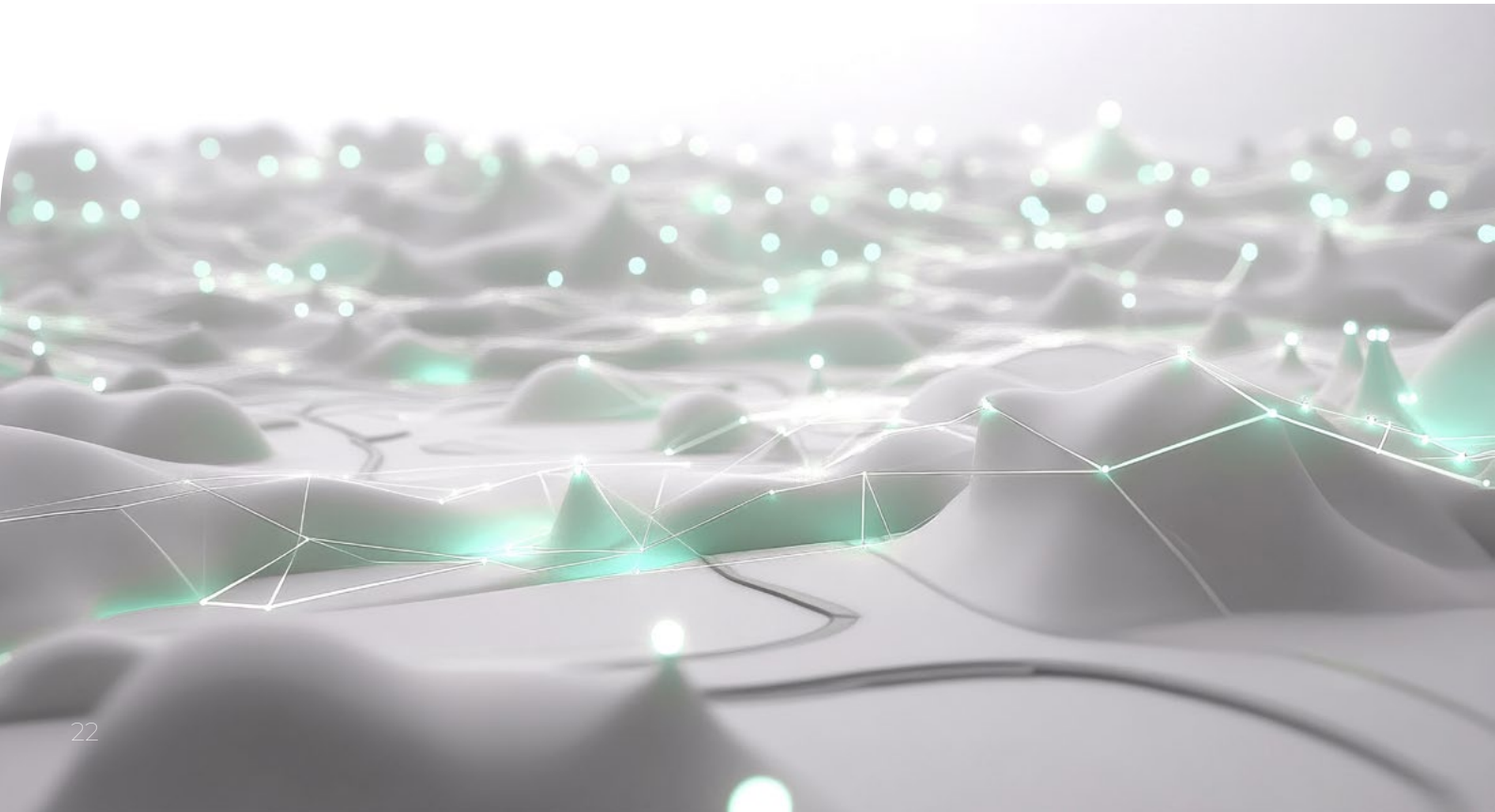
In technology procurement, the key is to invest time upfront to understand what you are buying, what you want, the product or service, and the risks involved, so they can be managed and communicated to the market when it matters most.

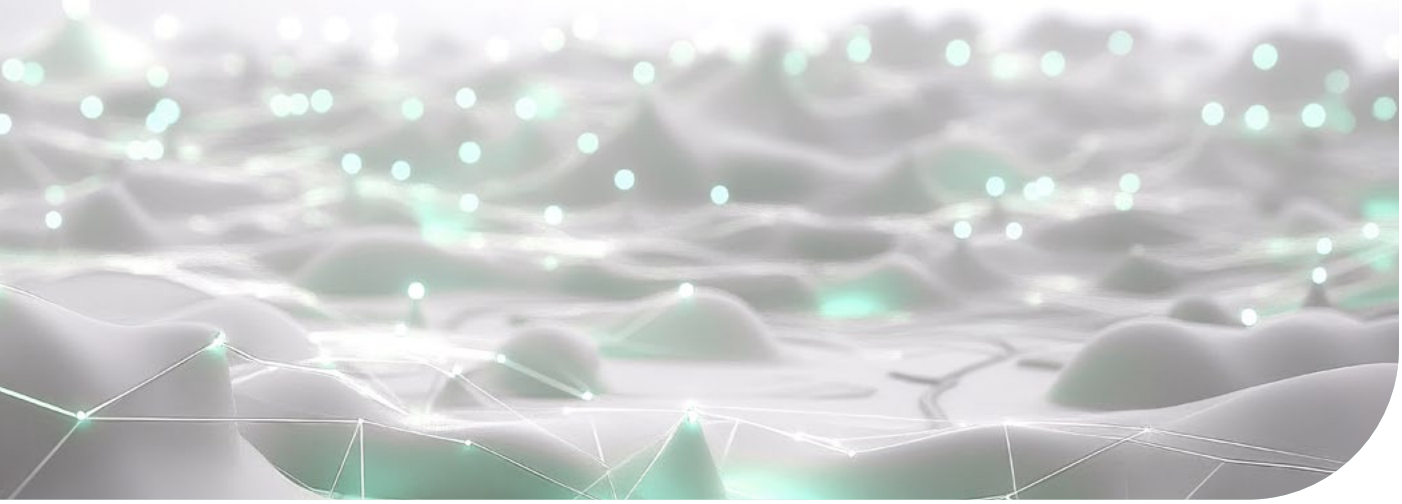
John Dieckmann
Partner, Projects and Technology
Clayton Utz

How does your organisation address supply chain cyber risk?



Source: World Economic Forum[16]





This kind of upfront work can also be embedded through standard-form procurement documentation that includes AI-related provisions covering customer data protection, transparency, accountability, and AI risk controls. This approach recognises that AI-related risk can arise across a wide range of procurements, not only in expressly AI-focused deals, including cloud services incorporating AI, hardware with embedded AI functionality, consultants using AI to produce deliverables, managed services involving AI-enabled solutions, and even arrangements involving model training. Standard clauses of this kind can help organisations address those risks more consistently and allocate them more clearly at the outset.

In the clouds

Cloud services present a particular procurement challenge. Major providers operate globally and offer standardised terms that limit liability, exclude consequential loss, and provide little scope for including bespoke risk management terms. Attempts to negotiate wholesale changes are rarely successful and often delay critical projects without materially improving outcomes.

Organisations need to be thoughtful and deliberate about applying risk management rules depending on how cloud services are used. Systems that are truly critical must have higher thresholds and practical safeguards, such as redundancy, monitoring, and exit plans. The task for procurement teams is to resist one-size-fits-all approaches and align contractual protections to specific use cases, data flows, and fallback arrangements.

Cloud contracting is often complicated by the fact that the provider is being asked to act as a single contractual interface for a solution built on multiple underlying third parties, says Mr Newcomb. That is part of the value of dealing with a single provider, but it also shapes the provider's willingness to accept risk, particularly where it cannot pass that risk down through the supply chain.

There's this fallacy that if it's in the cloud, it's someone else's problem... but the accountability for the data and the service delivery always remains with the organisation. You can't outsource the accountability, even if you've outsourced the infrastructure.

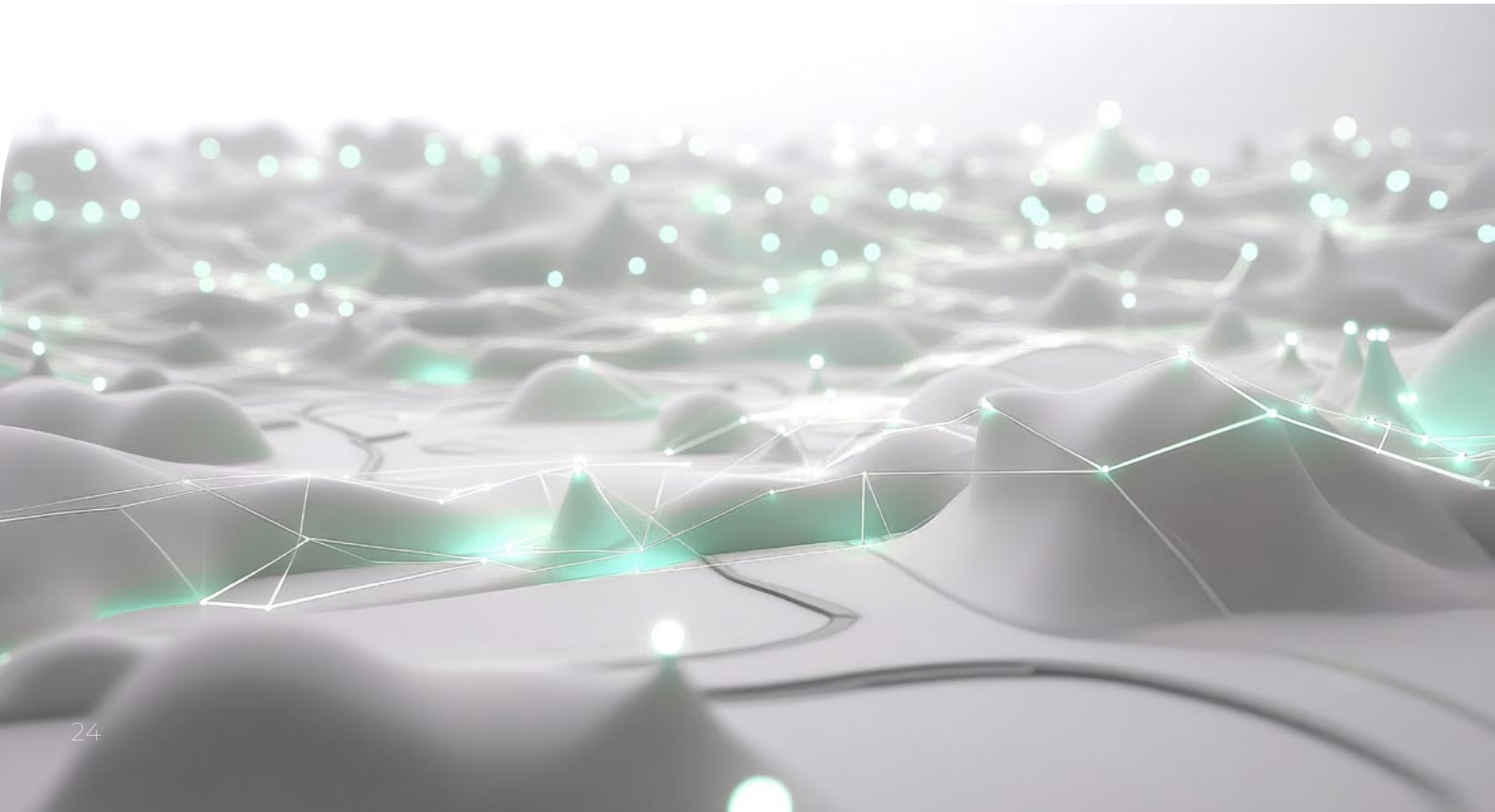
Angie Freeman
Co-Head of Digital
Clayton Utz

Reseller risk

Another recurring source of third-party risk arises in reseller arrangements. This commonly occurs where a service provider implements a solution built on third-party software, whether Software as a Service (SaaS) or licensed software, and acts as a reseller or intermediary for that product. The customer may focus its attention on negotiating the head agreement with the service provider, while the core technology asset, the third-party software itself, is supplied under separate, often boilerplate, terms from the upstream technology provider.

This means that important issues related to security, liability, data handling, service levels, and performance are often covered in an additional contract separate from the main services agreement. An organisation may negotiate detailed obligations with the service provider, only to find that those obligations are not matched, or cannot be flowed down, to the fourth-party provider that actually owns or operates the critical technology. The service provider may have legal liability for potential problems, without a practical route to getting the underlying problem fixed.

The first step to managing reseller risk, explains Mr Newcomb, is to identify the contractual model early and understand precisely what the service provider is supplying, and what is being supplied directly by a downstream technology vendor. From there, organisations can decide where negotiation effort is most needed. In some cases, particularly in larger or more critical transactions, there may be scope to negotiate terms with downstream providers, even major global vendors. Even where the contract remains separate, organisations should ensure the service provider retains meaningful responsibility for managing issues with that third party, including by using its commercial relationship and leverage with the downstream provider to help resolve problems.



Prime contractor risk

Using a prime contractor, or a vendor that manages an entire project including subcontractors, can also obscure underlying risks in the digital supply chain. This is a particular risk for government agencies, says Robert Dearn, a partner in Clayton Utz's Canberra office specialising in digital transformation projects for public sector clients. While engaging a single vendor to deliver an end-to-end solution can simplify a project, it can also mask underlying dependencies if the most material risks sit with a cloud provider, software vendor, or offshore service partner with whom the organisation has no direct contractual relationship.

"The minister and the public don't care that the defective patch that caused a data breach sat three contracts below our prime," says Mr Dearn. Contracts should require transparency over key subcontractors, access to information and assurance, and clear mechanisms to ensure obligations apply across the supply chain, he argues.

For very large or critical transactions, particularly in infrastructure-style projects, organisations may need to go further. Where a third-party technology component is critical to the continued operation of the solution, a direct agreement with that third party may be required in addition to the prime contract. This can preserve access to essential software or services if the prime contractor fails, and may include rights such as novation, breach notification, step-in arrangements, or the ability to maintain payments to the third party so that the underlying contract survives. In projects that depend on critical operational software, that additional contractual link can provide continuity that reliance on the prime contractor alone may not.

Across all of these contexts, a critical but often overlooked point is that the contract marks the beginning of risk management, not the end, says Mr Steenkamp. Contracts that sit unused provide little protection. Rights that are not exercised, metrics that are not monitored, and obligations that are not tested quickly lose their force. "The task is not only to invest effort in putting the contract in place, but also to invest effort in building a team around that contract that can manage it appropriately," Mr Dieckmann says.

It is important to get this right upfront. Renegotiating a contract is rarely quick or easy, particularly once dependency on a vendor has set in. Ultimately, procurement and contracting are not about eliminating digital third-party risk, but about making informed trade-offs grounded in the organisation's risk appetite and a realistic understanding of how services operate in practice.

Third-party resilience should be built into the criteria for success of a project from the outset and properly evaluated as part of the selection of a preferred provider.

Robert Dearn
Partner, Public Sector
Clayton Utz

Risk without borders

For organisations operating across multiple jurisdictions, digital third-party risk management is complicated by overlapping and sometimes inconsistent regulatory regimes. Financial institutions may need to comply simultaneously with APRA's prudential standards in Australia, as well as international rules such as the European Union Digital Operational Resilience Act[17] or the Singapore Monetary Authority's technology risk guidelines[18].

A common response is to map obligations jurisdiction by jurisdiction and layer additional contractual requirements as new rules emerge. Yet this approach can quickly become unmanageable, making procurement complex, fragmenting governance, and increasing the risk that controls are applied unevenly or inconsistently across the organisation.

A 'high-watermark' approach, which aims to meet the most demanding requirements across relevant regimes and apply them consistently across the organisation, reduces duplication and improves resilience.

Rather than asking what each regulator requires in isolation, organisations can first determine what a robust digital third-party risk posture looks like for their own operation, then use that position as a baseline against which regulatory obligations can be mapped and satisfied.

In practice, this means defining risk appetite and governance settings centrally, even when regulatory compliance is localised, to ensure consistent assessment and escalation of digital third-party risk across the organisation, regardless of where a service is delivered. It also means developing contracting strategies that anticipate jurisdictional complexity, rather than responding to it piecemeal. Model clauses, targeted addenda, and agreed fallback positions allow organisations to meet overlapping regulatory requirements without reopening entire agreements each time regulatory expectations shift. Advance planning is critical.

Perfect alignment across jurisdictions is unrealistic. The objective is coherence rather than uniformity: a governance framework that can absorb regulatory variation without fragmenting decision-making or diluting accountability.

You always rise not to the level of your potential, but of your preparation.

Brenton Steenkamp
Head of Cyber
Clayton Utz

Beyond compliance: How to apply a universal governance approach to digital third-party resilience

Some organisations have mature digital third-party risk frameworks. Others, including those in regulated sectors, continue to face weak governance, limited board-level understanding of risk, poorly defined risk appetites, or reliance on legacy systems that prevent them from shifting to more secure and resilient models. Addressing these gaps requires moving beyond compliance-driven approaches towards genuine digital resilience, with third-party risk embedded within broader enterprise risk management rather than treated as a standalone obligation.

Digital third-party resilience ultimately rests on effective risk governance: The same rules and standards that apply to financial, strategic, and operational risk apply. Established frameworks, such as ISO 31000:2018, are a good place to start. These provide a structured approach to identifying, analysing, treating, and monitoring risk, offering a practical foundation for embedding digital third-party resilience within a broader risk management framework.[19]

Ultimately, there is hard work to be done. Organisations should:

1. Establish and articulate risk appetite up front

Evaluate how much risk the organisation can tolerate, assess types of risks, and set out relevant time frames. Risk appetite should be approved at the board or executive level and integrated into decision-making, budgeting, and escalation procedures. Without this clarity, governance can become reactive and inconsistent.

Risk appetite must also account for the different types of risks posed by third parties. Being willing to accept occasional service interruptions from non-critical SaaS tools is different from being prepared to tolerate prolonged outages in essential infrastructure, for example. “You would expect to see a well-articulated risk appetite statement at the top of the house,” says Mr Nixon.

2. Clarify ownership and accountability

Assign clear accountability for third-party digital risk across functions. Ambiguity about whether IT, procurement, legal, or risk management owns the problem leads to gaps and duplication. A common pattern in resilient organisations is that a senior risk owner, often a chief risk officer or equivalent, is responsible for coordinating across functions and is accountable for the overall risk profile.

3. Integrate risk into operational decision-making

Periodic reviews are not enough. Third-party digital risk governance should be integrated into everyday decisions, including vendor selection, investment approvals, project prioritisation, architecture reviews, and incident response planning. Embedding risk considerations into core operational processes ensures they do not remain theoretical.

4. Move from static compliance to dynamic assurance

Good risk governance includes scenario analysis, stress testing, and simulations that challenge critical dependencies and validate assumptions about resilience.

A dynamic assurance approach includes periodic review of risk assessments, collaborating with vendors on incident response exercises, and stress tests to surface latent interdependencies. It is vital to base risk assessments not just on the technology (e.g., 'cloud' or 'AI'), but also on how it is used. Using software to support internal staff tasks presents much lower risk than using the same software to interact with customers, yet lumping them into a single bucket risks making simple services too complicated or failing to implement proper controls for riskier ones. Good risk governance starts by asking: How is this technology used, what depends on it, and what happens if it fails? Only then can the organisation set the appropriate level of control and testing.

"Sophisticated institutions map critical services and dependencies, including second- and third-tier vendors, and run crisis simulations and stress tests," says Mr Nixon. These range from state-sponsored cyber attacks on critical providers to cloud outages that simultaneously disrupt multiple vendors. "The analysis extends beyond direct impact to cascading effects across suppliers' suppliers and critical market infrastructure. Post-mortems then feed back into tighter contracts, stronger business-continuity plans and playbooks, and more rigorous governance and board engagement around these risks."

5. Tailor governance to organisational context

There is no universal template for managing third-party digital risk. A government agency with critical services, a bank with CPS 230 obligations, and a non-regulated commercial entity will all face similar underlying risks, but their tolerance, impact profiles, and regulatory constraints differ. Governance frameworks should be customised to reflect these realities.

Toolkit: an enterprise-wide digital third-party risk management framework

	Toolkit Item	What you need to think about	Who needs to be involved
Foundation setting	**1** **Start with risk tolerance**	• Which digital services are genuinely essential? • What level of disruption is tolerable, and for how long? • Where would failure, misuse or malfunction create regulatory, safety, financial or reputational harm?	• **Board and executive:** approval and ownership of risk appetite • **CRO:** coordination and calibration • **Legal:** regulatory and compliance input • **IT:** technical dependency context • **Business unit leads:** operational impact assessment
	2 **Understand services and value chains, not just suppliers**	• Map which third- and fourth-party digital services support critical functions. • Identify cloud, platform and model dependencies, including shared providers. • Examine where reliance is concentrated or systemic across the enterprise.	• **IT:** technical mapping and architecture review • **Procurement:** vendor landscape knowledge • **Business unit leads:** identifying which services are critical • **CRO:** risk assessment and prioritisation
Pre-procurement	**3** **Assess risk by use case, context, and dependency**	• What decisions or operations depend on it? • What happens if it fails, behaves unpredictably or is misused? • Can humans realistically intervene, and could the service be misused in reasonably foreseeable ways?	• **Business unit leads:** use-case identification and impact assessment • **IT:** technical dependency analysis • **Legal:** regulatory and liability implications • **CRO:** calibrating controls to actual use
	4 **Procurement should consider real-world service failure, not just vendor selection**	• How does the vendor manage operational resilience and security? • What testing, assurance or evaluation supports high-impact services? • What happens if the service fails under real-world conditions?	• **CRO:** stress-testing assumptions • **IT:** technical due diligence • **Business unit leads:** confirming requirements and acceptable trade-offs
Procurement and contracting	**5** **Embed the risk management into vendor selection and contractual frameworks**	• How will major changes be communicated and governed? • What rights exist to suspend, substitute or disengage? • If standard terms cannot support these needs, what governance and fallback planning will compensate?	• **Legal:** structuring protections and negotiation strategy • **Procurement:** vendor engagement and negotiation • **IT:** technical due diligence
	6 **Build post-execution mechanisms into contracts**	• How will key vendor obligations be linked to operational oversight? • How can contracts be structured to anticipate renegotiation when dependencies deepen? • For services with enterprise-wide impact, are structured review points built in, rather than relying solely on renewal cycles?	• **Legal:** contractual governance and renewal strategy • **Procurement:** relationship management, including a dedicated contract management team for critical vendors

	Toolkit Item	What you need to think about	Who needs to be involved
Operational assurance	**7** Treat contracts as living instruments for ongoing management	• Are critical assumptions reviewed periodically? • Are dependencies and exit feasibility assessed as services scale? • Does senior management have visibility over material digital dependencies?	• **IT:** monitoring technical KPIs and service levels • **Procurement:** relationship management • **Legal:** reviewing evolving obligations and renewal terms
	8 Test assumptions and prepare for loss of control	• What would we do if this service failed or behaved unexpectedly tomorrow? • Who would make the decision to suspend or disengage, and what information would they need? • How quickly could we switch, contain harm, or communicate externally? • Are joint testing exercises regularly conducted with critical vendors?	• **CRO:** scenario planning, designing and coordinating tests • **IT:** executing simulations and technical recovery exercises • **Board and executive:** oversight of results and strategic implications
Ongoing	**Document decisions and engage appropriately**	For critical digital services: • Document the intended purpose. • Record the material risks identified. • Capture the mitigation measures adopted. • Record the residual risks accepted and why. • Be transparent with regulators, customers and affected stakeholders. Clear documentation supports defensible decision-making and aligns with emerging expectations under AI and digital governance standards.	• **Board and executive:** sign off • **CRO:** risk assessments and residual risk acceptance; regulatory engagement • **Legal:** contractual protections and disclosure obligations; formal records • **Procurement:** vendor selection rationale and performance • **Business unit leads:** intended purpose and use cases • **Communications:** stakeholder transparency

Government agencies

- Clarify risk appetite for critical digital services, considering public accountability, and assess dependency across entire service ecosystems, not just isolated projects.
- Scenario-test continuity and exit plans (outages, vendor/transition failures), and use the findings to inform governance and procurement.

Regulated entities (e.g., CPS 230, SOCI)

- Translate regulatory expectations into operational decisions on resilience and extend oversight to upstream cloud and AI dependencies beyond tier-1 providers.
- Validate assumptions through regular stress testing and scenario analysis, ensuring board oversight of results.

Non-regulated entities

- Align governance effort with actual digital dependency risk, focusing on the most critical services and tolerable disruption levels.
- Build resilience incrementally through contracts, oversight, and testing aligned to renewals and service change.

Source: Clayton Utz, drawing on UC Berkeley Center for Long-Term Cybersecurity's AI Risk-Management Standards Profile for General-Purpose AI (GPAI) and Foundation Models

End notes

1 Australian Securities and Investments Commission, “Key issues outlook 2026,“ January 27th 2026. https://www.asic.gov.au/about-asic/news-centre/news-items/key-issues-outlook-2026/

2 World Economic Forum, “Global Cybersecurity Outlook 2026,” January 2026. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf; licensed under CC BY 4.0; https://creativecommons.org/licenses/by/4.0/

3 As above.

4 Microsoft, “Helping our customers through the CrowdStrike outage,” July 20th 2024. https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/

5 ABC News, “CrowdStrike outage tipped to leave Australian businesses with damage bill surpassing $1 billion,” July 22nd 2024. htottps://www.abc.net.au/news/2024-07-22/crowdstrike-outage-bill-for-australian-business-may-be-1-billion/10412748ends6

6 World Economic Forum. As above.

7 APRA, “Prudential Standard CPS 230: Operational Risk Management,” July 2025. https://www.apra.gov.au/sites/default/files/2023-07/Prudential%20Standard%20CPS%20230%20Operational%20Risk%20Management%20-%20clean.pdf

8 CISC, “Security of Critical Infrastructure Act 2018 (SOCI),” August 27th 2024. https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-ac t-2018

9 Stanford University HAI, “The 2025 AI Index Report,” 2025. https://hai.stanford.edu/ai-index/2025-ai-index-report

10 World Economic Forum. As above.

11 UNSW Sydney, “Beyond black box AI: Pitfalls in machine learning interpretability,” 2024. https://www.businessthink.unsw.edu.au/articles/black-box-AI-models-bias-interpretability

12 European Central Bank, “The rise of artificial intelligence: benefits and risks for financial stability,” 2024. https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html#toc5

13 ASIC, “ASIC warns governance gap could emerge in first report on AI adoption by licensees,” October 29th 2024. https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2024-releases/24-238mr-asic-warns-governance-gap-could-emerge-in-first-report-on-ai-adoption-by-licensees/

14 Department of Industry, Science and Resources, “Australia’s AI Ethics Principles,” December 2nd 2025. https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles/australias-ai-ethics-principles

15 UC Berkeley Center for Long-Term Cybersecurity, “AI Risk-Management Standards Profile for General-Purpose AI and Foundation Models, Version 1.1,” January 2025. https://cltc.berkeley.edu/wp-content/uploads/2025/01/Berkeley-AI-Risk-Management-Standards-Profile-for-General-Purpose-AI-and-Foundation-Models-v1-1.pdf

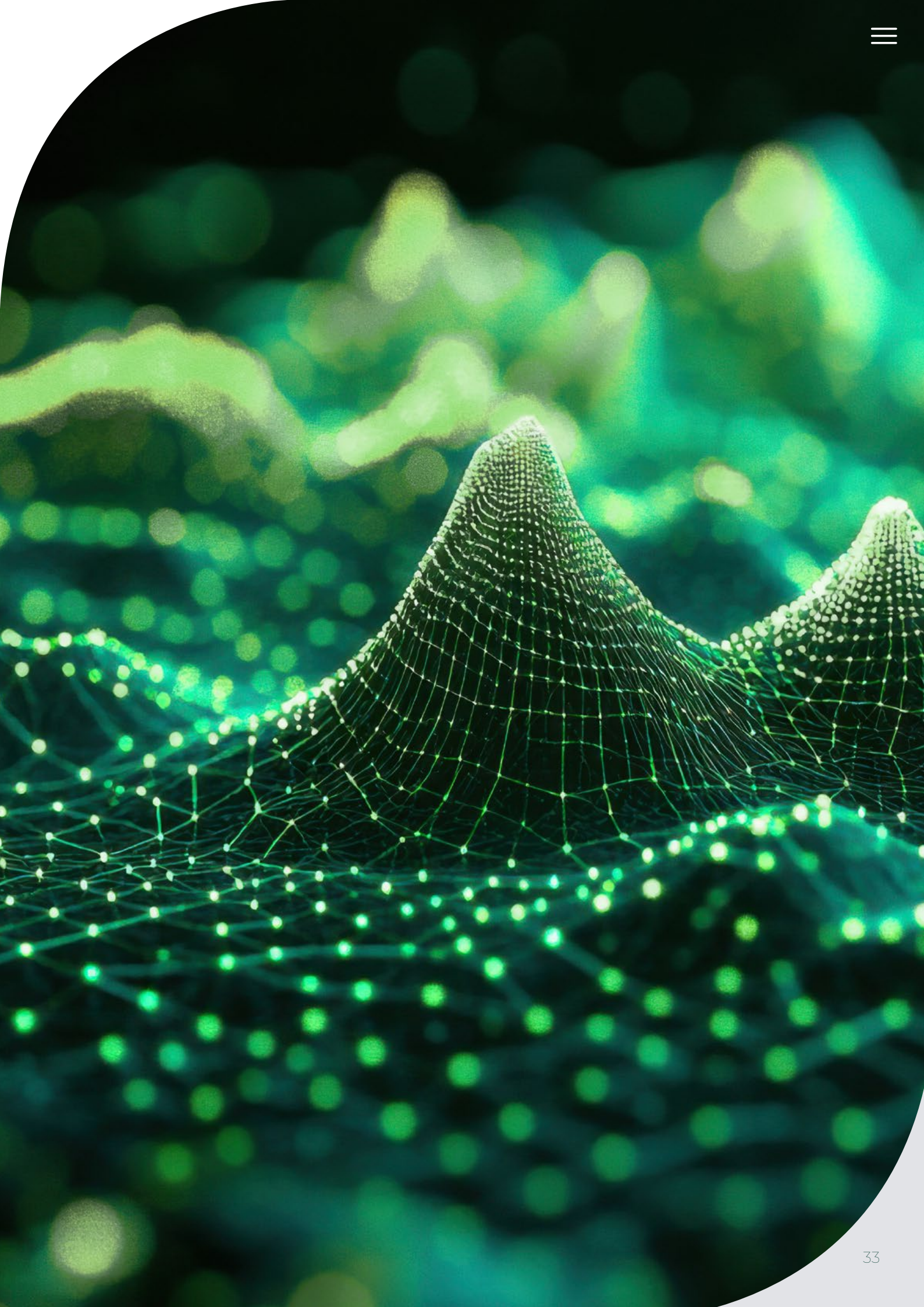
16 World Economic Forum. As above.

17 EIOPA, “Digital Operational Resilience Act (DORA),” January 17th 2025. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

18 Monetary Authority of Singapore, “Guidelines on Risk Management Practices - Technology Risk,” January 18th 2021. https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines

19 ISO, “ISO 31000:2018 Risk management - Guidelines,” 2018. https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

20 UC Berkeley Center for Long-Term Cybersecurity. As above.



CLAYTON UTZ

claytonutz.com