



Tech Modernisation: agility, resilience, and growth in the era of AI

The guide to building foundations of AI

Introduction

The rate of change in technology is accelerating once again, with AI infusing its profound capability into systems and services. In our work with partners in Australia and across the world, Cognizant knows that tapping into AI’s potential requires flexibility. We must be ready to experiment, test, and integrate with confidence. However, the constant question we hear from the marketplace is “how do we get the underlying foundations to be AI ready?”

We believe in pervasive AI, where AI is seamlessly integrated into the tools we use every day. Pervasive AI sits everywhere it needs to, but “not simply everywhere”. Our ability to integrate AI solutions is limited by existing complexity in our systems and processes. Finding the path to efficiently review these complexities will define our ability to embrace the tomorrow that is already upon us.

AI is prompting everyone to ask questions of technology. It gives us a mandate to modernise, reduce tech debt and improve agility. However, pursuing modernisation should not stop us from taking steps to start our AI journey already today.

Working with Adapt, an Australian IT research and advisory firm, we uncovered where leading Australian executives see technology modernisation on their list of organisational priorities in 2025.

Organisational goals in 2025: CIO	
1. Tech modernisation and simplification	6. Creating new revenue and business models
2. Improving operational effectiveness	6. Acquiring and retaining customers
3. Optimising costs	8. Attracting and retaining talent
4. Developing the AI strategy and roadmap	9. Creating a data-driven organisation
5. Building a secure and trusted organisation	10. Digitisation and automation of key processes

ADAPT CIO Edge Survey in Feb 2025. Sample size: 210 Australian CIOs

Achieving the above goals ultimately contributes to managing cost, ensuring security, and improving speed to value, which remain the CIOs target destination and every evolution in our IT systems must still be driving us toward these goals.

Average progress in modernisation

Infrastructure modernised

52

Applications connected via APIs

40

Building and reusing data assets

34

Orders taken entirely digitally

34

Workflows automated

26

Creating a single view of the customer/constituent

26

Applications consolidated compared to 12 months ago

22

Services available via omnichannel experience

19

Automating decision making

15

ADAPT CIO Edge Survey in Feb 2025. Sample size: 132 Australian CIOs

While infrastructure leads and is the starting point in typical modernisation programs, most new areas of modernisation momentum – such as automation, app consolidation, and creating single view customer intelligence – have a long way to go and remain relatively underexamined.

Making AI work in my enterprise environment

At Cognizant we have examined these findings and have worked with our experts to offer insights from our real-world experience in helping clients to modernise their enterprise and build environments for agility and resilience. It is our intent here with the creation of this **Tech Modernisation Guide** to offer practical recommendations on what we have found works, and what doesn't – to help accelerate adoption of AI for our partners and clients.

Four essential factors driving impactful modernisation

At Cognizant we believe there are four related streams of activity that build the path to a truly modernised enterprise technology environment.



Modern engineering



Data enablement



Legacy transformation



Security design

Through the following sections we highlight the importance of each. What they shift in your business potential, how their value can be established, and what others are already seeing from their progress in these areas to date.



Modern Engineering



Aligning business process prepares operations for AI evolution

An enterprise does not transform by declaring a five-year plan. Iterative experiments anchored to real outcomes are key to moving from old ways of working into the age of the AI-augmented modern engineering paradigm.

Enabling updated systems and processes built on modern engineering practice holds the power to improve both speed and quality in enterprise software development cycles. But it requires a commitment to real change led by leadership with strong support and training throughout the organisation.

It can be difficult to push through cultural barriers when trying to drive real change. Working with external partners can offer the third-party insight required to look clearly at where problems lie and how best to address them.

Measuring workflow to optimise process

While technologies change, the fundamentals of knowledge work do not. Investigation of engineering practice must examine enterprise-wide systems and processes to uncover the complete picture of interdependent cycle times, constraints, and the nature of the variations that define your unique business needs.

Everything must be on the table to iteratively test and measure the status quo, identify blockers, improve flow, and automate the right processes to elevate consistency and reduce unforced errors. Optimisation must take a global view of entire value streams. Local optimisation lacks the context needed to see where added speed in one process may result in negative impacts elsewhere in the value chain.

DORA is the tool of choice at Cognizant to measure workflow performance. This gives clarity to agility and throughput, enables observability and identifies where constraints lie in engineering processes. It reveals where we can optimise for greater quality and speed, giving organisations the metrics required to support the business case for evolving our engineering systems.

When leadership feels burnt by past failures, justifying upfront cost to establish a new library of automations, for example, to improve consistency and speed in engineering processes can seem too high based on the first deployment. But insights through end-to-end workflow measurement can demonstrate the savings generated after deployment 10, 50, and 500.

Average progress in modernisation

26%

feel they have progressed in workflow automation.

15%

have progressed automated decision making

ADAPT CIO Edge Survey in Feb 2025

Good tools generate gravity

Organisations trend toward a proliferation of tools, with pressure focused around tool evaluation as a focal point of cost, speed, and security. But this focus on how tools are being adopted as a proxy for modernisation is misplaced, with mandates providing an easy path to meeting such measures while losing sight of the outcomes that could be negatively impacted if bad tools result in poorer processes.

Mandates rarely translate to successful modernisation. Everyone knows the experience of new tools that are introduced but never adopted because they failed to generate enough excitement and value upon introduction.

Whether designing new automation templates for consistent and confident deployment processes or new applications that support a modernised workflow, the key to successful change is to show users the value in adopting the new. When new internal platforms enhance the developer experience, they succeed by providing enough value that teams are motivated to adopt them.

The ‘right’ tools feel easy, helping teams to reserve cognitive load for the complexity of the problem they are working on rather than the incidental complexity of poor tools and systems. They have a gravity, attracting users quickly who want the improvements to become part of their daily routine as soon as possible.

Automation breeds consistency

Achieving a tight automation loop is key to modern engineering practice. Through development, feedback, leveraging AI, security, and then rapid deployment, testing, and observability, automation gives us the consistency of workflow and confidence that we have maintained quality design through the templates we have put in place.

Some of the most transformative work we have delivered for partners is through automation that standardises around consistent deployment patterns. Using ready-to-deploy cloud infrastructure platforms designed with security as code and compliance as code, we can standardise behaviour, keep costs trackable, and dramatically reduce risk.

At some of Australia’s largest mining and retail enterprises, we have seen powerful and measurable results.

- Reduced deployment time by 80%
- Self-service increased from 0% to 60%
- Reduced manual touch by 66% - two-thirds of manual requests disappeared
- Turnaround times reduced by 80%

This has accelerated software teams, making it faster than ever to bring solutions into the business. Consistency through automation breeds confidence in deployment quality and achieves greater benefit to the humans across the business as important infrastructure can be deployed faster and with high reliability.

AI in modern engineering

AI holds great power as part of an optimised workflow. But you must have your modern engineering fundamentals in place to know the AI tools are delivering what you need.

Many have already seen code assistants as a positive contribution, and Github metrics point to a widespread increase in code velocity. But raw code velocity may exacerbate existing constraints and bottlenecks or introduce other impediments to production output quality, as well as place strain on traditional code review processes due to increased volume. Quality predicts speed, but speed does not predict quality.

Defects compound as we increase outputs through the speed benefits of AI, making safeguards more important than ever to minimise unintended bugs. We must avoid a new era of AI generated tech debt caused by poor oversight.

The more robust your modern engineering process is, the better placed you are for AI adoption. Automated quality checks, architectural fitness functions, and wider automations that ensure consistency all work together to preserve the stability of every aspect of your systems. With these in place, AI becomes a true team enhancement that can be adopted with confidence.

A man in a dark suit is walking away from the camera down a long, brightly lit corridor. The ceiling is a vibrant red, and the walls are made of glass, reflecting the light. The floor is highly reflective, showing a clear reflection of the man. At the end of the corridor, a large window offers a view of a city skyline. The overall atmosphere is modern and professional.

Legacy Transformation

Transforming legacy systems to resolve tech debt and increase agility

Old business systems and infrastructure become an issue for the enterprise when they start to weigh us down, becoming a pain point for cost and agility. When we take steps to deal with a complex legacy environment, we must remember we are looking to unshackle the enterprise from unnecessary costs and roadblocks to better meet the demands of the wider business today in a new operations environment.

Complexity is a symptom

Complexity does not happen by design. It is a symptom of a range of problems that have crept into technology systems over time. Sometimes complexity arrives as business users bypass IT to buy their own tech. Other times it is the emergence of exceptions to rules and standards that add fragmentation to our tech environment.

Regardless of how it enters our environment, the friction complexity introduces over time explains why IT systems start to see added cost as well as lowered visibility of what is happening, who is controlling it, and how well the tech is meeting business needs.

Application consolidation

Average progress in modernisation

Just 22%

of businesses feel they have progressed in application consolidation compared to 12 months ago.

ADAPT CIO Edge Survey in Feb 2025

Investment priorities of CIOs

63%

see application integration as an investment priority for the next 12 months. 64% rate enterprise architecture as a priority

ADAPT research shows that consolidation and automation are progressing slowly for many organisations. But the integration and improved enterprise architecture are high priorities for the year ahead.

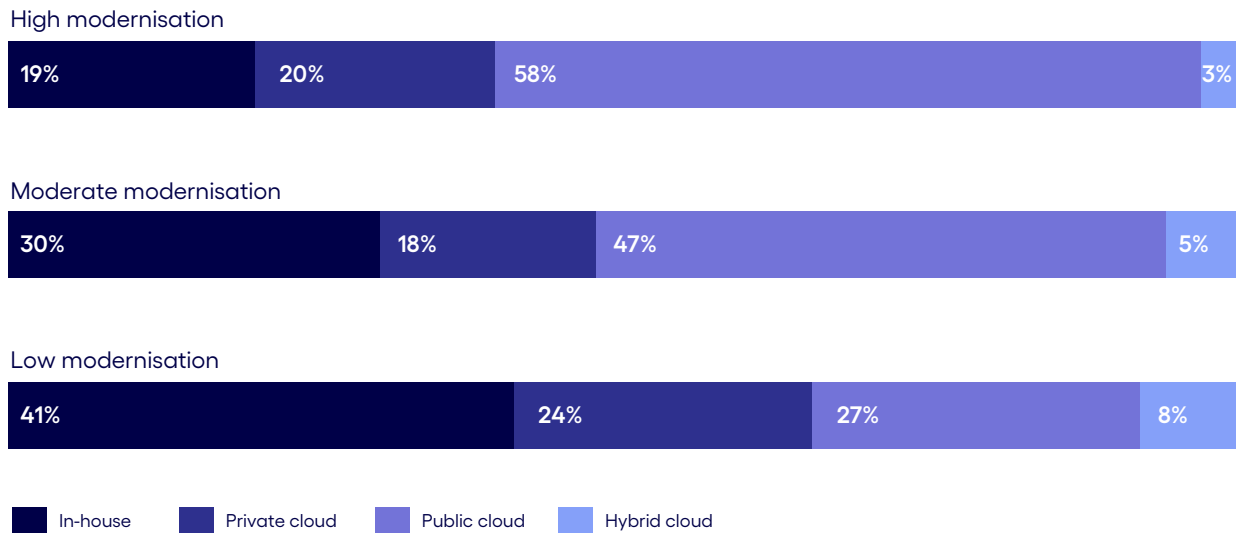
The work of consolidation and integration can be difficult and costly, and with a longer timeline for ROI it is a difficult business case to build. But pursuing application consolidation can be particularly powerful in heavily siloed businesses or where organisations have been acquired and integrated over time. These common scenarios lead to duplication across the technology environment.

Reducing application architecture complexity, depreciating and consolidating the portfolio of technology, and modernising application infrastructure has a significant impact on the return on the value of IT investment and the speed of delivery for the business.

The role of cloud in modernisation

ADAPT research found that organisations leveraging public cloud are 1.4x more likely to achieve high levels of modernisation compared to those keeping workloads primarily in-house. Upgrading infrastructure for better flexibility and scale is an essential step on the path to accessing new capabilities – especially AI.

Infrastructure modernisation and average workloads allocation



ADAPT Cloud and Infrastructure Edge Survey in Jul 2024. Sample size: 108 Australian Infrastructure leaders

However, well-known problems come with the ‘lift and shift’ style of moving to the cloud. A need to move quickly results in a lack of optimisation, with the work left on the tech debt “to-do” list while excessive costs hit the tech budget year after year.

Those leveraging public cloud are **1.4x** likely to achieve high levels of modernisation

A more subtle issue stems from a lack of investment in effective training in the skills required to manage cloud complexity. In the capex world of on-prem systems, costs are controlled through paperwork and sign offs to bring in new hardware. In the cloud, costs can potentially be unlimited with a single click. Establishing good FinOps and cloud cost governance practices are essential to cloud success.

In the shift out of the data centre and into the cloud, it can also feel natural for ClickOps to be part of the journey. But maintaining a ClickOps approach to deployment fails to embrace the consistency and efficiency of cloud automation. We must choose to establish standardised, cloud native approaches and infrastructure designs such as Infrastructure as Code to establish repeatable and dependable patterns that deliver strong observability, security hardening, cost control, and consistency.

The cost of tech debt

Solving legacy complexity is like changing the wheel on a bicycle while riding it. If you're just keeping up with delivering day-to-day business activity it's hard to find the capacity to invest in resolving these tech debt problems.

But tech debt is also an ongoing opportunity cost to the business. A cost to doing a lot more with the same spend, or the opportunity to spend a lot less to get the same outcome. These debts must be addressed to get our baseline effectiveness on track. As we examine legacy roadblocks for an organisation, we identify opportunities such as hollowing out legacy applications for a cost effective cloud transition.

Finding how to overcome these final humps in the legacy cost burden is essential to become confident in switching off old systems that carry cost and complexity. There can be internal resistance to arriving at that final 'switch off' and there are often doubts about the transition being complete. This is where working with an independent third party like Cognizant can help to ensure all dependencies have been resolved and to overcome internal friction and objections. Once achieved, we can stop checking the rearview mirror and shift our focus firmly toward the future.

Observability shines a light on complexity

The launchpad for solving complexity is capturing the clearest picture we can on where we are today and where we want to be tomorrow.

As with our modern engineering approach, observability is essential to making sure we understand the reality of what is happening with the systems that are being used. We use DORA metrics to inform recommendations on the right path forward, and we use FinOps to understand your cost position.

Our 2024 research on Cost Intelligence points to the importance of aligning costs to real business value. This offers many benefits, and it improves the tech team's ability to tell its story and state its business case to the wider organisation.



Optimising cloud for cost and performance

A leading insurance company across Australia and New Zealand successfully migrated its legacy data warehouse to Amazon Redshift data warehouse service but found that its cost base doubled and batch task execution was too slow. The Cognizant team worked with the insurer to assess where the data warehouse was underperforming to uncover the best approach for optimising toward the institution's target outcomes.

Cognizant found that organisation's Redshift cluster configuration was designed with more nodes than required across both production and non-production environments. The discovery process found that average utilisation was well-below capacity under this design. Adjustments to reduce nodes in the cluster could quickly improve cost without compromising performance.

To optimise batch processing, Cognizant moved the client from sequential to parallel SQL scripts execution, converted Datashare to materialised views and simplified data structures.

Through changes to the Redshift cluster design, the insurer saw its AWS costs reduced by over 65% with projected savings to the organisation over \$1 million per year. The optimized overnight batch jobs are now consistently completed well ahead of the deadline.

Through Cognizant's careful analysis and optimisation program, the insurance organisation gained the full benefit of its legacy migration into the Amazon Redshift data warehouse while achieving the cost and performance benefits.

The role of AI in resolving complexity

AI holds great potential to support complexity reduction and help simplify and modernise applications. It can be leveraged to provide fast analysis of code bases, to generate documentation. At a large Telco Cognizant has used AI across the software development life cycle (SDLC) to aid code reviews and merge duplicated processes. We also advise clients to use AI to enhance test case coverage, and to help engineer the uplift of included libraries to reduce security risks and reduce technical debt. All of these can contribute to accelerated build cycles with improved quality outcomes.



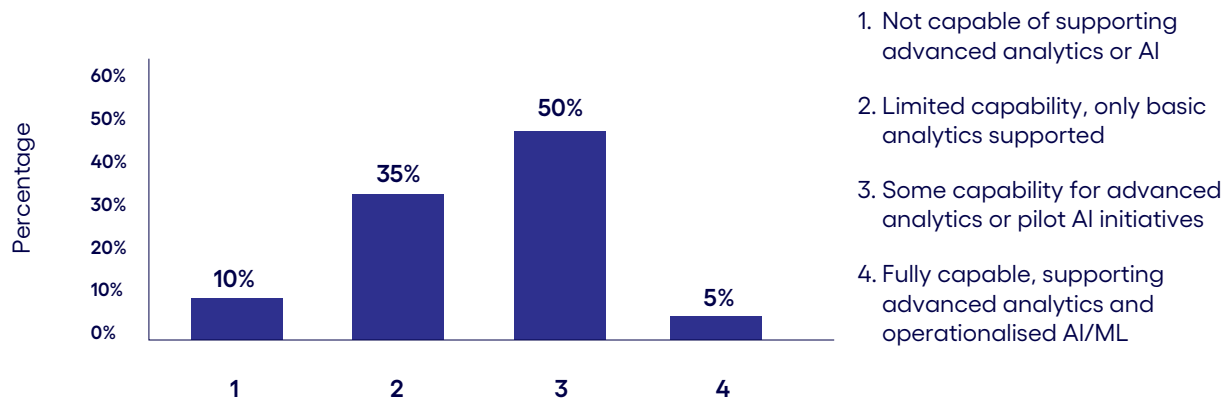
Data Enablement

Enabling data to support AI-empowered enterprise applications

Historically a cost centre, data is a fuel for business outcomes. We must empower the Chief Data Officer to drive new products and environments that become part of our revenue engine.

Data and AI go hand-in-hand for what comes next in business transformation. But data environments are complex, quite like our wider concerns with legacy systems. Data has grown almost exponentially since the cloud era began while the budgets to refine and align this data are heavily constrained.

Has your data environment enabled the adoption of advanced analytics, AI, or machine learning?



ADAPT CIO Edge Survey in Feb 2025. Sample size: 200 Australian CIOs

45% of organisations have limited or no capability to support advanced analytics & AI

So how do we maximise the value of our data as it exists today? We need to understand existing data and APIs that have been tested and productionised, to allow AI agents to leverage these as tool calls. This will generate additional value from their re-use. At Cognizant we create agentic frameworks to help enrich or accelerate business processes. Agentic frameworks leverage existing data and APIs and help lift the level of integration across applications and data sources.

Data governance as a challenge to scaling production

Feeding data into AI for a proof of concept has been a manageable process to date, but transitioning to production scale is a challenge. We see many organisations arriving at a conflict between data governance systems that can either be too loose or too restrictive.

Barriers to AI in 2025: CIO

After funding, data security is reported as **#2** barrier to scaling AI to production.

ADAPT CIO Edge Survey in Feb 2025

Governance has often been treated as a security problem, which is reflected in how few organisations in Adapt's research are achieving high levels of data integration. If it is governed, it must be locked down.

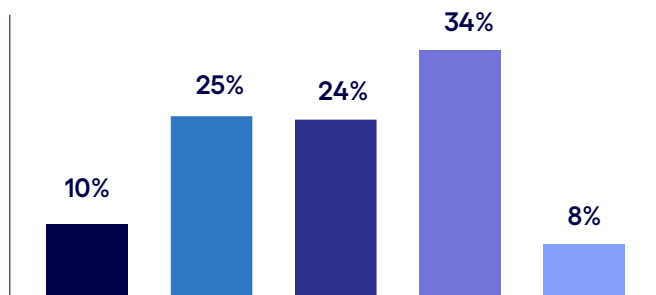
There are other ways to approach governance. While some systems may slow or block modes of access, and therefore progress, governance can instead be embedded into your ways of working.

Today we understand that lightweight, agile, iterative approaches to data governance allow for adaptability that maintains due care while responding to business needs.

Not all data is equal. Finance and marketing data, for example, require different governance models to enable the right restrictions and freedoms to deliver value in and around the business.

How mature is your organisation in assigning clear role and accountability for data governance?

Assigning clear role and accountability for data governance



35%

of organisations are immature in accountability for data governance.

As AI opportunities have arrived, data value maps have shifted. There are new ways to extract value for internal needs and new paths to monetise data. Understanding how to apply metadata from existing data systems and update value maps is key.

Some may explore opening broad access to data through BI systems and leave it to individual teams to unlock new value. But teams remain time poor and may not know what is even possible. This makes data literacy programs a powerful opportunity for growth. Advanced LLM-based interfaces that offer natural language assistance will also be a boon for self-service data insights.

The data opportunity must be managed within a wider modern engineering frame to successfully create the required flexibility without unacceptable risk.

Investment priorities of CIOs

62% of CIOs see data literacy, skills and culture as an investment opportunity.

ADAPT CIO Edge Survey in Feb 2025

Cloud and data vendors provide a range of free online training courses as part of the initiative to uplift data literacy. Organisations should leverage these courses to close the gap in the skills required to unlock the value in their enterprise data. They should also ensure that transfer of knowledge takes place on projects involving external technology services consultants, which is a standard practice at Cognizant.

One standard means too many exceptions

The new era requires a move away from “one standard plus exceptions” to stop many exceptions from becoming the norm. Designing a small number of governance models to suit all core needs and user personas gives you the data access control you need to meet all obligations and enjoy full data value wherever you need it.

It can be difficult to identify target outcomes for data systems and services. But there are tasks every enterprise can target to improve data maturity that will always hold value for scaled integration with AI.

- **Map data fundamentals:** Understand how we capture, store, and present our data to stakeholders across the business, whether for use in new data models, via APIs, or feeding advanced analytics tools. We also must map data to business value, both for current usage and its future potential.
- **Identify mission critical data:** Ensure the right data is accessible to the right stakeholders and systems. Clarify your stakeholders – scientists, analysts, dashboards. Mapping data to outputs and insight value adds confidence to how you plumb your data into AI-enabled tools and services.
- **Generate data value maps:** Going further, data value maps can give greater focus to how data will be used and help to balance data security and accessibility. Data value maps should be coupled with DevOps patterns for data or DataOps. This includes applying data interface contracts, adding the ability to leverage data masking and test data creation to help unblock innovation.



Security Design



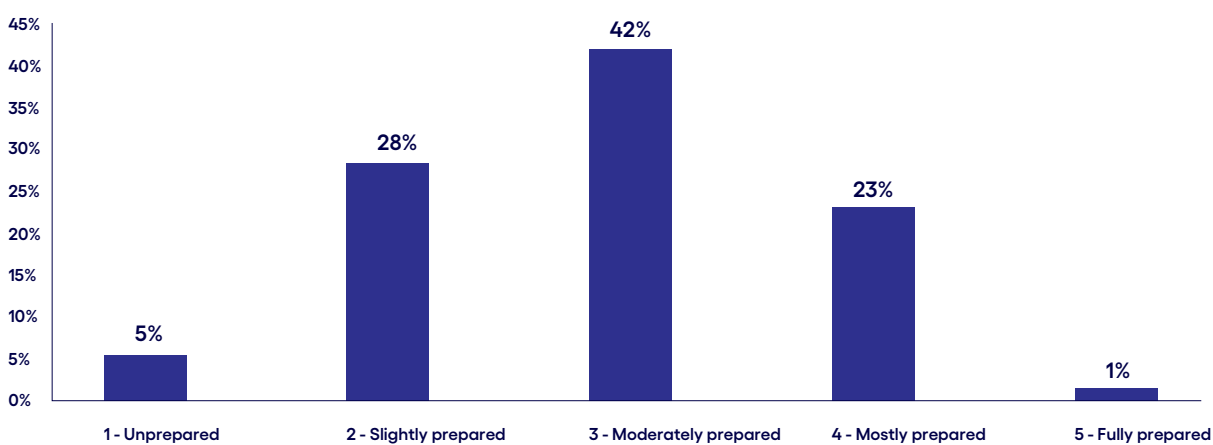
Security for new modes of AI integration and execution

In a world of increasing threats, ensuring adequate security levels aligned to your organisation's risk appetite is a key to delivering sustained business success.

Cybersecurity is crucial for defence against active threats, but also for building trust and confidence for compliance and innovation. While we continuously evolve to strengthen the security posture, adversaries are also evolving at rapid pace to find the weak links across people, processes, and technology to breach our defences.

AI presents both opportunity and risk in cyber security. AI enhances threat detection and response capabilities by automating the analysis of vast amounts of data, identifying patterns, and predicting potential threats with greater accuracy and speed. Yet attackers can exploit AI to develop more sophisticated attacks, such as AI-enhanced phishing and deepfake scams.

How prepared is your organisation to securely adopt and operationalise AI initiatives in the next 12 months?



Source: ADAPT Security Edge Survey in Apr 2025. Sample size: 111 Australian CISOs

Achieving the right risk balance is crucial as AI changes the playing field. Too many restrictions means security becomes a blocker to effective operations, which leads to poorer controls and practices when teams try to route around restrictions. The right posture allows organisations to leverage AI's full potential as a security enhancement while safeguarding against its misuse.

Organisational goals in April 2025: CISO

- | | |
|---|--|
| 1. Building a secure and trusted organisation | 6. Optimising costs |
| 2. Tech modernisation and simplification | 7. Improving resilience against risks (cyber, operational, market-based) |
| 3. Grow the business | 8. Developing the AI strategy and roadmap |
| 4. Improving operational effectiveness | 9. Safeguarding organisational data assets |
| 5. Ensuring governance and compliance | 10. Acquiring and retaining customers |

Source: ADAPT Security Edge Survey in April 2025. Sample size: 130 Australian CISOs

Security initiatives according to CISOs



Improving governance and compliance



Authentication and access management



Configuration and vulnerability management

Even as AI opportunities enter business planning, and with them new risks, the critical approach to managing the security environment remains focused on getting our fundamentals right.

Our recommendation is to continue focusing on three tiers of defence that support one another:

- User awareness to mitigate the most common risks.
- Effective security alert monitoring for real-time incident response
- Secure by Design frameworks that maintain a strong 24/7 bedrock.

AI for Security

AI offers tremendous opportunities as a security support system, improving our default security systems to reduce risk and improve our ability to respond to any given situation.

How much more or less are you expecting to spend on these same activities in 2025?

Cyber security (people, data and software)



ADAPT CIO Edge Survey in Feb 2025. Sample size: 149 Australian CIOs

41% of organisations plan to increase cybersecurity spend in 2025

Automated threat detection and response

AI can improve the efficacy of our traditional tools as we move away from rules based and signature-based monitoring and into behaviour-based security management. This adaptive approach can detect the most subtle signs of malicious activity across organisation-wide data to identify and mitigate attacks. This proactive capability greatly reduces the time to resolution compared with manual intervention.

We now deploy the SOUL tool to turn security playbooks into AI orchestrated automations that include end-to-end audit trails. We have seen typical cycles from threat detection to active response reduce from 8-16 hours down to 15-30 minutes through these automations.

False positive management

With thousands of alerts coming into security dashboards at false positive rates commonly around 60-70% it becomes the norm for alerts to be errors, making it easy for real incidents to slip past our human teams. By contextualising alerts with threat intelligence and insights drawn from real-time assessments of the network, we can now reduce false positives to below 10% and bring the focus onto real problems that need attention.

Investment priorities of CIOs

63% have cyber skills, awareness and engagement as an investment priority.

ADAPT CIO Edge Survey in Feb 2025

AI dashboards and analytics

A typical enterprise will have dozens of security controls across a range of tools and services. Getting a view of the full security posture requires many reports and integrations to see the full picture. We have built an orchestration layer using our Neuro AI framework that gives one unified console to CISOs and security operations teams. It includes a basic LLM that allows for simple queries to explore vulnerabilities, critical assets, risks of exploits, and other insights. Predictive systems can also now analyse risk of cyber attack against a given business and offer mitigation strategies that reduce our overall risk and continue to monitor and improve our posture.

Security skills shortages

With cybersecurity skills in limited supply, access to security expertise remains a key concern for organisations. AI can help to reduce dependency on human workloads by automating routine tasks and providing actionable insights.

Enhance user awareness training

Unsophisticated attackers now have access to tools that make it a breeze to create deepfakes and to exploit business users in a highly targeted fashion. But we can use AI to improve how we educate users and engage them in security literacy. Smarter, more engaging training to keep every user in the best possible mindset for avoiding the most common risks to our business environment.

Security for AI

With AI heading toward a new embedded normal throughout business IT systems, we must incorporate the new risks of AI into our security frameworks. This means data governance must be updated to accommodate new privacy and compliance norms if we allow data to flow into AI systems.

When updating security policies for AI, we recommend that key considerations should be:

- Which AI is allowed?
- Who owns the AI?
- Who owns the data?
- What types of data are acceptable?

We discussed the need for better data governance models and personas in the Data chapter. Bringing AI into persona designs alongside robust data classification is now more important, helping define layers of data security control for different uses around the business and in different AI services and platforms. For example, Personally Identifiable Information (PII) must be treated very differently than knowledge bases or general document libraries.



Secure data policy is critical to leveraging AI and defending against related risks.

How mature is your organisation in classifying data based on sensitivity and usage?

Classifying data based on sensitivity and usage



Adapt Security Edge Survey in April 2025. Sample size: 95 Australian CISOs

32% of organisations are immature in data classification for secure data policy

AI governance is becoming a cohort decision amongst the CIO, CISO, and data privacy officers, underpinning the future of security, integration, and wider business governance. Collective leadership must ensure that the drive for higher velocity through AI maintains a focus on the security requirements alongside the business requirements.

Automated code could be attacked with malware injection that gets deployed in your enterprise or custom LLMs could be poisoned in data attacks. This increases the emphasis on maintaining automated scanning and verification to mitigate such a risk.

Leveraging AI for cybersecurity

Using our custom Neuro Cybersecurity Platform, Cognizant is enabling real-time risk mitigation at enterprise-wide scale through an easy to consume user interface. By unifying the security management platform we overcome siloed operations to reduce risk exposure and enhance threat detection and response capability. The platform also helps to classify and protect sensitive data to further enhance confidentiality and data integrity, as well as improve identity and access management to improve confidence in control over critical systems.

Secure by Design in the Agentic AI era

A Secure by Design approach to an enterprise puts accountability across the organisation and not simply upon the security team. This is integrated into our modern engineering frameworks and templates, considering the security requirements at the system design stage across authentication, authorisation, access control, and data control.

Ensuring that default access is only as deep as required is crucial, particularly as more code is written by AI and agentic AI enters our technology environment. Agentic AI requires seamless integration across applications, data, and decision-making systems. This may require new forms of access to applications and data platforms, asking security controls to allow for agentic activity which can potentially look like a security risk.

We must understand at each layer what the agentic AI is going to do and who owns the outcomes. Understanding how agentic AI integrates into different systems becomes part of security controls and frameworks for security by design. And just as shadow IT introduces risks to security, so too will shadow AI as it trends toward agentic AI capabilities that mimic human usage of digital systems.

Conclusion



Bringing the AI empowered enterprise to life

There is no standard solution for technology modernisation. Our experience teaches that identifying the right problems is more critical than finding the right solutions. We know where to begin investigating the status quo for an enterprise and how to measure where constraints lie. We work with organisations to find what works best for their specific needs through smart, targeted experiments in parallel that are anchored to outcomes.

The four factors explored in this guide are interrelated in many ways. We see leading companies driving impactful modernisation through product-oriented mindsets, blending business and technology disciplines and tightly orchestrating both planning and project execution.

CIOs are (self-reporting) their effectiveness

29%

of CIOs feel they are ineffective at building the business case.

ADAPT CIO Edge Survey in Feb 2025

51%

report being ineffective at tracking the value captured from technology spend.

Building the case for a significant investment in technical evolution is not simple. Internal debates can stifle transparent dialogue and enterprise teams don't always have the skills to establish the clarity needed to explain urgency of action. That's why even the biggest enterprises partner with external providers to analyse what's happening and articulate the business case for change.

At Cognizant, we understand reference architectures and can apply highly validated methodologies to investigate your unique scenario and the best ways to redesign and replatform for the future. Our ability to map every business process to existing or proposed tech solutions paves the way for knowing how you can move toward your target architecture.

With Cognizant Neuro AI tools we can work with you to explore business case options in real-time. We can examine almost any business scenario and walk through a decision matrix to consider what is possible and where the best fit lies for your business.

Along with offering external credibility, our strategic support can deliver the data and business case you need without locking you into any ongoing commitments. And we can offer commercial models that are zero risk to your CFO.

To learn how Cognizant can help you on your path to modernisation, email contact_au@cognizant.com



Cognizant (Nasdaq-100: CTSI) engineers modern businesses. We help our clients modernize technology, reimagine processes and transform experiences so they can stay ahead in our fast-changing world. Together, we're improving everyday life. See how at www.cognizant.com or [@cognizant](https://twitter.com/cognizant).

World Headquarters

300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

280 Bishopsgate
London
EC2M 4RB
Phone: +44 207 297 7600

India Operations Headquarters

5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai 600 096
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters

1 Fusionopolis Link, Level 5
NEXUS@One-North, North Tower
Singapore 138542
Phone: +65 6812 4000

© Copyright 2025–2027, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the express written permission of Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.