2025

Turning Hesitation into Action: **How Risk Leaders Can Unlock AI's Potential**

Contents

Carl Solder
Chief Technology Officer
Cisco Australia and New Zealand

Cisco foreword

“Artificial Intelligence (AI) represents the single greatest challenge to businesses and organisations that we have seen in this century.”

Carl Solder

Artificial Intelligence (AI) represents the single greatest challenge to organisations that we have seen in this century. Its potential is immense, but the path to success is neither straightforward nor guaranteed. What's clear is organisations that move quickly to build knowledge and capability will be best placed to reap the rewards of AI. For Australian organisations, that journey must begin now.

It is true that every investment carries risk, and when those risks are difficult to quantify, hesitation is a natural response. This tension and lack of local AI use cases that inspired Cisco’s collaboration with the Governance Institute of Australia. As the leader in cybersecurity, AI and networking, we know that Australia is lagging in its adoption – an anomaly given Australia is typically an early technology adopter. Why is this the case? Together, we have engaged the nation’s risk management community to explore how AI is perceived and understood, the opportunities it promises, and the challenges it presents.

Our goal is to encourage timely, yet responsible approaches to AI adoption – approaches that allow organisations to innovate with confidence while safeguarding against unintended consequences. By doing so, we hope to accelerate AI uptake in ways that are both ambitious and safe.

Daniel Popovski
AI, Cyber and Tech Policy and Advocacy Lead
Governance Institute of Australia

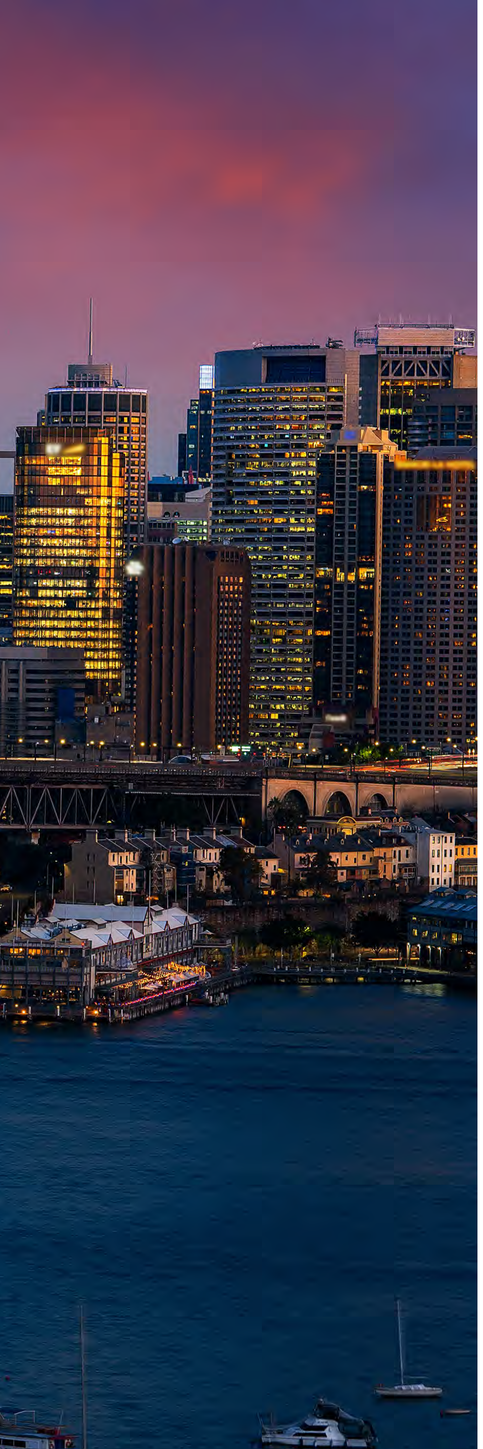
Governance Institute of Australia foreword

As AI permeates into all aspects of our lives, impacting the way we live, work and play, our expectations over its ethical deployment have greatly increased. The Governance Institute of Australia, a professional association for governance and risk management professionals in Australia, conducted research and found that Australians now consider AI to be the second most difficult future development to navigate.[1]

Whilst Australians have embraced technologies quickly in the past, we are observing greater hesitancy with AI, particularly in workplace environments and across boardrooms. For governance and risk professionals, ethically and responsibly deploying this powerful technology can often feel overwhelming.

Change doesn't occur in isolation. It requires us to start critical conversations and map support from board directors, executive teams, staff members, and stakeholders. The conversations illuminated in this paper demonstrate how governance and risk professionals have moved organisations from inaction to action through their own lived experiences.

If you are facing barriers or uncertainties in developing ethical AI deployment pathways across your organisation, I recommend reflecting on the shared experiences throughout this paper.



Part one

Executive summary

The impact of Artificial Intelligence (AI) is often compared to that of the birth of the Internet. Its rapid emergence and breadth of applications suggest it may be even more transformative given the speed at which it's been developed and been universally adopted.

However, those organisations wanting to embrace and adopt AI face numerous barriers. The principal among these are the difficulties of assessing AI's risks versus its rewards.

The enormous potential of AI brings significant risks: security, data management, reputational damage, staff discontent, investment in upskilling, role changes, financial investment, capital risk, and difficulties in scaling from pilot projects to production. These risks mean strong leadership is essential for the effective adoption of AI.

This raises an important question: who in the leadership team is best placed to safely steer AI's adoption?

Australia's risk professionals have previously played a vital role in the digital transformation of businesses and, therefore, are best placed to play a fundamental role in assisting their organisations to capitalise on the benefits of AI while avoiding its pitfalls. They can do this by using their skills in risk assessment, governance, and controls to understand the risk versus reward equation and rebalance it, so that the risks of embracing AI becomes more beneficial than not embracing AI. First, risk professionals must ensure they, and their teams, have the knowledge and skills needed to assess AI's opportunities, understand and control its risks.

This report is the product of a joint initiative between Cisco, a leader in AI and Cybersecurity, and the Governance Institute of Australia (GI), a professional association for governance and risk management professionals in Australia. It is based partly on the synthesis of several quantitative studies, including the **Cisco AI Readiness Index 2024** and **Governance Institute of Australia's 2025 AI Deployment and Governance Survey Report,** as well as extensive discussions with risk professionals conducted under the Chatham House Rule.

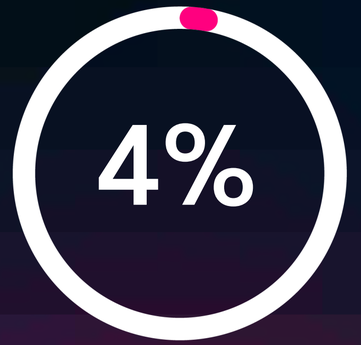
Participants in the roundtable represented senior risk owners from diverse industries, including finance, insurance, education, not-for-profit, and retail. The representatives brought experience from global banks and insurance companies, an international airline, a 'group of eight university', a major international aid agency, one of Australia's largest retail property companies, and some of Australia's most respected charities.

This report has been created to be a springboard for conversations and actions regarding the critical role risk professionals play in assisting organisations to maximise the benefit of AI opportunities.

Part one

“I have spent a lifetime trying to encourage people to take a **risk intelligently.** That is the job of the risk officer.”

Contributed by a participant in the risk owner roundtable



of Australian organisations in 2024 considered themselves fully prepared to deploy and leverage AI technologies.[5]

of Australian businesses in 2025 view themselves as Pacesetters, a sharp improvement from the previous year.[6]

Part one

The AI adoption lag

AI is reshaping how organisations operate – improving efficiency, reducing costs, and creating new services. A 2024 report by Cisco, known as the AI Readiness Index, revealed that only 4% of Australian businesses were fully prepared to deploy and leverage AI technologies. It also revealed that Australia lags in AI adoption compared to other nations. Additionally, the Governance Institute of Australia's recent 2025 AI Deployment and Governance Survey also highlight gaps in investment. Without decisive action to build safe adoption pathways, Australia risks falling further behind global peers.

This important context set the scene for this report, as a catalyst for research and industry roundtables in which risk perception emerged as a key barrier to adoption.

At the time of concluding this report, Cisco's 2025 edition of the AI Readiness index revealed early Australian data showing a sharp improvement in the percentage of Australian organisations ranking themselves as 'Pacesetters', meaning they are fully ready to leverage and deploy AI technologies (shifting from 4% in 2024 to 22% in 2025). This increase highlights how organisations may have progressed their education in what AI could do for them and are now shifting into risk identification to put AI pilots into production.

Still, the risk owners report warns that this rapid acceleration of confidence highlights the importance of ensuring AI's growth is managed securely. Risk professionals must help organisations invest in comprehensive AI strategies and governance structures, not to slow progress, but to ensure foundations can support their ambition and opportunity. Without active risk management during this transition, Australia could lose the ground it has gained.

Several factors have been proposed as to why Australia's uptake of AI lags its peers, including limited education and understanding of AI's potential, training, and capability.

Yet beneath the surface lies a more fundamental challenge: **a pervasive distrust of AI that breeds hesitation in the face of its perceived risks.**

> *"While the benefits of AI can be difficult to quantify, the risks from poorly executed implementations are clear. These include ethical and reputational damage from poor implementations; security and privacy breaches from weak governance; and operational or strategic failures resulting from flawed processes or misjudged investments."*
>
> Contributed by a participant in the risk owner roundtable

Part one

In the absence of clear returns from AI investments, these risks can present a seemingly insurmountable challenge. This is, despite many of the risks arising from AI, similar to those presented by earlier transitional technologies, such as the creation of the Internet. In many instances, the tools and capabilities for AI risk assessment and management already exist, but are simply unknown to risk professionals or not viewed as a tool specific to AI risk assessment.

All of this discussion of AI risk may be masking an even greater issue – the risk that arises from doing nothing, and the possibility that competitive organisations and countries that embrace AI will gain an unassailable advantage.

The role of the risk professional is to understand and manage these risks and to illuminate the best path forward for their organisation. This is why risk professionals are vital to the safe and secure implementation of an AI strategy.

Modern risk professionals already play a vital role in helping organisations find and pursue growth opportunities by contributing to business strategy. They are adept at creating governance structures and applying controls to minimise potential risks.

Risk professionals can bring the strategic vision and tactical rigour needed to help organisations seize AI's opportunities safely. Should they fail to do so, their organisations risk falling behind AI-powered competitors and emerging challengers.

This suggests that many businesses have shrugged off the hesitancy demonstrated in the 2024 Index and embraced the concept that, when it comes to AI, the risk of doing something is less than the risk of doing nothing.

However, this rapid progression also highlights the need for risk professionals to engage deeply with AI strategies and tactics to ensure proper risk assessments and mitigations are not sidelined by the march of progress.

AI adoption in Australian business is no longer a question of if or when. It is now. The key questions are now about safe and effective implementation. The new Index highlights a fivefold increase in 'pacesetters', proving that education works. The next step for Australian businesses is empowering risk owners to guide safe AI pilots. Cisco's findings show that once organisations understand and map risk, they unlock AI's full potential.

"This makes AI a true representation of the age-old test of knowing when the risk of doing something outweighs the risk of doing nothing."

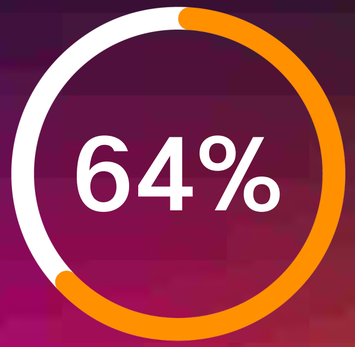
Contributed by a participant in the risk owner roundtable

Part two

“Sometimes the old school mindset puts the hurdle of ‘what’s the return on investment’ in front of a decision. The return is the right to be in business tomorrow.”

Contributed by a participant in the risk owner roundtable

of organisations could not measure return on investment for AI initiatives effectively.[2]



of organisations had yet to offer any AI training programs.[2]

Part two

Risk vs reward: The challenge and opportunity of AI

We know that Australia's risk professionals already play a critical role in helping organisations identify, assess, manage, and monitor risks that impact their objectives, operations, or reputation. These risks can come in many forms. This includes specific risks affecting assets or impacting workers, to broader risks to reputation and economic performance, all the way through to existential risks relating to long-term strategy and planning.

The risk skillset is therefore vital to help protect organisations, their people, and their assets from harm.

Traditionally, this has meant analysing risk factors and applying controls, such as those needed to meet legal and regulatory obligations. However, the rapid rise of AI is stretching this remit and demanding new skills and approaches to address emerging risks that fall outside conventional frameworks.

AI itself is not a new concept, evolving since its initial adoption in corporate IT environments around 30 years ago. Some forms of AI, such as machine learning, are already deeply embedded in processes like image recognition and text-to-speech processing.

Much of today's excitement around AI has been driven by the rapid emergence of generative AI systems, which are capable of mimicking human abilities such as answering complex questions or creating content across different media. Easy to prompt with simple sentences, this wave of generative AI burst into public view in late 2022 with the release of OpenAI's ChatGPT-3.5. Since then, numerous generative AI systems have been launched, and the technology has become increasingly integrated into mainstream business software applications.

Part two

No other technology in recent memory has caught the interest of such a broad spectrum of professional roles and organisational functions. AI stands apart in both the scale of attention it commands and the magnitude of the opportunities it presents.

From a risk perspective, what sets today's generative AI solutions aside from previous generations is that the outcomes are probabilistic and therefore not always consistent. While all AI systems require strong governance relating to the data from which decisions are made (to ensure high levels of data quality and integrity), AI systems based on machine learning systems are deterministic, meaning they almost always generate consistent output from the same input.

The probabilistic nature of generative AI means that outcomes can vary even when the inputs remain the same. Hence, there is a heightened need for decision-making frameworks that consider the ethics, fairness, transparency, and explainability of the outputs of generative AI systems. The tendency for generative AI systems to 'guess' responses in the absence of clear data can also lead to errors, usually referred to as 'hallucinations'.

This is where the risks from current-generation AI systems come into sharp focus, including the criticality of ensuring accountability in AI-driven decision-making.

> ***"It is hard for the risk team to present to the C-suite, and to the board, a clear understanding of the intersection between AI risk and reward, how you can derive a competitive advantage, and link that back to strategy."***
>
> Contributed by participant in the a risk owner roundtable

Part two

Broadly speaking, the risks associated with AI implementations can be categorised follows:

Ethical and reputational risks

One of the key benefits of AI is the ability to automate both mundane and complex tasks that were previously the exclusive domain of human beings. However, numerous instances have been reported in which AI systems produce biased, discriminatory or incorrect outputs. When exposed in the public domain, such outcomes can lead to consequences ranging from an erosion of trust to direct harm to individuals.

Security and privacy risks

For AI systems to work effectively, they must be trained using relevant data. Organisations must therefore be careful to ensure that training data is appropriately sourced, fit for purpose, and used in ways that are commensurate with ethical and legal obligations. Poor data practices can result in the leakage of sensitive corporate information or the violation of people's privacy rights, making it essential that secure training grounds and strong parameters are used to prevent privacy risks.

Operational and strategic risks

AI projects can consume large amounts of capital and have significant environmental impacts, meaning investments must be considered carefully. This is a difficult challenge given the shortage of data on expected returns and a lack of people who are experienced with scoping out AI projects.

Opportunity risk

There is a significant risk of losing competitive advantage against businesses that have explored and optimised AI effectively. From a risk perspective, this means weighing whether the risk of investing in AI outweighs the risk of waiting, and potentially allowing competitors to build a stronger position. Alternatively, failing to invest can mean missing an opportunity to better serve customers, employees, or achieve other benefits. The strong result from the Cisco 2025 AI Readiness Index, which showed that the percentage of Australian businesses that had nominated themselves as 'Pacesetters' had leapt from 4% to 22% in a single year, suggests many organisations are now leaning in favour of the risk of doing something as being the lesser risk.

> *"Staying still means falling behind in the productivity race."*
>
> Contributed by a participant in the risk owner roundtable

Part two

This **opportunity risk** is most evident to risk professionals who see their role encompassing the shaping of their organisation's long-term strategy, and who are prepared to weigh the many factors that will shape future challenges and opportunities.

In some respects, AI-related risks mirror those that risk professionals have managed for decades and may be addressed through established governance frameworks and controls.

In summary, the wheel for assessing AI risks has already been invented. It just needs to be applied in the right way.

However, the ability for risk professionals to appropriately assess the tactical and strategic risks of AI is made more difficult by additional factors.

Speed

The speed at which AI has evolved (and especially generative AI) means few organisations have a strong AI skill set, with the Governance Institute finding that 64% of organisations are yet to offer any AI training programs.[2]

Lack of examples and ROI

Use cases for AI are poorly defined, with limited information available regarding their Return On Investment (ROI). The Governance Institute found that 93% of organisations could not measure return on investment for AI initiatives effectively (2025 AI Deployment and Governance Survey Report)[2]. This lack of proven use cases and clear ROI statements has led organisations to adopt a 'wait and see' stance on AI, in the hope of learning from the successes of others before acting themselves. With AI technologies advancing quickly, fast followers may find it impossible to close the gap on early adopters.

Shadow AI use

Participants spoken to for this report suggest that many employees are already using AI tools, sometimes without official sanction or oversight, in a phenomenon known as 'Shadow AI'. Additionally, participants have professed low awareness of the availability of tools that could control some of these risks.

Security

Many organisations associate AI risk with cybersecurity risk, which has been estimated to cost the Australian economy upwards of $30 billion annually (CyberCX Newsroom). They fear this risk will be amplified by AI.

Complex and unclear regulations

Participants discussed how the regulatory environment regarding AI was poorly articulated, meaning they had to piece together their understanding from multiple pieces of legislation, including the Privacy Act 1988, consumer rights, workplace health and safety laws, directors' responsibilities, and various aspects of sector-specific regulatory regimes. When asked specifically if the organisations participating in this research had created a safe enterprise 'Sandbox' to experiment and trial AI without risk of confidential data leakage, the response was negative, but interest was strong. This is concerning from a security standpoint.

Part two

In short, the benefits of AI are not sufficiently well understood to overcome the associated risks, meaning the funds available for AI projects remain limited. Many pilot programs have reported disappointing results, leading to further negativity regarding the value of AI investments. This, in turn, is reducing the opportunity for AI projects to demonstrate value and restricting opportunities for executives and staff to gain knowledge that could contribute to the success of future projects.

However, it was also the consensus of participants that those organisations that embrace AI quickly – and safely – stand to benefit from a fast-evolving set of technologies with high potential for reducing costs and providing foundations for new service offerings.

This is where risk professionals can play a critical role – by balancing the need to protect long-term interests with preventing harm.

> *"We see it as an opportunity, and we want to realise it as quickly and as deeply as we can."*
>
> Contributed by a participant in the risk owner roundtable

“One of our key objectives is to reduce the likelihood of consequences. But one of our main areas of focus is ensuring we can realise the opportunities that the business wants to realise.”

Contributed by a participant in the risk owner roundtable

Part three

The AI risk relationship

If an organisation considers AI as essential to its long-term success, it must establish governance and controls that allow it to pursue AI benefits safely. Risk and governance professionals are central to this task, providing both strategic guidance and the implementation of controls for assessment, management, and monitoring.

Risk professionals have the opportunity to work alongside the CEO, board, and other strategic leaders to offer both encouragement and oversight to ensure that AI adoption delivers timely and sustainable gains. By partnering with technical specialists and business leads, risk professionals can both increase their own appreciation for AI's capabilities while also ensuring that governance and risk management practices are understood and communicated throughout the organisation.

Ultimately, this should lead to AI being considered within long-term strategic decision-making, in addition to its use in tactical applications with appropriate governance in place. Stakeholders can then align with the AI strategy with a clear understanding of the lines of responsibility, and safely and confidently engage in projects such as pilot programs and sandbox environments to drive learning and practical outcomes.

By extending their engagement into the operational layers of the organisation in this way, risk professionals can ensure that teams understand not only the strategic rationale for adopting AI, but also the expectations and guardrails that define its safe and responsible use.

The expectations of a risk professional in the AI era can be articulated as follows:

1.	Risk professionals must be deeply involved in their organisation's AI strategy
2.	Risk professionals must play an active role in developing appropriate AI governance structures and controls
3.	Risk professionals must play a role in communicating the AI strategy

Part three

“Ten years ago, everyone had a digital strategy, and many still do, but digital is the business in many ways, and AI presents almost the same challenge in needing to be an integrated part of the business strategy.”

Contributed by a participant in the risk owner roundtable

The expectations of a risk professional in the AI era can be articulated as follows:

1. Risk professionals must be deeply involved in their organisation’s AI strategy

The organisations that view AI as vital to their long-term success will also view it as a fundamental pillar of their business strategy. For many, there will be no distinction between their AI strategy and their business strategy (as has happened with digital strategies). For risk professionals, this requires them to become educated in the broader capabilities and applications of AI as it impacts the business. It also requires them to be contributors to organisational strategy, alongside the CEO and other strategy stakeholders. This is especially true in light of the findings of the 2025 AI Readiness Index, which showed a sharp improvement in the percentage of organisations that are embracing AI. This is a sudden change that demands commensurate risk oversight.

Achieving this outcome might require the risk professional to forge stronger ties with AI technology specialists within their organisation or its service providers, to help bridge knowledge gaps and ensure that AI opportunities can be mapped to appropriate controls. This could lead to the creation of an AI risk and governance steering committee, made up of members of the risk and technology functions, and augmented by business leaders whose functions are the initial or most significant recipients of AI capabilities: from IT, HR, finance, operations, as an example. Through this process risk professionals may find themselves becoming the translators between technical capability and business strategy.

Part three

2. Risk professionals must play an active role in developing appropriate AI governance structures and controls

Just as risk professionals today play a vital role in setting tolerances and guardrails for risks related to financial transactions or occupational health and safety, the adoption of AI will require a similar understanding of potential risks and how they can be monitored and mitigated.

Implementation of these guardrails must happen early in the development of an AI strategy, so they can be used to minimise potential harms that might arise during the 'learning phase' of AI adoption, and stimulate the adoption of behaviours that will be essential to the development of a safe AI culture.

Voluntary safety standards, frameworks, and guardrails can guide risk professionals, such as those set out in the ISO 420001 International Standard for Artificial Intelligence Management Systems, or the NIST AI Risk Management Framework, developed by the U.S. National Institute of Standards and Technology[4].

> ***"It is not just a matter of tech and risk; it is a whole organisation effort that is required to adequately understand it."***
>
> Contributed by a participant in the risk owner roundtable

3. Risk professionals must play a role in communicating the AI strategy

If AI is to be a fundamental part of the business strategy, then all stakeholders should be educated in its use, its impact on the organisation, and the expectations placed upon stakeholders regarding its use. Raising awareness in this way might also serve to prevent the emergence of 'Shadow AI', which arises when employees implement their own AI tools in the absence of a defined AI strategy, and/or when the potential risks of such behaviour have not been articulated and controlled.

The need to raise awareness regarding AI strategy and implementation might also see the risk function working closely with the people & culture function and internal communications. This will ensure that appropriate training is provided to staff so they can utilise AI tools productively and safely, and create appropriate cultural settings and messages that balance any appetite for experimentation with an understanding of potential risks, such as risks when working with personal information.

This could be facilitated through the creation of AI hackathons, which demonstrate AI capabilities, and the development of 'Sandbox' environments for safe experimentation with AI tools. Raising awareness in this way might also prove critical to managing workers' expectations and anxieties regarding the impact that AI could have on specific tasks and job functions.

Part three

“Everyone plays a part in this – it absolutely is a whole-of-organisation thing.”

Contributed by a participant in the risk owner roundtable

Part four

Recommendations

The challenge and opportunity of AI is significant, and for those risk professionals who are in the early stages of learning about AI, the scope of possible actions can seem overwhelming.

The following recommendations provide starting points to help accelerate learning and AI adoption, whatever the size of the business.

Suggested actions for risk professionals:

1. Build knowledge
2. Create an interdisciplinary AI governance committee
3. Embed AI with the organisation's strategy
4. Invest in appropriate controls
5. Raise AI awareness across the workforce
6. Measure AI project results

Suggested actions for risk professionals:

1. Build knowledge

AI's origin within the technology function has meant its core concepts and capabilities are rarely taught outside of technology streams, meaning it represents a significant 'unknown' for risk professionals.

The various kinds of AI available to businesses today (such as machine learning and generative AI) come with different risks, while implementation strategies can range from developing native capabilities (such as through training of organisation-specific generative AI agents) to adopting prepackaged AI applications and services within Software-as-a-Service platforms.

Appreciating the fundamentals of how different forms of AI work, and the risks they carry, represents a solid starting point for knowledge building. This knowledge gap must be bridged quickly to ensure risk professionals can both appreciate the capabilities of AI and map appropriate controls to its risks.

This learning process can be accelerated by having risk professionals forge close ties with their organisation's CIO or CTO, or with external service providers. This requirement should be embraced by all participants in strategic planning and risk activities, and ideally, by all business function leaders who are likely to be impacted by AI implementations.

2. Create an interdisciplinary AI governance committee

This should consist of a mixture of risk professionals, technology professionals, and business leaders working together to develop and implement appropriate governance principles and controls.

Having a separate AI-focused committee will ensure appropriate focus is given to this topic in its early stages, with potential for this activity to be folded into broader governance structures once confidence is achieved. It will also be important to ensure cross-functional teams speak the same language regarding AI, and conduct an audit to determine where AI has already been adopted within the organisation.

3. Embed AI with the organisation's business strategy

The fundamental nature of AI as an enabling capability, and its potential to influence almost all aspects of operations, means the concept of an AI strategy may become indistinguishable from the overall strategy of the organisation that it supports.

While the initial AI capability development phase may require special focus, this should occur in close alignment with the overall organisational strategy to reduce the chances of 'strategic drift' and ensure that AI investments are aligned to defined outcomes.

4. Invest in appropriate controls

Following on from the creation of the AI Governance Committee, organisations must invest in appropriate controls to ensure their governance structures can be implemented and monitored at a tactical level. These controls will include policies and procedures, but might also involve the implementation of tools for permissions and monitoring, while also managing risk factors such as data loss or the unvetted release of AI apps and agents into the public realm. Risk professionals play a critical role in the development and implementation of these controls, drawing on their experience from other risk domains.

5. Raise AI awareness across the workforce

Risk professionals should work closely with people & culture and communications functions to ensure that staff understand the ‘why, what and how’ of the AI strategy. AI’s potential to affect all workers means it is essential that they understand and align with the organisation’s AI strategy.

Failure to engage transparently raises the prospect of workers rejecting the introduction of AI due to the fear of negative consequences for their employment. Engagement starts with clear communication of the overall approach and of specific areas of impact as they are identified. Such transparency helps manage uncertainty regarding how AI will affect individual roles, protecting morale during a period of significant change.

Raising awareness of AI’s capabilities also empowers employees to identify opportunities where AI can support their tasks, enabling them to suggest implementations that improve both their own working life and overall organisational productivity. Finally, clear communication of AI strategies and expectations reduces the risk of unsanctioned or unsafe adoption (Shadow AI) by guiding employees toward approved, well-governed tools and uses.

6. Measure AI project results

Many reports describe high failure rates for AI projects, including frequent difficulties with growing projects beyond pilot programs (Harvard Business Review, Beware the AI Experimentation Trap). The experimental nature of many AI implementations contributes to these failure rates, making it critical for organisations to capture lessons learned and feed them back into future projects and measures of strategic success.

It is also important to define appropriate metrics for how success in AI projects is measured. These metrics should be measured over both the short and long term to ensure that the benefits of AI are sustainable. This also helps to ensure that people can see the success of AI projects and their benefits. Knowledge capture ensures that initiatives remain within risk guidelines while also delivering tangible results.

Part five

Conclusion

This project saw discussions conducted with risk professionals from organisations of all sizes and from many sectors, providing a candid insight into the challenges currently facing boardrooms nationwide.

Themes of education, accountability, fear of failure, lack of AI pilots or the use of secure sandboxes, and a cautious ‘watch and learn’ approach all demonstrated a need for a mindset change in the boardroom – one that accepts the criticality of bringing an enthusiastic and intelligent approach to understanding and managing AI risk. Only when the risks of AI are understood in this way will the dam break, and allow Australian businesses to embrace the productivity benefits of AI safely and securely.

AI offers capabilities that will touch almost all aspects of an organisation. This, coupled with the accessibility and utility of the current generation of generative AI tools, means AI has captured the public’s imagination much faster than previous innovations, even including the world wide web or mobile smartphones. Each new era of technology creates winners and losers, and it is those organisations that understand the possibilities early that are in the best position to experience them.

In a corporate setting, AI presents significant opportunities for streamlining existing services and creating entirely new ones. As such, its importance from a competitive perspective cannot be overstated.

However, the emergence of AI, along with the hype that has surrounded it, has also created significant uncertainty as to how extensive its benefits might be and how they can be achieved. AI has also presented a new set of risks for organisations, in the form of, but not limited to, potential privacy breaches or reputational damage from poorly implemented AI services.

For these reasons, AI has stamped itself as a matter worthy of the engagement of risk professionals. It has also shown risk professionals that the role of risk is absolutely critical to its safe and secure adoption.

We hope through this project that we have spurred conversations, not only about why AI is such a critical area of study for risk professionals, but also about why those professionals play a critical role in ensuring that organisations can progress forward and maximise the opportunities from AI while minimising risks.

The future cannot be predicted, but AI ensures it will be unlike the past. Those organisations that thrive will be the ones that recognise their opportunities and navigate their risks.

This is a task at which Australia’s risk professionals excel, making that function one of the most critical components in any organisation’s AI adoption strategy.

Appendix

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that is revolutionising the way organisations connect and protect in the AI era. For more than 40 years, Cisco has securely connected the world. With its industry-leading AI-powered solutions and services, Cisco enables its customers, partners and communities to unlock innovation, enhance productivity and strengthen digital resilience. With purpose at its core, Cisco remains committed to creating a more connected and inclusive future for all.

About Governance Institute of Australia

Governance Institute of Australia is the only fully independent professional association dedicated to the advancement of governance and risk practice in Australia. Our internationally recognised qualifications equip a diverse professional network of business leaders to make good decisions for the benefit of Australia's economy and society. With a history dating over 100 years, Governance Institute is Australia's leading and trusted voice of governance.

Brad Howarth
Author and Researcher

Brad is a researcher, writer, trainer, speaker, and facilitator with more than 30 years' experience investigating and interpreting technology-driven change.

His career began as an enterprise technology journalist working with various Australian industry titles and national publications, including Business Review Weekly, The Australian, and Australian Financial Review BOSS Magazine. His coverage has included broader topics such as the evolution of technology and how digitalisation has impacted job functions and entire industries. Brad has authored four books, the latest of which, Innovation is for Everyone (co-authored with Peter Fritz AM), investigates Australia's innovation track record and future opportunities.

Brad's deep knowledge and storytelling skills have led him to be a sought-after keynote presenter at major events. He regularly performs the role of event host and facilitator for meetings and workshops, including the management and delivery of advisory board sessions.

Carl Solder
Chief Technology Officer
Cisco Australia and New Zealand

Carl Solder currently serves as the Chief Technology Officer for Australia & New Zealand (ANZ).

Prior to this role, Carl was Cisco's Vice President of Engineering for the Enterprise Networking and Cloud Engineering organisation at Cisco HQ in San Jose, California. In this role, he was responsible for Technical Strategy for the Enterprise Network and Cloud portfolio. His portfolio included the Catalyst Routing, Switching and Wireless platforms, the Intent Based Networking Software Innovations around Automation, Assurance, Machine Learning and Artificial Intelligence as well as the Policy, Identity and Segmentation Software solutions that include Cisco's Identity Services Engine (ISE).

Through his time at Cisco, Carl has also held various Engineering leadership roles in Cisco HQ San Jose and served as a Distinguished Engineer working on early developments in the area of Mass Scale Data Centre Architectures, OpenFlow and Software Defined Networking.

With more than 35 years of technical, business and sales leadership experience in the ICT industry, Carl has a diverse ICT background that provides great insight into emerging market transitions.

David Siroky
Head of AI
Cisco Australia and New Zealand

David brings the latest insights from leading edge AI deployments across the region, along with learnings from Cisco's internal AI usage which spans over 1000 GPUs and multiple cloud providers - to clients to help align solutions with business strategy, and unlock the full potential of AI.

Previously – David built and lead the Dell APJ team focused on Generative AI, HPC and Data Analytics. His team designed some of the largest AI systems in the APJ region, ran organisation-wide AI transformation and upskilling programs.

At Microsoft, David was Director of product management & marketing at Microsoft – leading multiple product cycles from engineering spec to market introduction. David has a background in computer science, market research, analyst relations, economics, and public relations.

Daniel Popovski
AI, Cyber & Technology Policy, & Advocacy Lead
Governance Institute of Australia

Daniel is the AI and tech policy and advocacy lead at Governance Institute of Australia, where he develops research publications, policy positions, and advocacy activities to support the Australian governance community to ethically and responsibly deploy AI in the workplace. He is a member of the Standards Australia AI technical standards committee and leads the Australian delegate to the UNESCO Global AI alliance.

Daniel has a decade of policy and advocacy experience, having held leadership roles across a diverse range of government departments and national industry bodies. Daniel began his career as an economic advisor to Australia's largest and most representative business group, the Australian Chamber of Commerce and Industry and has held affiliated roles with the OECD Business and Industry Advisory body and International Chamber of Commerce. Daniel is a recipient of an Australia Day medallion for excellence in policy design and program delivery whilst working at the Department of Industry, Innovation and Science.

Daniel holds a Juris Doctor from the University of NSW, Bachelor of Economics with Honours (UTS), and a Bachelor of Arts and Bachelor of Commerce (UOW). He graduated from the ANU New Technologies Law program and was awarded the Norton Rose Fullbright Prize for first place in cyber law.

Daniel's expertise stems from deep knowledge across best practice AI, cyber, tech governance, risk, and compliance management practices. He is an advocate for the design, development and deployment of ethical and human-centric digital technologies to support healthier, more productive workplaces and improved environmental, social, and economic outcomes.

Citations

[1] 10th Ethics Index, Governance Institute of Australia

[2] 2025 AI Deployment and Governance Survey Report

[3] CyberCX Newsroom

[4] NIST AI Risk Management Framework

[5] Cisco's AI Readiness Index 2024

[6] Cisco's AI Readiness Index 2025


CISCO
Governance
Institute
of Australia