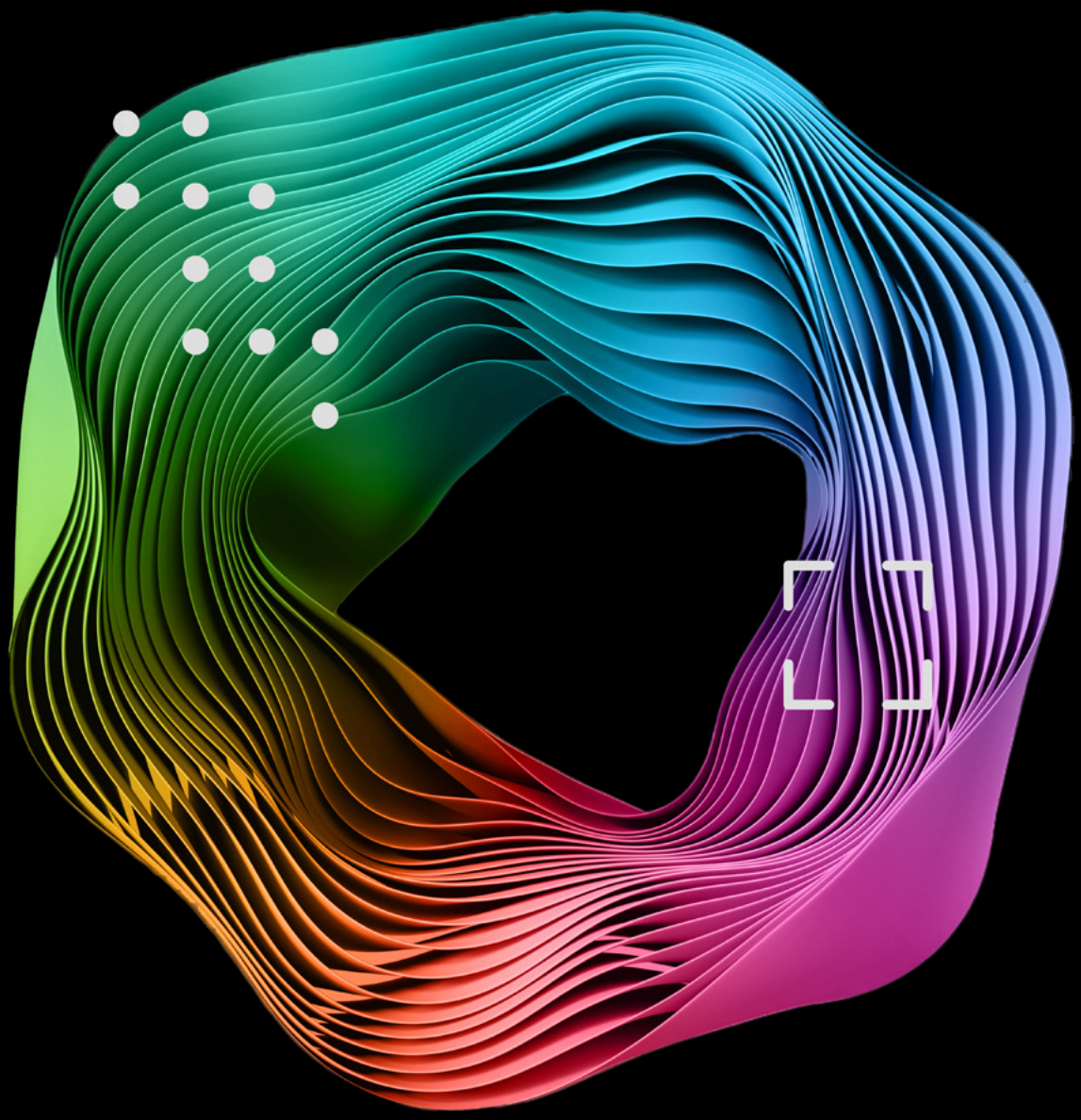
Deloitte.



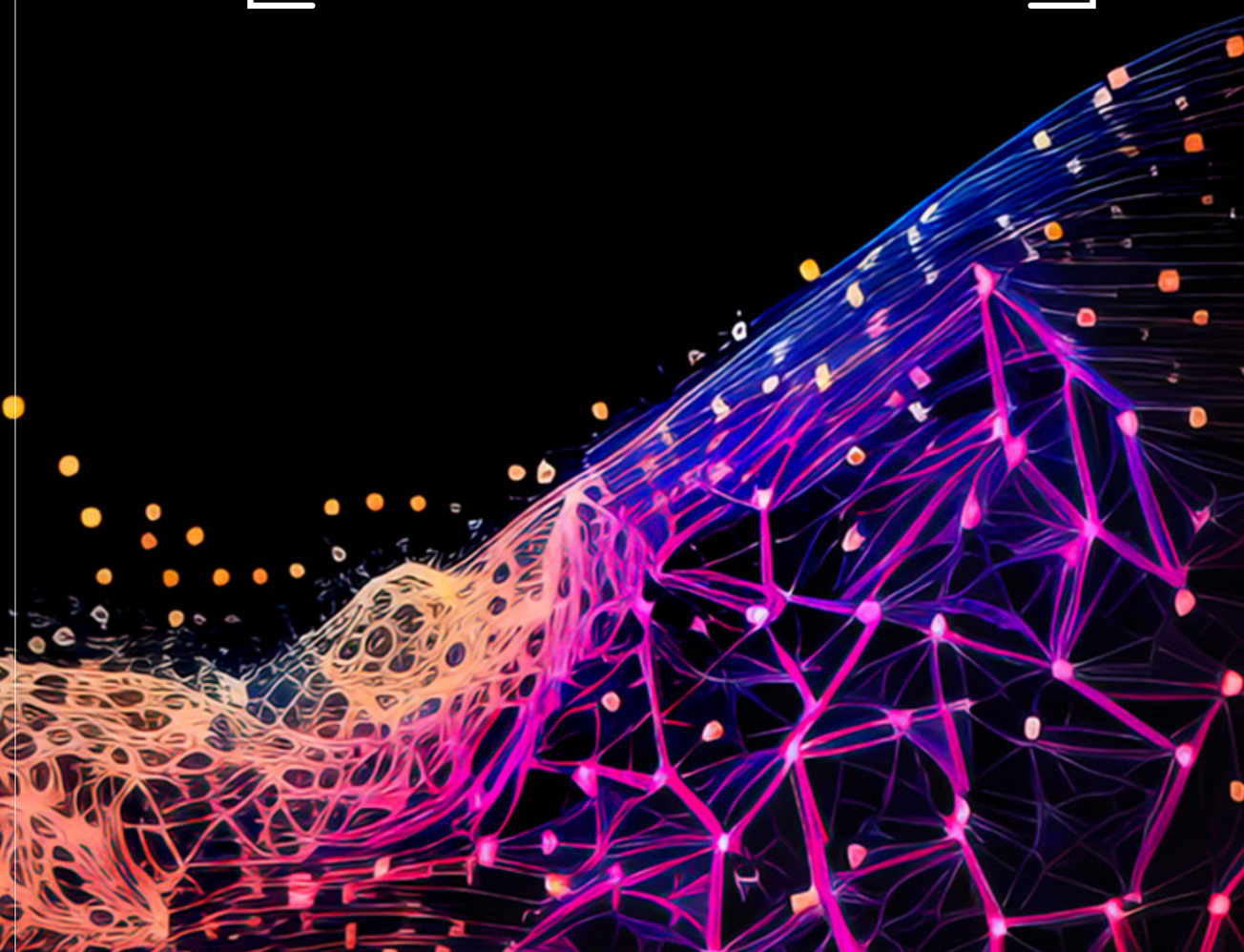
Deloitte
Access Economics

AI at a crossroads

Building trust as the path to scale

Deloitte Asia Pacific | AI Institute

Contents



Report overview

This report was co-developed by Deloitte Access Economics and the Deloitte AI Institute to provide insights to Asia Pacific C-suite executives and tech leaders, on how they can improve their governance structures and organisation settings to develop more trustworthy AI solutions.

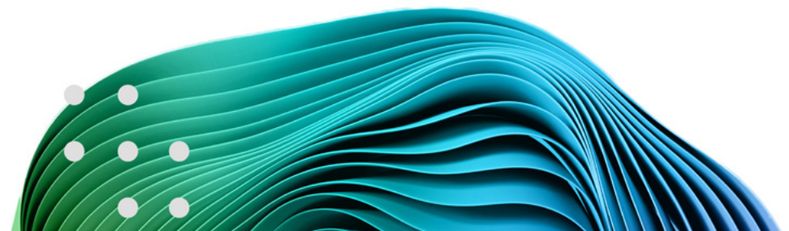
Deloitte has created a Trustworthy AI Framework that identifies seven dimensions necessary for organisations to have trust in their AI solutions – transparent and explainable, fair and impartial, robust and reliable, respectful of privacy, safe and secure, responsible and accountable.

But what needs to be in place for organisations to achieve trustworthy AI? Good AI governance.

For C-suite executives and board members, activating and supporting effective AI governance practices can be challenging amidst competing priorities. To help address this ambiguity, we've developed an AI Governance Maturity Index to identify what good AI governance looks like in practice. This index contains a set of criteria to assess AI governance within an organisation and was applied to the responses of nearly 900 surveyed senior leaders from Australia, China, India, Indonesia, Japan, Malaysia, New Zealand, Philippines, Singapore, South Korea, Taiwan (China), Thailand, and Vietnam.
A range of industries, organisation sizes and public sector organisations were included in the responses.

The survey questions aimed to understand the maturity level of AI governance across organisations, identify key enablers of effective AI governance and assess the benefits to organisations from having these arrangements in place.

1. TRANSPARENT AND EXPLAINABLE
2. FAIR AND IMPARTIAL
3. ROBUST AND RELIABLE
4. RESPECTFUL OF PRIVACY
5. SAFE AND SECURE
6. RESPONSIBLE
7. ACCOUNTABLE



AI at a crossroads:
Building trust as the path to scale

As senior leaders move from experimenting to rolling out AI solutions, a number of key risks – such as security vulnerabilities, privacy and legal risk – are experienced by the organisation. While AI solutions offer powerful productivity tools, they can lead to data breaches, loss of reputation and business and regulatory fines if the risks of these tools are not managed properly.

Concerningly, more than half of technology workers do not believe their workplace can address AI related risks. To understand how effective AI governance can help to address these risks and unlock the potential of AI, Deloitte has surveyed nearly 900 senior leaders from 13 locations across the Asia Pacific region in one of the most comprehensive stocktakes of AI governance maturity levels to date.

There is a rising number of incidents from using AI across all industries

Over a quarter of organisations have experienced an increase of incidents related to AI in the past financial year.

Increase in incidents recorded in the past financial year, by industry

Good governance also leads to greater AI adoption and financial returns

28% more staff using AI solutions across the business

3x more likely to be using AI solutions in areas such as R&D, operations and production, and customer service, marketing and sales

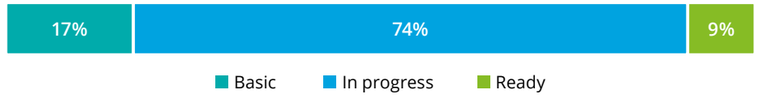
4.6 percentage points higher in **revenue growth** from AI solutions

45% of senior leaders believe good governance **improves reputation** among customers

Yet more than 90% of organisations can improve AI governance

Deloitte's Governance Maturity Index uses 12 indicators to assess AI governance across organisations.

Distribution of AI Trustworthy Index across Asia Pacific



Actions to build Trustworthy AI

1. Prioritise AI governance to realise the returns from AI
2. Understand and leverage the broader AI supply chain
3. Build risk managers, not risk avoiders
4. Communicate and ensure AI transformation readiness

01

Navigating the risks from rapid AI adoption

The adoption of AI across the Asia Pacific region is transforming the business landscape. The rapid emergence of generative AI (GenAI) has only accelerated this process, with investment in AI across the Asia Pacific region expected to grow fivefold by the end of the decade, reaching $117 billion USD by 2030.[1] GenAI has quickly become the region's fastest-growing enterprise technology.

Behind the rapid pace of adoption are employees, who often outpace their leaders. A previous Deloitte study on Generation AI found that more than two in five employees were already using generative AI at work, with young employees leading the way.[2]

This pace and scale of AI adoption means leaders are encountering AI related risks in real time as they experiment and roll out the technology. Our survey of nearly 900 senior leaders reveals that risks related to security vulnerability (86%), surveillance (83%) and privacy (83%) are the most common concerns for senior leaders when using AI (Figure 1). These risks have become even more pronounced since the advent of GenAI, which has seen a step change in the capabilities of the technology alongside more user-friendly interfaces that have broadened the number of people who can use these powerful tools.

> "Over half of technology workers believe their workplace does not have the appropriate settings to identify or address AI-related risks according to a Deloitte study."[3]

Security vulnerabilities can arise from AI solutions or the vast amount of data used by the solutions, which can become targets for theft or data breaches, and can result in significant costs. The global average cost of a data breach reached nearly $5 million USD in 2024, a 10% increase from the previous year.[4] Of course, for large organisations, this cost can be significantly higher.

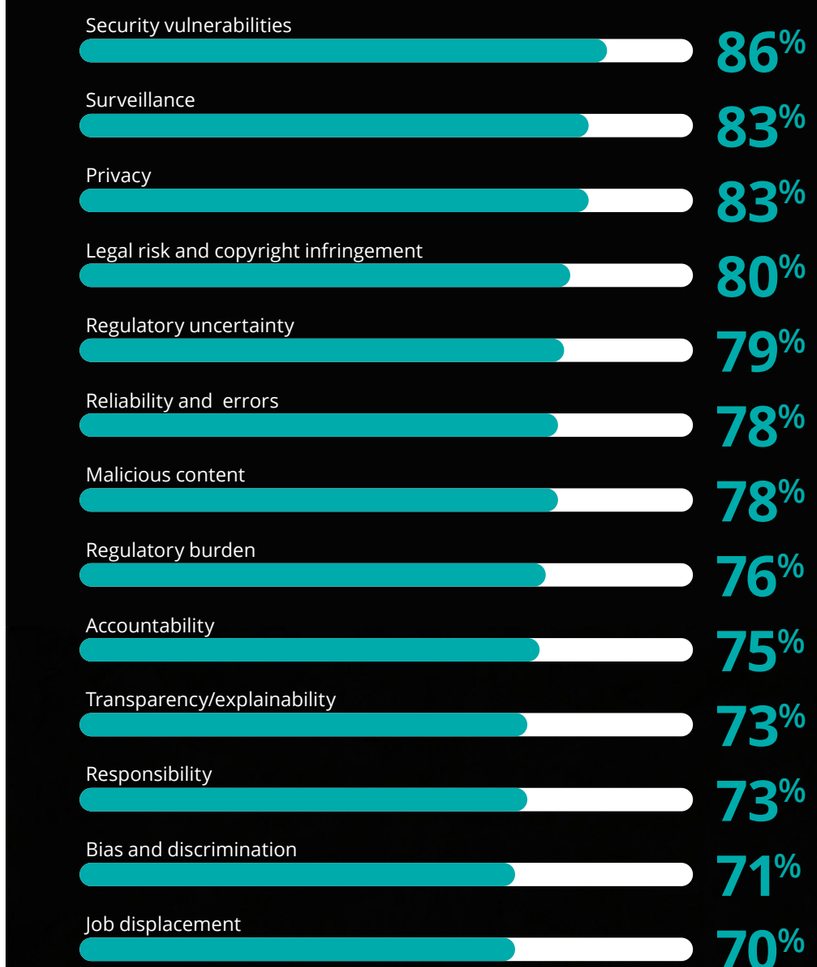
There are also broader costs that are difficult to quantify, such as damage to brand and loss of customers. The erosion of consumer confidence and the negative impact on brand reputation can have long-lasting effects, making it crucial for businesses to manage AI and cybersecurity effectively. At the same time, there is a strong consumer preference for businesses that use AI in a way that aligns with their ethical standards, such as transparency when AI is used. Research indicates that 62% of consumers place higher trust in companies whose AI interactions they perceive as ethical, and 53% are willing to pay a premium for such products and services.[5]

Organisations must also ensure that their use of AI is compliant with evolving legislative and regulatory requirements, which was a shared theme among the most common risks identified by senior leaders. While there has been a focus on developing and enacting regulations and legislation across Asia Pacific governments, these existing regulatory requirements are usually a minimum standard for organisations to meet rather than comprehensive best practices. As a result, senior leaders must develop, adopt and enforce organisational trustworthiness standards for AI solutions and systems.[6]

Addressing AI-related risks is essential: without proper management, these risks could lead to strained customer relationships, regulatory penalties or public backlash. Furthermore, fear of these risks can also deter organisations from using AI. The *State of AI Enterprise* survey found that three out of the four biggest challenges to developing and using AI tools are risk, regulation and governance issues.[7] This highlights the importance of effective AI governance for managing the ethical and operational risks associated with AI and fully leveraging this technology.

Figure 1

Top concerns about potential risks associated with using AI



Source: Deloitte Trustworthy AI survey (2024)

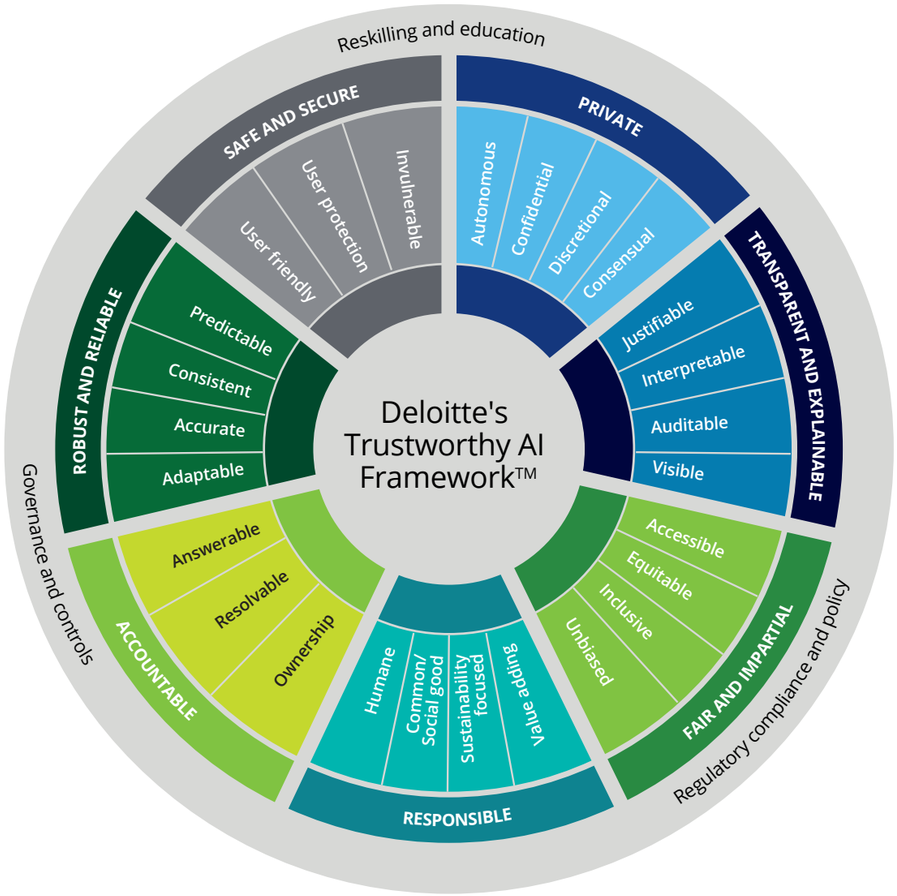
02

What does good AI governance look like?

Developing trustworthy AI solutions is essential for senior leaders to successfully navigate the risks of rapid AI adoption and fully embrace and integrate this transformative technology. Trustworthy AI provides a level of certainty that the technology is ethical, lawful and technically robust and provides confidence for senior leaders to use AI solutions throughout their organisation.

Deloitte has developed a Trustworthy AI Framework that outlines seven key dimensions that are necessary to build trust in AI solutions – 1) transparent and explainable, 2) fair and impartial, 3) robust and reliable, 4) respectful of privacy, 5) safe and secure, 6) responsible, and 7) accountable (Figure 2). This framework and criteria should be applied to AI solutions from ideation through to design, development, procurement and deployment.

Figure 2: Deloitte Trustworthy AI framework



Source: Deloitte (2024)

Developing trustworthy AI solutions that meet these seven criteria does not happen automatically. Organisations must have robust AI governance to provide the structure that ensures AI solutions align with these principles.

At its core, good AI governance is required at all stages of the technology lifecycle and is embedded across technology, processes, and employee training. Governance arrangements require tailoring to the sophistication of AI solutions used, location and industry-specific regulations, and internal organisational policy and standards.

AI governance can often feel elusive with constantly shifting goalposts. To assist organisations to take practical steps to achieving trustworthy AI, we have created an AI Governance Maturity Index.

This Index, based on 12 key indicators across five pillars (organisational structure, policy and principles, procedures and controls, people and skills and monitoring, reporting and evaluation), assesses an organisation's AI governance maturity (Table 1). Based on these indicators, we categorise organisations as 'Basic', 'In progress' or 'Ready' in terms of their AI governance maturity. Further details about the Index and the underlying questions are available in Appendix B.

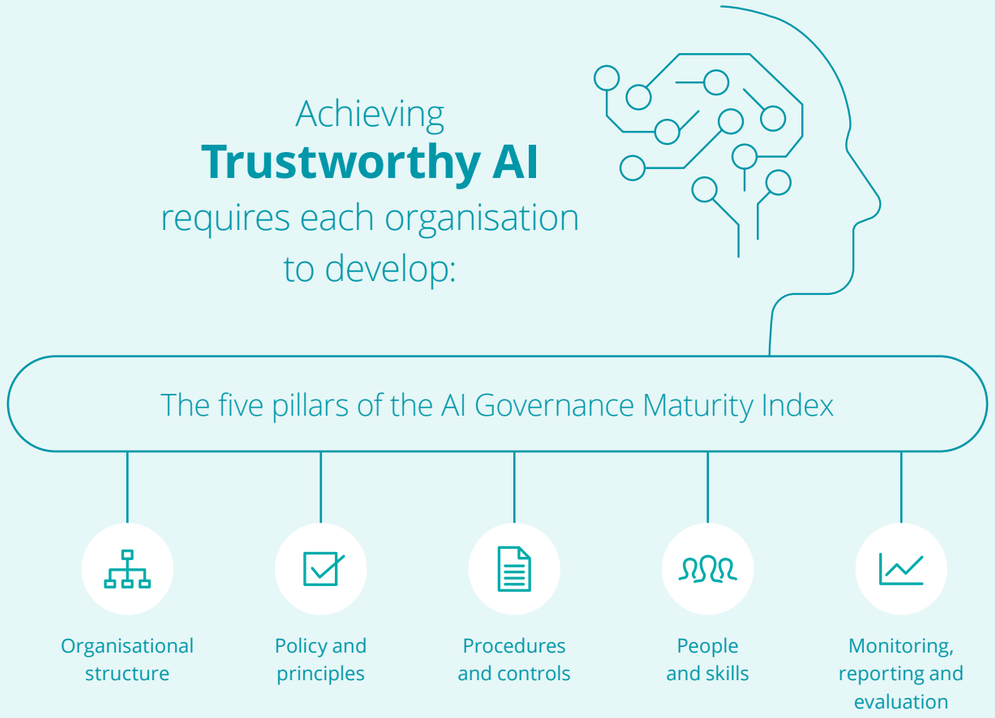
Table 1: Deloitte AI Governance Maturity Index

Pillars	BASIC	IN PROGRESS	READY
Organisational structure	Lack of roles and responsibility assigned for AI governance.	Identified some roles and responsibilities for individuals and groups for AI governance.	Board accountability defined, with roles and responsibilities assigned to management to support organisation wide AI governance.
Policy and principles	No AI policy in place or principles to guide AI governance.	Basic or draft policy in place with generic principles to guide AI governance.	Robust policy, grounded in by well-defined principles tailored to organisation's unique context.
Procedures and controls	No risk procedures or controls for development, deployment or use of AI systems.	Risk procedures and/or controls under development for development, deployment or use of AI systems.	Existing system of risk procedures and/or controls sufficient to guide development, deployment or use of AI systems.
People and skills	No resources or training for staff to support use of AI responsibly.	Resources currently being developed for employees to use AI responsibly.	Resources, including guidelines for use and training, are available to employees to use AI responsibly.
Monitoring, reporting and evaluation	No mechanism for monitoring or reporting on AI systems in operation.	Mechanism and tools for monitoring or reporting on AI systems in operation under development.	Existing mechanism and tools for monitoring or reporting on AI systems in operation.

Source: Deloitte (2024)

The figure below depicts how each of the pillars in the Deloitte AI Governance Maturity Index is a foundational element that can enable an organisation to achieve trustworthy AI. Furthermore, the Index identifies the practical arrangements and activities that an organisation should undertake to achieve the seven dimensions highlighted in the Trustworthy AI Framework.

Figure 3: Deloitte AI Governance Maturity Index and the Deloitte AI Governance Maturity Index



Source: Deloitte (2024)

There is no one-size-fits-all approach to AI governance. The specific governance structures will vary depending on the industry, regulatory environment, AI ambition and type of AI solutions being adopted. For instance, an AI-powered chatbot providing employees with information about HR policies will require different control processes compared to a bank's AI-driven credit application solution that interfaces directly with customers. Comparing common features of AI governance can help organisations identify areas for improvement in their governance standards.

It should also be noted that higher levels of AI Governance Maturity do not automatically lead to trustworthy AI outcomes. If governance procedures are in place but are not effectively implemented, understood by staff or well-tailored to the business context and strategy, trustworthy AI outcomes may not be achieved. Effective AI governance is different for every organisation. For this reason, it is important for organisations to continuously evaluate and refine their AI governance framework to ensure that it is right-sized to their unique needs and evolving regulatory requirements.

CASE STUDY

Empowering the future: **Energy Queensland's commitment to responsible AI and sustainable innovation**

Energy Queensland is Australia's largest, wholly government-owned electricity company, servicing over 2.3 million customers and employing more than 9,300 people across its distribution, retail, and integrated energy solutions businesses.

Sharyn Scriven, CIO Energy Queensland expresses that **"AI is a game changer and as it matures will help aid our business and people to achieve our vision and 2032 Corporate Strategy."**

Josh Gow, General Manager of Customer and Emerging Platforms, recognises that integrating AI is an important focus area for Energy Queensland to drive operational excellence and enhance customer experience, supporting the organisation's ambitious strategy. While Energy Queensland has been using AI for several years, there has been a shift from niche specialised use cases to broader use case evaluation and deployment.

Drafting an AI policy has been essential for Energy Queensland to ensure the right policies and settings are in place before introducing new AI solutions. This has involved developing an AI Policy and a roadmap for use case rollout across the organisation, along with necessary actions to establish appropriate guardrails. To ensure the AI policy adhered to industry best practices and was implemented correctly, Energy Queensland had the AI policy independently reviewed by an external organisation, as well as internally. Josh explains:

"Our AI policy is under continued review, as a living, breathing document, given the rapidly changing environment of AI and maturing industry standards and guidelines. Our monthly AI steering committee includes senior executives who regularly discuss the progress, risks and opportunities of AI."

Testing and piloting AI use cases before full implementation is an important feature of Energy Queensland's approach to AI. Trialling AI through internal use cases has been a strategic choice to create an environment where it has been 'test and learn focused to further evaluate risk and opportunity incrementally', according to Josh. This has involved trialling enterprise tools and building AI platform services to initially support corporate users with heavy documentation, meetings and emails.

Effective and responsible use of AI requires team members with the right capabilities alongside powerful AI solutions. For this reason, 'control group releases' are being conducted and reviewed, where employees in different roles participate in a controlled release, education and training program before further deployment.

"Ensuring we capture the value, opportunity and continue to manage the risk that AI will bring with further adoption is critical. It's a matter of when, not if, AI will be in broader use across many more technologies. Not everyone will get the same AI and it may also be 'under the hood'. We need to tailor how AI will aid our company to ensure it is effective, responsible, and valuable."

Key features to ensure trustworthy AI

- **AI policy**
- **AI steering committee**
- **Piloting and trialling AI programs internally**
- **Training programs**

03

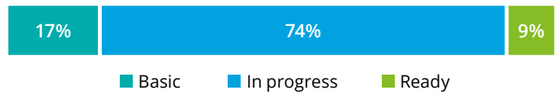
AI governance across Asia Pacific

Fewer than one in ten organisations across the Asia Pacific have the governance structures necessary to achieve trustworthy AI. Using our AI Governance Maturity Index, we classify 91% of organisations as having 'Basic' or 'In progress' AI Governance structures in place, highlighting substantial room for improvement in AI governance (Chart 1).

Examining the five pillars of the AI Governance Maturity Index, organisations across Asia Pacific have the greatest opportunity for improvement in policies and principles as well as procedures and controls. Currently, 31% and 23% of organisations, respectively, are categorised at 'Basic' levels in these two pillars. In contrast, organisations performed better in the organisational structure and monitoring and evaluation pillars, with more than 90% achieving at least 'In Progress' status.

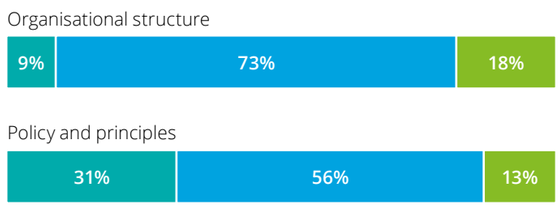
Achieving a 'Ready' status for the AI Governance Maturity Index overall requires high performance across all five pillars. While nearly one in five organisations achieved a 'Ready' status in one of the pillars, only half that shared achieved 'Ready' for their AI governance overall. This highlights the need to consider AI governance in a holistic sense to develop the conditions required for trustworthy AI.

Chart 1: Distribution of AI Trustworthy Index across Asia Pacific



Source: Deloitte Trustworthy AI survey (2024)

Chart 2: Distribution of Trustworthy AI Index across pillars



Source: Deloitte Trustworthy AI survey (2024)

Addressing the overconfidence bias

Leaders may overestimate the maturity of AI Governance. Deloitte's *State of Generative AI in the Enterprise* survey found that 23% of organisational leaders rated their risk management procedures and governance as highly prepared. However, this more detailed study, exploring the underlying structure of AI governance revealed only 9% had actually achieved a 'Ready' level of governance.[8] While the specific questions and sample differ, the extent of the variation in these studies suggests that senior leaders need to have a detailed understanding of their AI governance maturity. This is pertinent as overconfidence can represent a barrier to improving AI governance; if leaders believe they have sufficient settings in place to manage AI risks, they are less likely to explore how they can improve.

PILLAR 1

Organisational structure

Having clearly identified roles within an organisation that are accountable for managing AI standards helps to ensure any emerging AI-related issues are addressed appropriately. For most organisations surveyed, this responsibility lies with senior leadership, with 91% of organisations having a board member or C-suite executive explicitly responsible. A further 7% nominated a non-executive AI lead as responsible for managing risks and standards, while less than 2% of respondents were not able to identify anyone primarily responsible in their organisation.

How organisations structure the teams responsible for ethical, legal and regulatory compliance related to AI may vary. Just over a quarter (28%) of organisations have a centralised ethics and risk team to monitor trends and detect risks related to AI use, while the majority (61%) of organisations have dedicated professionals working in all or some departments or teams (Chart 3). The remaining organisations have either some teams with dedicated professionals or no dedicated roles for AI use.

More important than the structure of the team is having clear responsibility and accountability for AI standards, yet this is less common in smaller organisations. For organisations with more than 1,000 employees, only 3% have no dedicated AI risk roles, compared to 23% of those with fewer than 100 employees.

Chart 3: Structure of team responsible for ethical, legal and regulatory compliance related to AI

Source: Deloitte Trustworthy AI survey (2024)

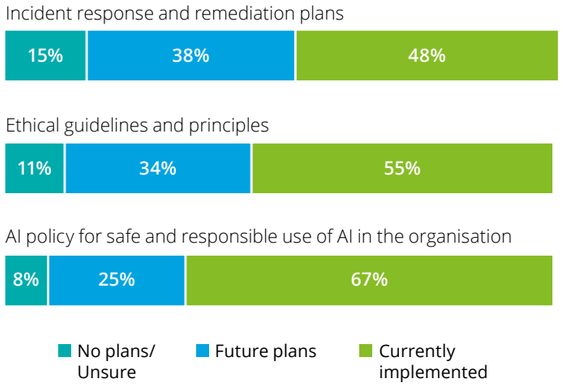
PILLAR 2

Policy and principles

Clear, broadly understood policies and principles are a fundamental prerequisite for effective AI governance. This AI policy differs from an AI strategy, with the latter including broader elements such as ambitions related to AI and key metrics to measure progress. While most organisations across Asia Pacific have an AI strategy in place, many are missing key elements of good governance in their AI policy. More than half of AI policies lack timelines for implementing AI governance goals or contain ethical guidelines and principles related to AI.

Including these governance features in an AI policy is key for employees to see the value. Among organisations with an organisation-wide AI strategy, 30% report that not all employees see the strategy's value. Where the AI policy includes monitoring or auditing, i.e. having a defined risk appetite, response and remediation plan integrated with broader organisation policies, employees are more likely to see the value in the strategy.

Chart 4: Implementation of trustworthy AI policies



Source: Deloitte Trustworthy AI survey (2024)

PILLAR 3

Procedures and controls

The third pillar explores day-to-day practices for managing AI-related risks and standards in an organisation. This includes an assessment procedure to identify and manage AI-related risks, a comprehensive inventory of AI solutions used, and control frameworks that mitigate risks associated with the use of an AI solution. With the fewest organisations categorised as 'Ready' for this pillar, progress in this area will be key for improving trustworthy AI performance across the region.

A key element of effective AI governance is a system for employees to report queries or incidents related to AI use in the workplace. Yet, two in five organisations lack such a reporting mechanism. Organisations with formal reporting systems see five times more queries and twice as many reported incidents – indicating that those without these systems may be blind to emerging risks associated with AI. This issue is only growing more urgent, especially in Asia Pacific, where the number of queries and incidents continues to rise (see Chart 5).

Chart 5: Change in the number of incidents related to AI in FY24 compared to FY23

Source: Deloitte Trustworthy AI survey (2024) Note: excludes 'unsure' answers (6)

PILLAR 4

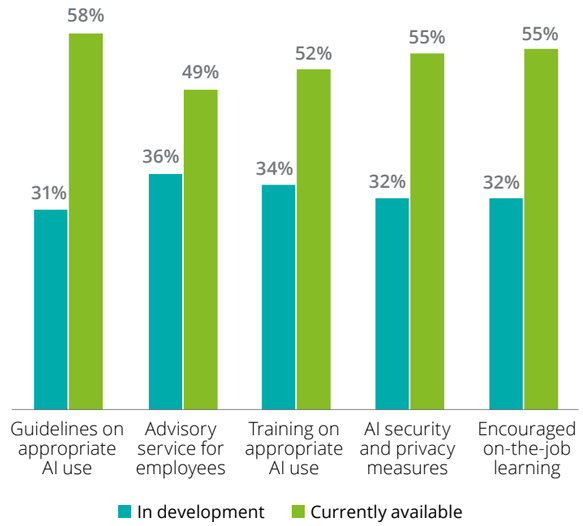
People and skills

Employees play a crucial role in ensuring trustworthy AI. Yet, this remains a challenge for many organisations, where only 56% of employees, on average, have the skills and capabilities to use AI responsibly.

Training can be a powerful tool to bridge this gap. Organisations that provide AI training see a 27% higher share of employees equipped to use AI safely compared to those that don't – though just 52% of organisations surveyed currently offer such programs. That said, 72% of organisations that currently don't offer training are actively developing programs for their teams.

The majority of organisations do offer guidelines on responsible AI use, and 55% encourage on-the-job learning and experimentation and slightly fewer organisations have an advisory service or body for employees (49%). Private sector organisations lead in offering AI use guidelines and training, whereas public sector organisations are more likely to focus on security measures and encourage on-the-job learning.

Chart 6: Resources available to employees to support them using AI



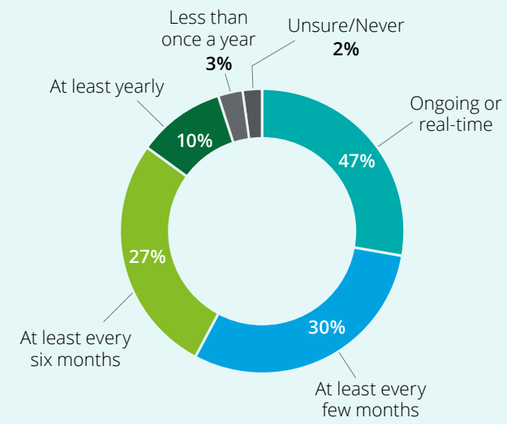
Source: Deloitte Trustworthy AI survey (2024)

PILLAR 5

Monitoring, reporting and evaluation

Having AI governance systems that are responsive to changing requirements and emerging issues is critical to ensuring organisations can respond to risks and incidents as they emerge. Overall, organisations performed relatively well in this pillar, with the equal highest share (18%) achieving 'Ready' status. The majority (85%) of organisations evaluated their AI governance against internal standards at least every six months (i.e. those evaluating at least every six months, three months or in real-time). Monitoring and evaluating whether AI governance is complying with any changes in regulatory requirements is another element of this pillar. Nearly three-quarters of organisations review legal and regulatory requirements at least every six months.

Chart 7: Frequency of evaluating AI systems against internal organisation standards



Source: Deloitte Trustworthy AI survey (2024)

How does trustworthy AI compare across industries?

The results for the AI Governance Maturity Index and individual pillars vary by industry. We find that organisations within technology, financial services and professional services more generally have the highest share of organisations that are 'Ready' for trustworthy AI. Meanwhile, public sector and life science and healthcare organisations have a lower share. A high-level summary of four key industries is over the following pages. A similar summary for key geographies across Asia Pacific is available in Appendix D.

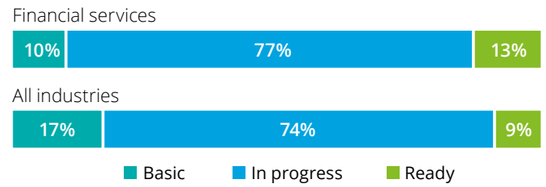
Spotlight on

Financial services industry

Being a knowledge and data intensive industry, financial services have been leading adopters of digital innovation. The relatively higher levels of regulation and sensitive financial information held by these organisations means that governance processes have needed to develop rapidly in response to new innovations.

Our AI Governance Maturity Index shows the financial services industry has higher levels compared with other industries. Demand for financial services is growing, particularly among younger and more tech literate consumers, which suggests good governance will be required for future growth in the industry. Complying with regulations and protecting client data will be key issues as the sector continues to adopt AI technologies.

AI Governance Maturity Index



Note: may not sum to 100% due to rounding

Top three expected **benefits** of effective AI governance

- Higher levels of trust in the outputs or results from AI solutions (57%)
- Greater use of AI solutions as a result of higher trust (47%)
- Faster deployment of AI solutions across the organisation (47%)

Top three concerns about **risks** associated with using AI

- Reliability and errors (92%)
- Legal risk and copyright infringement (88%)
- Security vulnerabilities (87%)

Top three **barriers** associated with using or implementing AI

- Concerns about regulatory, legal, ethical, compliance and other risks (45%)
- Technology implementation challenges (38%)
- Lack of appetite for innovation and/or insufficient experimentation (32%)

70% of financial services organisations have a system for employees to raise concerns.

57% of financial services organisations' employees have the required level of skills to use AI solutions in ethically and legally.

42% of financial services organisations reported an increase in incidents received in the last financial year.

68% of financial services organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for financial services = 60

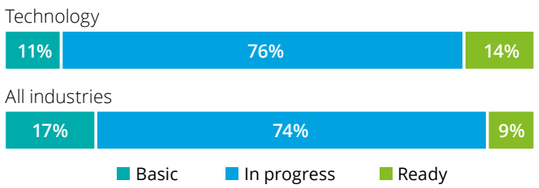
Spotlight on

Technology industry

The technology industsry is at the forefront of AI disruption and a key enabler of developing AI solutions for other industries. As long-time users of AI solutions, the industry has more established governance processes compared with other industries, leading to higher results in the AI Governance Maturity Index.

Based on the Deloitte Generation AI report, technology employees lead in adoption of GenAI into their workflow, allowing the sector to be highly responsive to new developments. The sector faces key challenges in managing legal and confidentiality risks surrounding the use of data in technology solutions. As the sector provides technology support to other industries, prudent governance will be a priority to maintain customer trust.

AI Governance Maturity Index



Note: may not sum to 100% due to rounding

Top three expected **benefits** of effective AI governance

- Greater use of AI solutions as a result of higher trust (58%)
- Higher levels of trust in the outputs or results from AI solutions (54%)
- Faster deployment of AI solutions across the organisation (53%)

Top three concerns about **risks** associated with using AI

- Legal risk and copyright infringement: legal liabilities or responsibilities (84%)
- Privacy: risk of sensitive, confidential or personal data breaches (83%)
- Security vulnerabilities: risks of hacking/cyber-attacks, unauthorized access or misuse of AI systems (81%)

Top three **barriers** associated with using or implementing AI

- Technology implementation challenges (39%)
- Concerns about regulatory, legal, ethical, compliance and other risks (34%)
- Insufficient understanding of the technology and its potential (33%)

62% of technology sector organisations have a system for employees to raise concerns.

63% of technology sector organisations' employees have the required level of skills to use AI solutions in ethically and legally.

24% of technology sector organisations reported an increase in incidents received in the last financial year.

71% of technology sector organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for technology sector = 160

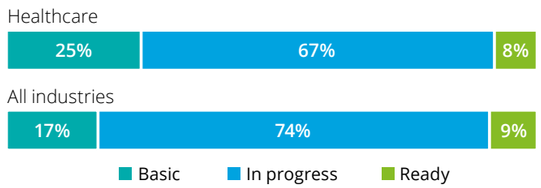
Spotlight on

Life sciences and healthcare industry

AI solutions in healthcare often require personal data – such as medical conditions and demographic information – which require robust privacy and security standards. The nature of this data contributes to security vulnerabilities being one of the top risks identified by the industry. Patients require this certainty before providing consent for their data to be used in AI solutions, hence the improved reputation among customers and social licence to operate being key benefits.

The relatively higher share of 'Basic' organisations in this industry is consistent with evidence that healthcare can be slower to embrace digital transformation and there can be resistance among employees. This could mean healthcare organisations are prevented from using AI solutions unless AI governance is improved.

AI Governance Maturity Index



Note: may not sum to 100% due to rounding

Top three expected **benefits** of effective AI governance

- Improved reputation amongst customers (44%)
- An established social license to operate AI solutions (42%)
- Greater regulatory compliance (42%)

Top three concerns about **risks** associated with using AI

- Security vulnerabilities: risk of hacking / cyber (86%)
- Surveillance: invasion of privacy due to pervasive surveillance (86%)
- Regulatory burden: the extent of reporting and process requirements associated with using AI solutions (83%)

Top three **barriers** associated with using or implementing AI

- Insufficient understanding of the technology and its potential (39%)
- Lack of executive commitment (33%)
- Lack of strategy and vision for AI implementation (33%)

55% of healthcare organisations have a system for employees to raise concerns.

51% of healthcare organisations' employees have the required level of skills to use AI solutions in ethically and legally.

31% of healthcare organisations reported an increase in incidents received in the last financial year.

61% of healthcare organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Life Sciences and Healthcare Sector = 36

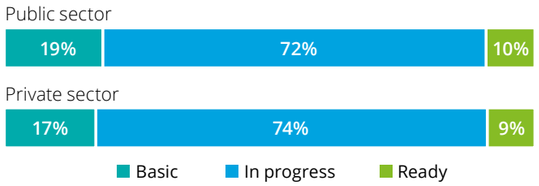
Spotlight on

Public sector

Public sector organisations across Asia Pacific face key challenges relating to regulation and ethical use of AI. Being flexible and quick to respond to the new concerns emerging around the use of AI technologies is a priority to stay on top of the shifting environment.

AI has the potential to enhance the efficiency of public services to deliver digital services to citizens, but in doing so data security must be ensured to protect against risks of cyber-attacks. This is contributing to a relatively higher share of organisations with concerns around security vulnerabilities and surveillance.

AI Governance Maturity Index



Note: may not sum to 100% due to rounding

Top three expected **benefits** of effective AI governance

- Higher levels of trust in the outputs or results from AI solutions (56%)
- Greater use of AI solutions as a result of higher trust (54%)
- Faster deployment of AI solutions across the organisation (48%)

Top three concerns about **risks** associated with using AI

- Security vulnerabilities: risk of hacking / cyber (87%)
- Surveillance: invasion of privacy due to pervasive surveillance (83%)
- Malicious content (82%)

Top three **barriers** associated with using or implementing AI

- Technology implementation challenges (38%)
- Concerns about regulatory, legal, ethical, compliance and other risks (37%)
- Insufficient understanding of the technology and its potential (36%)

65% of public sector organisations have a system for employees to raise concerns.

57% of public sector organisations' employees have the required level of skills to use AI solutions ethically and legally.

28% of public sector organisations reported an increase in incidents received in the last financial year.

69% of public sector organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Government and Public Services = 172
The Public Sector is defined by the ownership of the organisations within the sector, whereas the other industries are defined by a specific good or service that is being produced. The organisations in the Public Sector operate in a number of industries such as health and finance.

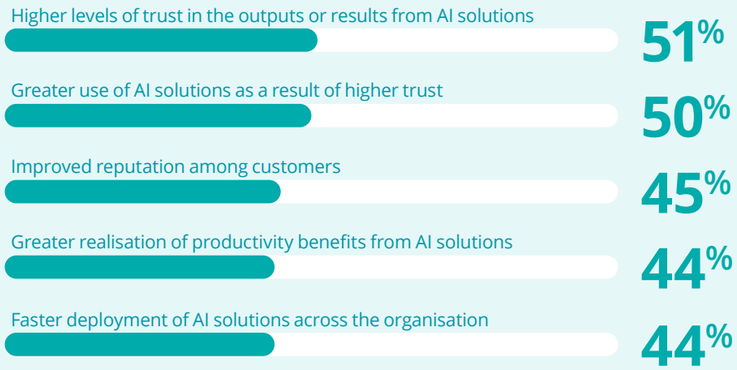
04

The dividends from good AI governance

Organisations that invest in developing their AI Governance maturity are attaining significant dividends with senior leaders recognising that they will not unlock the opportunities from AI unless they can trust the outputs.

Chart 8

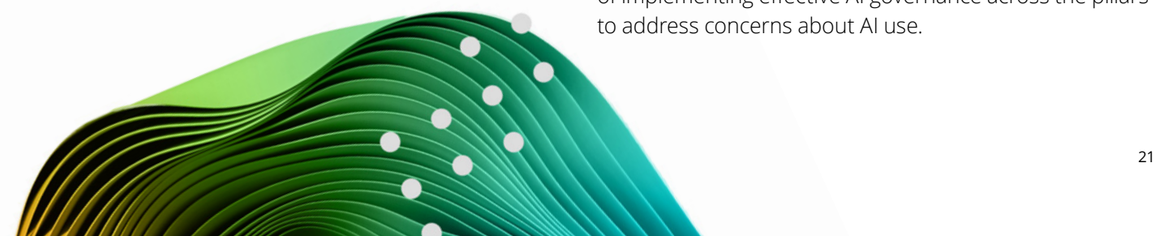
Top five benefits of trustworthy AI



Source: Deloitte Trustworthy AI survey (2024)

One of the most common benefits associated with effective AI governance is **higher levels of trust in the outputs or results from AI solutions,** with half (51%) of senior leaders selecting this benefit (Chart 8). A separate study found that transparent AI systems improve users' trust by 30%, thereby increasing the likelihood of adoption and utilisation.[9]

Greater trust in AI outputs comes from governance providing tangible actions to mitigate the risks discussed in the earlier chapter that senior leaders are facing when using AI. For example, implementing incident responses and remediation plans can provide leaders with confidence that issues will be appropriately managed. Those organisations with 'Ready' levels of AI Governance Maturity were less likely to be concerned about key risks such as security, privacy or legal risk (Chart 9). Both 'In progress' and 'Basic' organisations had similar levels of concerns about the risks, highlighting the importance of implementing effective AI governance across the pillars to address concerns about AI use.

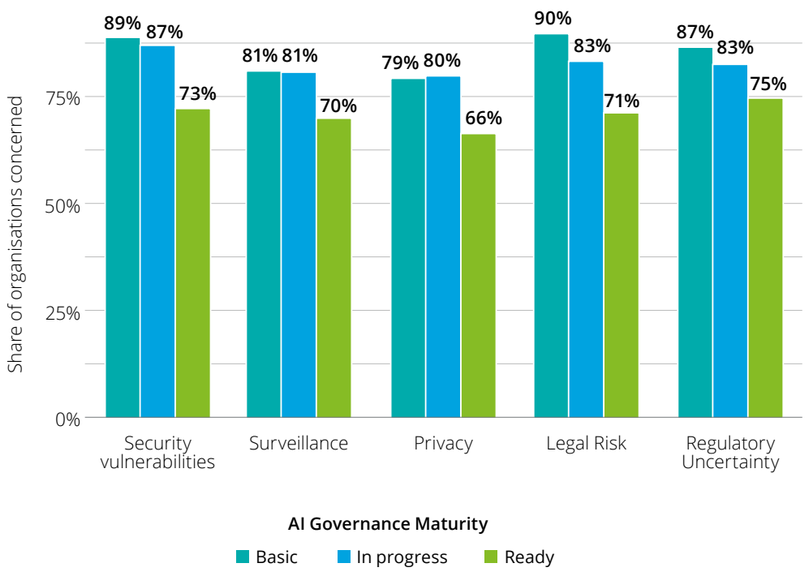


Greater use of AI solutions across the organisation is another key benefit of having effective governance, with half of senior leaders reporting this benefit. This result was validated using econometric modelling, which found that organisations attaining a 'Ready' level in the AI Governance Maturity index have deployed AI solutions across three additional areas of the organisation, compared to otherwise similar organisations with only a 'Basic' level.[10] For example, **'Ready' organisations are three times or more likely to use AI in customer service, marketing and sales, operations and production, and research and development (R&D).**

In addition, establishing governance arrangements for AI also increases the **extent of use** within the area where the AI solution has been deployed. Organisations with a 'Ready' rating have 16 percentage points, on average, more employees using AI tools compared with 'Basic' organisations. This is equivalent to **a 28% increase in the number of users of AI for the average organisation.** This result holds even when comparing organisations that have deployed AI solutions to the same sub-areas (e.g., marketing and sales or research and development) within their business – suggesting that trustworthy AI overall supports better uptake of AI solutions among an organisation's staff. For further details about the modelling for this report, please see Appendix C.

"Modelling undertaken for this research shows that effective AI governance increases both the breadth of AI use (across the organisation) and depth (used by more employees) of deployed AI solutions in an organisation."

Chart 9: Concerns about key risks, by AI Governance Maturity



Source: Deloitte Trustworthy AI survey (2024)

Customers are increasingly concerned about ethical considerations and data privacy when it comes to AI. In fact, only half of consumers feel that the benefits realised from online services outweigh data privacy concerns.[11] Having effective AI governance demonstrates a commitment to these values, enhancing the organisation's reputation. This **customer reputational benefit** was recognised by 45% of senior leaders.

Both traditional AI and GenAI tools have shown that they can significantly boost productivity. According to Deloitte's analysis of 11,900 young employees and students, whom we've dubbed "Generation AI", daily users of GenAI save 5.3 hours each week.[12] This may have increased as users become more familiar with using the technology and the capabilities of the technology continue to develop.

Another study indicates that companies using AI solutions report a 15% increase in operational efficiency and productivity.[13] **Our findings show that effective governance frameworks can make AI solutions even more productive, with 44% of senior leaders reporting higher productivity gains.** The modelling for this report shows that higher levels achieved on the Trustworthy AI Index are associated with higher revenue growth over the past year. An extra 15 points on the Trustworthy AI Index score is associated with 4.6 percentage points higher revenue growth, even after controlling for the level of AI use. For a large organisation (with more than 1,000 employees) that experienced growth of $100 million from Financial Year 2024 to 2025, the organisation would realise an increase of $4.6 million of revenue growth as a result of a higher level of Trustworthy AI. For the median organisation (with 19.5% revenue growth last year), this would reflect a near 25% increase. For further details about the modelling for this report, please see Appendix C.

"Having the right AI governance can make AI solutions more productive. Higher AI Governance Maturity scores leads to an increased revenue growth, even after accounting for the amount of AI solutions being used."

There can be a misconception that AI governance can lead to internal business red tape, consequently slowing down AI adoption in an organisation. Yet, effective AI governance can streamline the process of deploying AI solutions by establishing clear procedures and controls. 44% of senior leaders believe effective AI governance can lead to faster deployment of AI solutions across the organisation and this result is reinforced by another study, which found that organisations with strong AI governance frameworks deploy AI solutions 20% faster than those lacking such frameworks.

05

Building the foundations for trustworthy AI

Effective AI governance is critical for organisations when integrating AI solutions into their operations and business models. As shown in previous chapters, more effective governance leads to greater use of the technology and increased returns while helping to manage downside risks.

So, what are the critical steps that organisation leaders can take now to improve their AI governance? Based on the analysis of our findings, four high-impact actions stood out:

RECOMMODATION 1

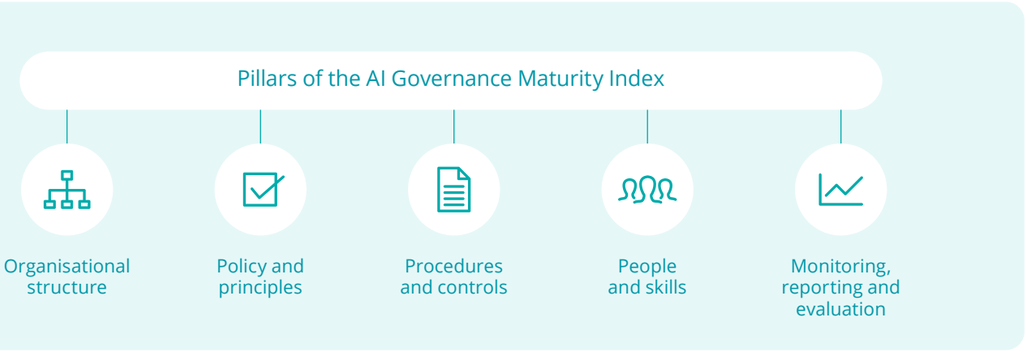
Prioritise AI governance to realise the returns from AI

1

The AI Governance Maturity Index has revealed that the majority of organisations can substantially improve their AI governance. This research shows that enhancing AI governance is not a 'nice to have' but a critical enabler to leverage one of the most powerful enterprise technologies. The first step in prioritising AI governance is understanding the starting point.

The AI Governance Maturity Index identifies five pillars – organisational structure, policy and principles, procedures and controls, people and skills and monitoring, reporting and evaluation – that organisations can use to evaluate their own systems and identify areas for improvement. Our research suggests that many organisations should focus primarily on both the policies and principles and procedures and controls pillars.

Continuous evaluation of AI governance is also required to address new or emerging risks related to AI or as solutions are deployed. Changing regulations for specific locations and industries requires businesses to remain at the forefront of standards related to AI governance.



RECOMMODATION 2

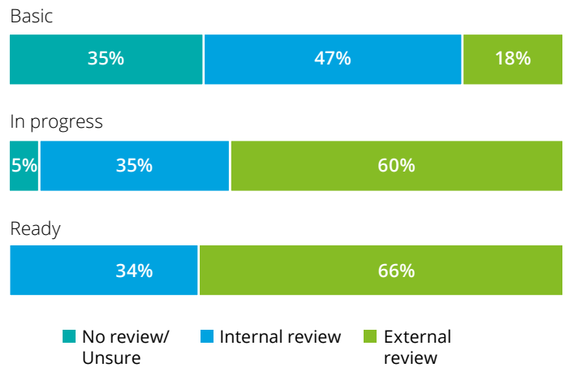
Understand and leverage the broader AI supply chain

2

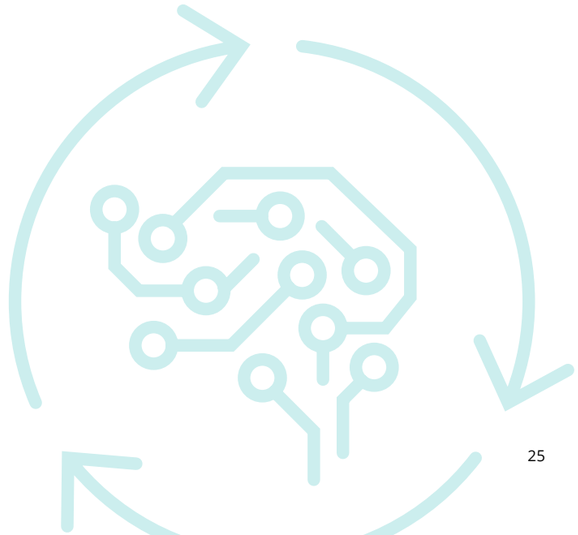
Understanding an organisation's own use of AI alongside its interactions with the broader 'AI supply chain' – i.e. developers, deployers, regulators, platform providers, end users and customers – can help organisations develop a more holistic understanding of AI governance requirements. For example, 15% of senior leaders report their organisations are using a combination of purchased 'off-the-shelf' AI solutions, AI solutions developed in-house, and publicly available AI applications. Each of these sources of AI requires a tailored governance approach.

Senior leaders can also leverage the broader 'AI supply chain' to improve their AI governance settings as this group is likely to have expert and/or different perspectives. Increasingly, organisations are looking to build a 'Third level of Defence' in their governance framework by engaging external audit organisations. To be effective in this role, these audits do need to occur throughout the AI solution lifecycle. Notably, organisations that have engaged an external organisation to review the implementation of AI solutions are associated with higher Trustworthy AI indices (Chart 10). Two-thirds of organisations classified as 'Ready' have had the implementation of AI solutions reviewed by an external party. Consultations for this research also found that engagement with relevant industry associations can be helpful for understanding unique requirements for AI governance.

Chart 10: Types of reviews of AI implementation and AI Governance Maturity Index



Source: Deloitte Trustworthy AI survey (2024)



RECOMMODATION 3

Build risk managers, not risk avoiders

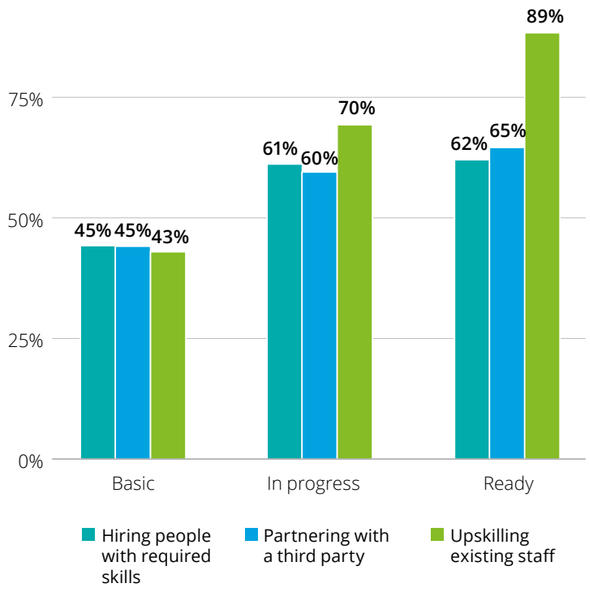
3

Human judgement and action (or reaction) are critical to successful AI governance. The employees – whether they are designing, deploying, or using the AI solutions themselves – will have valuable insights about the functionality and potential risks related to using AI solutions. Importantly, developing the skills and capabilities of employees can help to identify, assess and manage risks that can lead to preventing or mitigating risks that emerge rather than risk avoidance or risk ignorance. With this in mind, people and skills are a critical pillar within the AI Governance Maturity Index, but despite its importance, this pillar remains the area where organisations consistently score the lowest on average.

'Ready' organisations are more likely to actively develop skills and capabilities to ensure that employees are using AI ethically and responsibly. Nearly 90% of organisations classified as 'Ready' in the AI Governance Maturity Index are upskilling their existing staff to close the skills gap relating to the ethical and legal use of AI. On the other hand, only 43% of 'Basic' organisations are upskilling existing staff to close this gap. 'Ready' organisations are also partnering with third-party organisations with the right skills (65%) as well as hiring employees with the right skills (63%).

These actions are having a tangible impact on closing the AI skills gap, and continuously updating and refreshing these skills will be critical as the capabilities of the technology and regulatory environment evolve. Organisations classified as 'Ready' are associated with higher proportions of employees with the required level of skills and capabilities to use AI in an ethical and legally compliant way (73%), compared to 40% of employees in 'Basic' organisations.

Chart 11: Closing the skills gap approaches and AI Governance Maturity Index



Source: Deloitte Trustworthy AI survey (2024)

RECOMMODATION 4

Communicate across the organisation and ensure AI transformation readiness

4

Effective communication is important in the day-to-day governance of AI and will be necessary to bring your people on the journey. This includes being transparent about the long-term AI strategy, the benefits and risks to the business, upskilling teams on how to use AI models and reskilling people whose activities may be performed by AI in the future. It is essential to ensure that all stakeholders are aware of the risks and benefits associated with AI, and that they can make informed decisions about its use and raise a concern. This requires clear and transparent communication, as well as a willingness to engage in dialogue. Practical actions organisations can include scenario planning for high-risk events, narrative development so leaders and employees can tell a credible, human story about the role and impact of the technology, and crisis exercising to test readiness for a severe but plausible event.

"Establishing good AI governance often requires a mindset change in the organisation. When having initial conversations, some colleagues question whether governance was just a IT issue. Having a number of conversations about how AI intersects across the whole businesses – from IT, cyber, risk to regulatory compliance – has led to recognition that every team is accountable when it comes to good AI governance."

Director of Data Strategy, major telecommunications provider

Appendices

Appendix A
Survey

In September and October 2024, we surveyed 899 senior leaders across thirteen locations across the Asia Pacific region. The survey aimed to assess the maturity level of AI governance structures and understand the benefits of good AI governance.

Respondents were specifically targeted to be in senior roles like chief risk officers, chief compliance officers and chief data officers across various sectors, including public, private and not-for-profit, and a range of industries (including finance, education, health and technology).

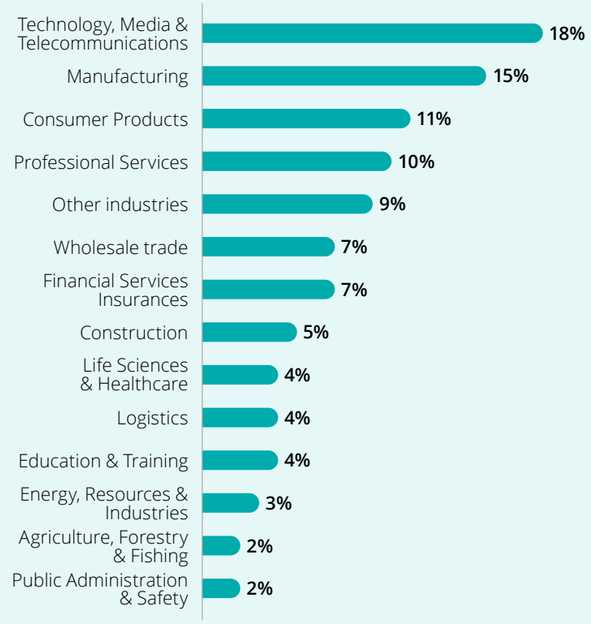
Table A1 shows the number of respondents in various locations across the Asia Pacific region. Charts A2 and A3, present the industries of employment and the role of respondents.

Table A1: Location of survey respondents

Locations	Number of respondents
Australia	112
China	103
India	102
Japan	104
New Zealand	53
Southeast Asia	321
Indonesia	64
Malaysia	51
Philippines	52
Singapore	51
Thailand	51
Vietnam	52
South Korea	52
Taiwan (China)	52
Total	**899**

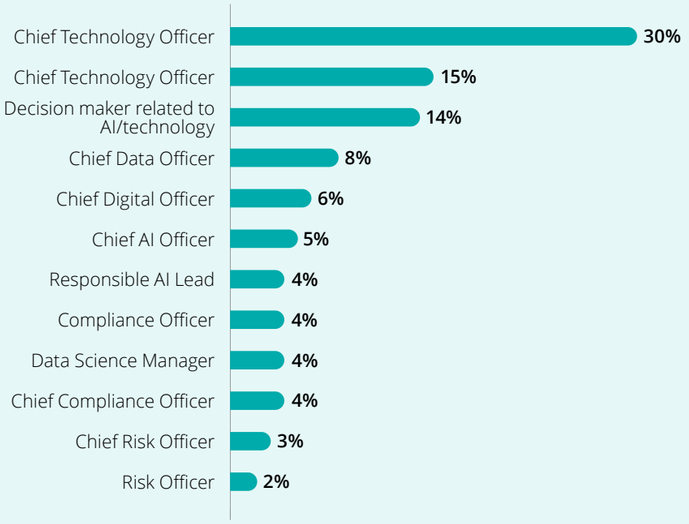
Source: Deloitte Trustworthy AI survey (2024)

Chart A2: Industry of survey respondents



Source: Deloitte Trustworthy AI survey (2024)

Chart A3: Position of survey respondents



Source: Deloitte Trustworthy AI survey (2024)

Appendix B
Deloitte AI Governance Maturity Index

The Deloitte AI Governance Maturity index developed for this research is informed by the answers to 12 questions (some with multiple sub-questions) organised into five key pillars outlined below. This methodology was applied to nearly 900 organisations based on the responses to the survey.

Organisational Structure

1) Who in your organisation is primarily responsible for ensuring that ethical, legal and technical standards of AI are articulated and evaluated in your organisation?

Possible answers: The Board, Chief Executive Officer, Chief Technology Officer, Chief Digital Officer, Chief Data Officer, Chief Compliance Officer, Chief Information Officer, Chief Risk Officer, Chief AI Officer, Senior executive team, Compliance officer, Responsible AI lead, Heads of department/general manager/senior manager), AI development teams, other

2) Which of the following elements of organisational structure related to AI use are currently in place in your organisation?

a. AI governance operating structure with board oversight
b. AI committee responsible for overseeing AI governance, including representatives from legal, compliance, IT, HR, and other relevant departments
c. Clearly defined roles and responsibilities for AI governance across the AI lifecycle, e.g. Business Outcome Owner, AI System Owner, Data Owner, Domain Architect etc.

3) Which of the following best describes how the team responsible for ethical, legal and regulatory compliance related to AI is structured in your organisation?

a. We do not have formal ethics, risk or compliance roles related to AI use
b. Some departments/teams have dedicated ethics, risk and compliance professionals related to AI use
c. Every department/team has its own dedicated ethics, risk and compliance professionals related to AI use
d. There is a centralised ethics, risk and compliance team that works across the organisation to monitor trends and detect risks related to AI use
e. None of the above
f. Unsure / prefer not to say

Policy and Principles

1) How would you best characterise the strategy for leveraging AI within your organisation?

a. No AI strategy exists and no steps are being taken to develop one
b. No AI strategy currently exists but steps are being taken to actively develop one
c. Some departments/teams have their own AI strategy
d. There is an organisation-wide AI strategy, but not everyone sees its value
e. There is an organisation-wide AI strategy and it's a priority, but we don't track progress
f. There is an organisation-wide AI strategy, which includes clearly defined processes to prioritise and measure the value of our analytics initiative
g. Unsure / prefer not to say

2) Which of the following elements are included within your AI strategy or governance framework?

a. AI policy for safe and responsible use of AI in the organisation
b. Ethical guidelines and principles
c. A clearly defined AI risk appetite for your organisation
d. Timelines for implementation of AI governance goals and procedures
e. Funding for implementation of the governance initiatives
f. Monitoring and auditing processes
g. Incident response and remediation plans
h. Performance metrics and KPIs
i. Integration with other relevant policies (privacy, data governance and cyber) or strategic objectives of the organisation

3) Which of the following elements are in place with regards to AI systems used or deployed within your organisation?

a. Clear assignment of roles and responsibilities for the oversight and ongoing monitoring for AI systems
b. Clear assignment of accountability for decisions made or derived with use of AI systems
c. Protections are in place to ensure AI systems do not use data beyond its intended and stated use
d. Users understand how the AI system makes decisions that impact them
e. Mechanisms are in place to detect and mitigate biases in AI systems to ensure fairness and equity
f. AI systems are designed and operated responsibly, with an aim for human, social and environmental wellbeing
g. AI systems are designed and operated to produce consistent and accurate output, withstand errors and recover quickly from unforeseen disruptions
h. AI systems are protected from unauthorised access and exploitation by attackers
i. Data anonymisation and pseudonymisation measures are in place to protect personal and sensitive information

Procedures and Controls

1) **Are there systems in place for employees to raise concerns about the use and output of AI?**

   Possible answers: Yes; No; Plans for systems to be implemented; Unsure

2) **Which of the following practices, procedures or controls related to AI use are in place in your organisation?**

   a. AI risk taxonomy that define the set of risk of AI solutions
   b. AI risk assessment procedure that supports identification and management of AI-related risks in development, trialling and implementation
   c. AI controls framework that seeks to mitigate any risks associated with use of an AI solution
   d. A current inventory of AI solutions used by your organisation, including both internally developed or procured
   e. AI governance platform that evaluates and monitors AI system activities for risk and compliance
   f. System to capture information across the AI lifecycle to support audit by independent third parties
   g. Procedures in place for risk or complaints handling by external parties (clients or other stakeholders) for AI use.

People, Skills and Culture

1) **Which of the following resources are available to employees to support them using AI in an ethical, legally and regulatory compliant and accurate way?**

   a. Provided guidelines on how to use AI appropriately at work
   b. Developed an advisory service or body for employees to query aspects of using AI with team members experienced in risk and regulatory compliance
   c. Provided training on how to use AI appropriately at work, understanding the ethical, legal, and regulatory compliance risks associated with it
   d. Introduced security and privacy measures around the use of AI systems (e.g., data encryption and access controls)
   e. Encouraged on-the-job learning (e.g., independent experimentation by employees, communities of practice, discussions between team members)

2) **Based on your best estimate, what share of employees have the required skills and capabilities to use AI in a legally and ethical compliant way?**

Monitoring, reporting and evaluation

1) **How frequently does your organisation review existing legal or regulatory requirements for using AI at work to protect rights and prevent misuse?**

   a. At least every few months
   b. At least every six months
   c. At least yearly
   d. Less than once a year
   e. None of the above
   f. Unsure / prefer not to say

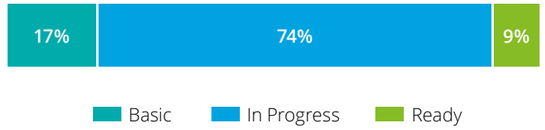
2) **How often are you evaluating your AI systems to ensure that they are meeting your organisation's standards for AI?**

   a. Ongoing or real-time
   b. At least every few months
   c. At least every six months
   d. At least yearly
   e. Less than once a year
   f. None of the above
   g. Unsure / prefer not to say

Each answer was given a score between 0 and 100, with the 'best' answer in each question given a score of 100. For example, if an organisation answered that 'there is an organisation-wide AI strategy with defined processes to prioritise and measure value', it received a score of 100 for that question, while if only some departments had AI strategies, a score of 60 was given. The score for each pillar is the average score for questions within each pillar, and the overall index is equal to the average score for each pillar.

Those with a score below 50 were categorised as 'Basic', those with a score between 50 and 90 were categorised as 'In progress' and those with a score above 90 were categorised as 'Ready'. The distribution of categories based on these scores is presented below:

Chart B1: Distribution of AI Governance Maturity Index scores



Source: Deloitte Trustworthy AI survey (2024)

The average, median scores for each pillar of the index are presented in the table below along with the share of organisations receiving a 'Basic' or 'Ready' score.

AI Governance Maturity Index Pillar	Average	Median	% Basic	% Ready
Overall Index	70.8	68.0	9%	17%
Organisational Structure	73.9	72.0	9%	18%
Policy and Principles	58.4	66.3	31%	13%
Practices, Processes and Controls	64.8	67.5	23%	10%
People, Skills and Culture	67.2	70.0	22%	14%
Monitoring, Reporting and Evaluation	76.0	80.0	6%	18%

Appendix C
Econometric Modelling

To estimate the relationship between good AI governance practices and measures of business performance, Ordinary Least Squares regressions were estimated. To reduce the risk of omitted variable bias, key characteristics of organisations were included as control variables. These control variables are listed in the table below:

Control variable	Details
Country of headquarters	Self-reported country of headquarters (of 13 options)
Industry	Self-reported ANZSIC (1-digit) category (of 19 options)
Number of Employees	Self-reported number of full-time equivalent (FTE) employees (of 4 options)
Sector	Sector of organisation (public, private or non-profit)
Revenue	Self-reported revenue in FY2023-24 (continuous, converted to USD at October 2024 exchange rates)

The two dependent variables are the number of areas of the business (out of 10 options) that respondents indicated had 'fully implemented' AI solutions, and the share of workers in the business using AI solutions in their work (between 0 and 100).

The key independent variable of interest is the Deloitte AI Governance Maturity Index, calculated as described in the appendix above. Specifications using both the numeric value and the categorisation into three categories were estimated.

In addition, recognising an organisation's level of AI adoption is likely correlated with both the error term and the independent variables, the share of workers using AI was included as a control. The inclusion of these variables does not significantly change the key parameter estimates. For models with the share of workers using AI as the independent variable, the number of areas of the business with fully implemented AI solutions was used as a control.

Formally, regressions of the form were estimated:

1) Share of Workers Using AI=$\beta_0+\beta_1$*Index Score+β_2*Areas with AI tools+Control Variables

2) Areas with AI tools=$\beta_0+\beta_1$*Index Score+β_2*Share of Workers Using AI+Control Variables

3) Revenue growth=$\beta_0+\beta_1$*Index Score+β_2*Share of Workers Using AI+Control Variables

Regression summary tables for these regressions are presented below. These models should be interpreted with caution, as data is self-reported and it is possible that there are remaining unobserved factors correlated with both the explanatory variables and the error term, biasing estimates. Results should be interpretated as correlations only.

Model 1: dependent variable – share of workers using AI tools

Variable	Estimate	Std. Error	P-Value
Index Score	0.30543	0.0646	<0.00001
Areas with AI tools	2.02022	0.3996	<0.00001
R^2	0.1978		
Adjusted R^2	0.1510		

Model 2: dependent variable – share of workers using AI tools

Variable	Estimate	Std. Error	P-Value
Index category – 'In progress'	8.27383	2.865	<0.00001
Index category – 'Ready'	15.7533	4.123	0.004
Areas with AI tools	2.257	0.393	<0.00001
R^2	0.1881		
Adjusted R^2	0.1394		

Model 3: dependent variable – areas with AI tools

Variable	Estimate	Std. Error	P-Value
Index Score	0.0555	0.0061	<0.00001
Share of Workers Using AI	0.0197	0.0039	<0.00001
R^2	0.3352		
Adjusted R^2	0.2965		

Model 4: dependent variable – areas with AI tools

Variable	Estimate	Std. Error	P-Value
Index category – 'In progress'	1.3557	0.283	<0.00001
Index category – 'Ready'	3.0569	0.396	<0.00001
Share of Workers Using AI	0.0226	0.004	<0.00001
R^2	0.3120		
Adjusted R^2	0.2707		

Model 5: dependent variable – revenue growth in FY23-24

Variable	Estimate	Std. Error	P-Value
Index Score	0.0031	0.0018	0.0884
Share of Workers Using AI	0.0017	0.0011	0.1355
R^2	0.0677		
Adjusted R^2	0.004769		

Appendix D
Location spotlights

Spotlight on **Australia**

Australia population: 27.1 million | GDP: $1.7 trillion USD

Top three expected **benefits** of effective AI governance

- Higher levels of trust in the outputs or results from AI solutions (47%)
- Greater use of AI solutions as a result of higher trust (46%)
- Greater regulatory compliance (42%)

Top three concerns about **risks** associated with using AI

- Surveillance: invasion of privacy due to pervasive surveillance (88%)
- Privacy: risk of sensitive, confidential or personal data breaches from AI systems (88%)
- Security vulnerabilities: risks of hacking / cyber (85%)

Top three **barriers** associated with using or implementing AI

- Concerns about regulatory, legal, ethical, compliance and other risks (44%)
- Insufficient understanding of the technology and its potential (34%)
- Lack of talent and/or technical skills (29%)

55% of Australian organisations have a system for employees to raise concerns.

55% of Australian organisations employees have the required level of skills to use AI solutions in ethically and legally.

23% of Australian organisations reported an increase in incidents received in the last financial year.

63% of Australian organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Australia = 112

Spotlight on **China**

China population: 1,419 million | GDP: $18.2 trillion USD

Top three expected **benefits** of effective AI governance

- Greater use of AI solutions as a result of higher trust (52%)
- Greater realisation of productivity benefits from AI solutions (51%)
- Faster development of AI solutions across the organisation (50%)

Top three concerns about **risks** associated with using AI

- Security vulnerabilities: risk of hacking / cyber (86%)
- Legal risk and copyright infringement (80%)
- Regulatory burden: the extent of reporting or process requirements associated with using AI solutions (80%)

Top three **barriers** associated with using or implementing AI

- Technology implementation challenges (38%)
- Lack of appetite for innovation and/ or insufficient experimentation (36%)
- Lack of talent and/or technical skills (34%)

54% of Chinese organisations have a system for employees to raise concerns.

57% of employees in Chinese organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.

39% of Chinese organisations reported an increase in incidents received in the last financial year.

74% of Chinese organisations are partnering with a third party to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for China = 103

Spotlight on **India**

India population: 1,451 million | GDP: $3.95 trillion USD

Top three expected **benefits** of effective AI governance

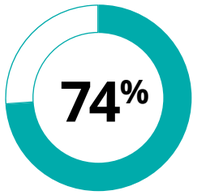
- Higher levels of trust in the outputs or results from AI solutions (63%)
- Improved reputation among customers (60%)
- Greater use of AI solutions as a result of higher trust (57%)

Top three concerns about **risks** associated with using AI

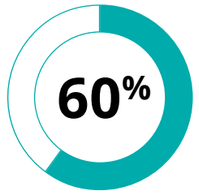
- Security vulnerabilities: risk of hacking / cyber (92%)
- Privacy: risk of sensitive, confidential or personal data breaches (91%)
- Regulatory uncertainty: changing requirements that may result in being unaware of obligations (89%)

Top three **barriers** associated with using or implementing AI

- Technology implementation challenges (50%)
- Insufficient understanding of the technology and its potential (35%)
- Concerns about regulatory, legal, ethical and other risks (32%)

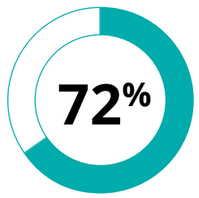


of Indian organisations have a system for employees to raise concerns.



of employees in Indian organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.

of Indian organisations reported an increase in incidents received in the last financial year.



of Indian organisations are hiring people with the required skills to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for India = 102

Spotlight on **Japan**

Japan population: 123.8 million | GDP: $4.1 trillion USD

Top three expected **benefits** of effective AI governance

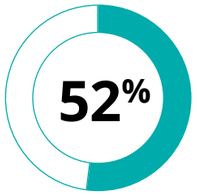
- Higher levels of trust in the outputs or results from AI solutions (51%)
- Improved reputation among customers (49%)
- Greater use of AI solutions as a result of higher trust (45%)

Top three concerns about **risks** associated with using AI

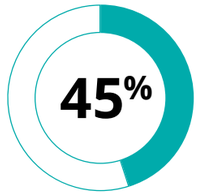
- Security vulnerabilities: risk of hacking / cyber (88%)
- Surveillance: invasion of privacy due to pervasive surveillance (85%)
- Privacy: risk of sensitive, confidential or personal data breaches (83%)

Top three **barriers** associated with using or implementing AI

- Lack of talent and/or technical skills (38%)
- Concerns about regulatory, legal, ethical, compliance and other risks (36%)
- Technology implementation challenges (33%)

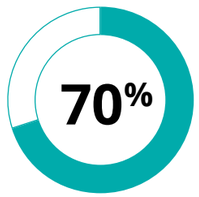


of Japanese organisations have a system for employees to raise concerns.



of employees in Japanese organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.

of Japanese organisations reported an increase in incidents received in the last financial year.



of Japanense organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Japan = 104

Spotlight on

South Korea

South Korea population: 51.8 million | GDP: $1.7 trillion USD

Top three expected **benefits** of effective AI governance

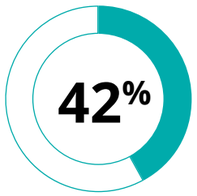
- Greater use of AI solutions as a result of higher trust (46%)
- Greater regulatory compliance (42%)
- Faster development of AI solutions across the organisation (40%)

Top three concerns about **risks** associated with using AI

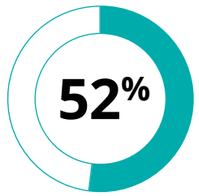
- Security vulnerabilities: risk of hacking / cyber (85%)
- Surveillance: invasion of privacy due to pervasive surveillance (85%)
- Regulatory burden: the extent of reporting or process requirements associated with using AI solutions (83%)

Top three **barriers** associated with using or implementing AI

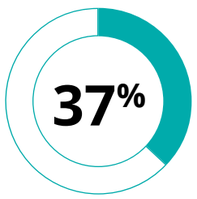
- Technology implementation challenges (35%)
- Lack of strategy and vision for AI implementation (33%)
- Concerns about regulatory, legal, ethical, compliance and other risks (31%)



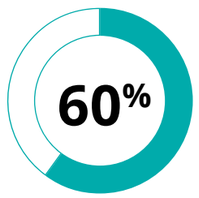
of South Korean organisations have a system for employees to raise concerns.



of employees in South Korean organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.



of South Korean organisations reported an increase in incidents received in the last financial year.



of South Korean organisations are hiring people with the required skills to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Korea = 52

Spotlight on

New Zealand

New Zealand population: 5.2 million | GDP: $253 billions USD

Top three expected **benefits** of effective AI governance

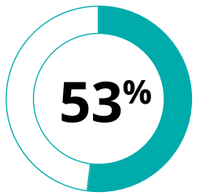
- Greater use of AI solutions as a result of higher trust (51%)
- Greater realisation of productivity benefits from AI solutions (42%)
- Improved reputation among customers (38%)

Top three concerns about **risks** associated with using AI

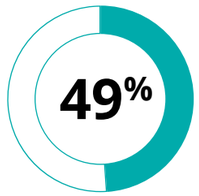
- Reliability and errors (87%)
- Security vulnerabilities: risks of hacking / cyber (85%)
- Privacy: risk of sensitive, confidential or personal data breaches from AI systems (85%)

Top three **barriers** associated with using or implementing AI

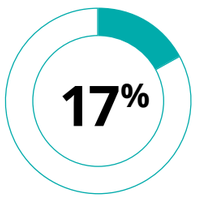
- Concerns about regulatory, legal, ethical, compliance and other risks (40%)
- Insufficient understanding of the technology and its potential (38%)
- Insufficient funding (36%)



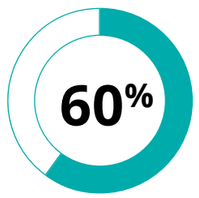
of New Zealand organisations have a system for employees to raise concerns.



Of employees in New Zealand organisations employees have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.



of New Zealand organisations reported an increase in incidents received in the last financial year.



of New Zealand organisations are partnering with a third party to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for New Zealand = 53

Spotlight on **Taiwan** (China)

Taiwan (China) population: 23.4 million | GDP: $756.59 billions USD

Top three expected **benefits** of effective AI governance

- Greater realisation of productivity benefits from AI solutions (64%)
- Faster deployment of AI solutions across the organisation (48%)
- Improved reputation among customers (44%)

Top three concerns about **risks** associated with using AI

- Security vulnerabilities: risks of hacking / cyber (85%)
- Surveillance: invasion of privacy due to pervasive surveillance and data collection capabilities (85%)
- Regulatory uncertainty: changing requirements that may result in being unaware of obligations (81%)

Top three **barriers** associated with using or implementing AI

- Technology implementation challenges (40%)
- AI use cases and investment disconnected from strategy (40%)
- Lack of appetite for innovation and/or insufficient experimentation (37%)

56% of Taiwanese organisations have a system for employees to raise concerns.

53% of employees in Taiwanese organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.

46% of Taiwanese organisations reported an increase in incidents received in the last financial year.

60% of Taiwanese organisations are hiring people with the required skills to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Taiwan (China) = 52

Spotlight on **Singapore**

Singapore population: 5.8 million | GDP: $501 billions USD

Top three expected **benefits** of effective AI governance

- Improved reputation among customers (43%)
- Higher levels of trust in the outputs or results from AI solutions (43%)
- Greater regulatory compliance (39%)

Top three concerns about **risks** associated with using AI

- Security vulnerabilities: risks of hacking /cyber (96%)
- Privacy: risk of sensitive, confidential or personal data breaches from AI systems (94%)
- Reliability and errors (94%)

Top three **barriers** associated with using or implementing AI

- Insufficient understanding of the technology and its potential (41%)
- Concerns about regulatory, legal, ethical, compliance and other risks (37%)
- Technology implementation challenges (31%)

67% of Singaporean organisations have a system for employees to raise concerns.

50% of employees in Singaporean organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.

35% of Singaporean organisations reported an increase in incidents received in the last financial year.

69% of Singaporean organisations hiring people with the required skills to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Singapore = 51

Spotlight on **Indonesia**

Indonesia population: 278.7 million | GDP: $1.37 trillion USD

Top three expected **benefits** of effective AI governance

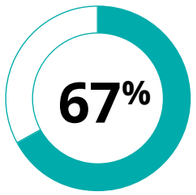
- Higher levels of trust in the outputs or results from AI solutions (67%)
- Faster development of AI solutions across the organisation (63%)
- Greater use of AI solutions as a result of higher trust (61%)

Top three concerns about **risks** associated with using AI

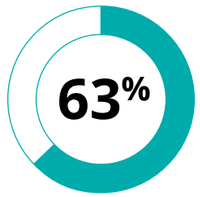
- Security vulnerabilities: risk of hacking / cyber (88%)
- Surveillance: invasion of privacy due to pervasive surveillance (84%)
- Legal risk and copyright infringement: legal liability or responsibilities associated with the use of data by AI solutions (83%)

Top three **barriers** associated with using or implementing AI

- Insufficient understanding of the technology and its potential (41%)
- Concerns about regulatory, legal, ethical, compliance and other risks (38%)
- Technology implementation challenges (e,g., maintenance, integration with existing systems) (36%)

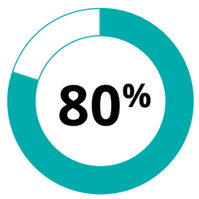


of Indonesian organisations have a system for employees to raise concerns.



of employees in Indonesian organisations employees have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.

of Indonesian organisations reported an increase in incidents received in the last financial year.



of Indonesian organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Indonesia = 64

Spotlight on **Malaysia**

Malaysia population: 33.4 million | GDP: $400 billion USD

Top three expected **benefits** of effective AI governance

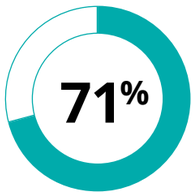
- Higher levels of trust in the outputs or results from AI solutions (65%)
- Greater use of AI solutions as a result of higher trust (63%)
- Faster development of AI solutions across the organisation (53%)

Top three concerns about **risks** associated with using AI

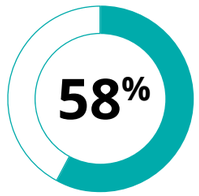
- Security vulnerabilities: risk of hacking / cyber (90%)
- Surveillance: invasion of privacy due to pervasive surveillance (84%)
- Privacy: risk of sensitive, confidential or personal data breaches from AI systems (82%)

Top three **barriers** associated with using or implementing AI

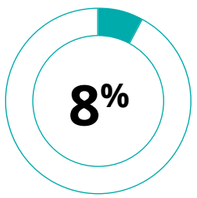
- Technology implementation challenges (e,g., maintenance, integration with existing systems) (51%)
- Insufficient understanding of the technology and its potential (37%)
- Lack of talent and/or technical skills (33%)



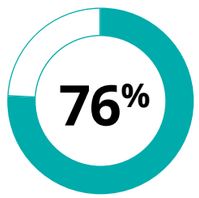
of Malaysian organisations have a system for employees to raise concerns.



of employees in Malaysian organisations employees have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.



of Malaysian organisations reported an increase in incidents received in the last financial year.



of Malaysian organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample Size for Malaysia = 51

Spotlight on Vietnam

Vietnam population: 100.3 million | GDP: $430 billion USD

Top three expected **benefits** of effective AI governance

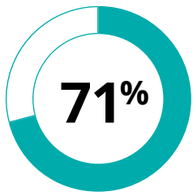
- Improved reputation among customers (67%)
- Greater realisation of productivity benefits from AI solutions (65%)
- Higher levels of trust in the outputs or results from AI solutions (62%)

Top three concerns about **risks** associated with using AI

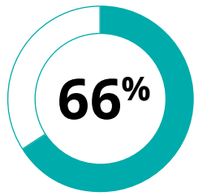
- Privacy: risk of sensitive, confidential or personal data breaches from AI systems (81%)
- Responsibility: lack of sense of responsibility among developer and users of AI systems, potentially leading to careless or unethical use (81%)
- Reliability and errors: incorrect outputs, unpredictability and potential for malfunction or unexpected behaviours (e.g. hallucinations) (79%)

Top three **barriers** associated with using or implementing AI

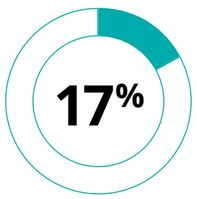
- Lack of talent and/or technical skills (56%)
- Concerns about regulatory, legal, ethical, compliance and other risks (40%)
- Lack of strategy and vision for AI implementation (37%)



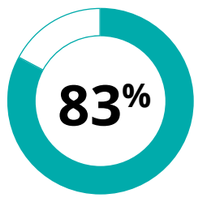
of Vietnamese organisations have a system for employees to raise concerns.



of employees in Vietnamese organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.



of Vietnamese organisations reported an increase in incidents received in the last financial year.



of Vietnamese organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Vietnam = 52

Spotlight on Thailand

Thailand population: 66.1 million | GDP: $515 billions USD

Top three expected **benefits** of effective AI governance

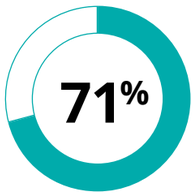
- Higher levels of trust in the outputs or results from AI solutions (55%)
- Greater use of AI solutions as a result of higher trust (51%)
- Faster deployment of AI solutions across the organisation (43%)

Top three concerns about **risks** associated with using AI

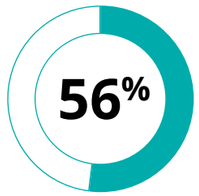
- Security vulnerabilities: risk of hacking / cyber (76%)
- Surveillance: invasion of privacy due to pervasive surveillance (75%)
- Legal risk and copyright infringement: legal liability or responsibilities associated with the use of data by AI solutions (71%)

Top three **barriers** associated with using or implementing AI

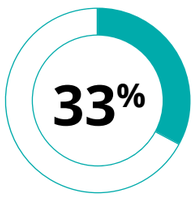
- Insufficient understanding of the technology and its potential (41%)
- Technology implementation challenges (37%)
- Concerns about regulatory, legal, ethical, compliance and other risks (35%)



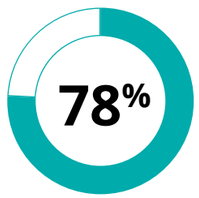
of Thai organisations have a system for employees to raise concerns.



of employees in Thai organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.



of Thai organisations reported an increase in incidents received in the last financial year.



of Thai organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Thailand = 51

Spotlight on **Philippines**

Philippines population: 115.8 million | GDP: $437 billions USD

Top three expected **benefits** of effective AI governance

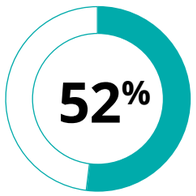
- Higher levels of trust in the outputs or results from AI solutions (67%)
- Greater use of AI solutions as a result of higher trust (52%)
- Improved reputation among customers (48%)

Top three concerns about **risks** associated with using AI

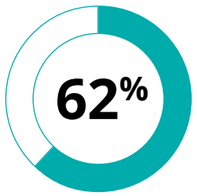
- Surveillance: invasion of privacy due to pervasive surveillance (90%)
- Security vulnerabilities: risk of hacking / cyber (85%)
- Privacy: risk of sensitive, confidential or personal data breaches from AI systems (83%)

Top three **barriers** associated with using or implementing AI

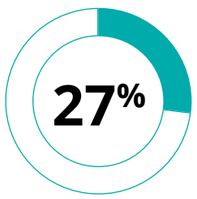
- Lack of talent and/or technical skills (38%)
- Technology implementation challenges (37%)
- Lack of strategy and vision for AI implementation (33%)



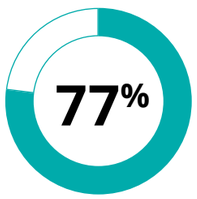
of Filipino organisations have a system for employees to raise concerns.



of employees in Filipino organisations have the required level of skills and capabilities to use AI solutions in an ethically and legally compliant way.



of Filipino organisations reported an increase in incidents received in the last financial year.



of Filipino organisations are upskilling existing staff to close the skills gap relating to ethical and compliant use of AI.

Note: Sample size for Philippines = 52

References

1 Deloitte (2024) “Generative AI in Asia Pacific”, https://www.deloitte.com/nz/en/services/consulting/perspectives/generative-ai-in-asia-pacific-may-2024.html

2 Ibid

3 Deloitte Access Economics (2024) “ACS Australia’s Digital Pulse 2024: Decoding the Digital Decade”, https://www.deloitte.com/au/en/services/economics/perspectives/acs-australias-digital-pulse-decoding-the-digital-decade.html

4 IBM (2024), “Cost of a data breach Report”, https://www.ibm.com/reports/data-breach

5 Capgemini Research Institute (2020), “AI and the ethical conundrum” Report, https://www.capgemini.com/news/press-releases/ai-and-the-ethical-conundrum-report/

6 Deloitte Centre for Regulatory Strategy (2024), “Generative AI: Application and Regulation in Asia Pacific”, https://www.deloitte.com/au/en/Industries/financial-services/analysis/generative-ai-application-regulation-asia-pacific.html

7 Deloitte (2024) State of AI in Enterprise, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf

8 Deloitte (2024) State of AI in Enterprise, https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consulting/us-state-of-gen-ai-q3.pdf

9 Haresamdram et.al, IEEE Access (2023), “Three levels of AI transparency”, https://ieeexplore.ieee.org/document/10042109

10 Ten areas of the business were presented to senior leaders: operations and/or production, marketing and sales, finance, human resources, customer service, research and development, information technology, management and administration, legal and compliance and logistics.

11 Deloitte (2023), Data privacy and security worries are on the rise, while trust is down. Consumer data privacy and security | Deloitte Insights

12 Deloitte Access Economics (2023), “Generation AI: ready or not, here we come!”, https://www.deloitte.com/content/dam/assets-zone1/au/en/docs/services/economics/deloitte-au-generation-ai-2023-160524.pdf

13 Schrage, M. et. Al, MIT Sloan Management Review (2023), “AI is helping companies redefine, not just improve, performance”; https://sloanreview.mit.edu/article/ai-is-helping-companies-redefine-not-just-improve-performance/

14 The third level of defense refers to a managing risks where the first level of defense are business users or direct managers, the second level of defense is risk and compliance teams and third level of defense is independent assurance

Contacts and contributors

For more information, to discuss the findings in this document or to be connected with the relevant person at at Deloitte, please contact:

Key contacts

Chris Lewin
Artificial Intelligence Lead Partner, Asia Pacific
chrislewin@deloitte.com

Dr. Elea Wurth
Trustworthy AI Lead Partner, Asia Pacific and Australia
ewurth@deloitte.com.au

John O’Mahony
Deloitte Access Economics Partner, Australia
joomahony@deloitte.com.au

Stuart Scotis
Transformation with Disruptive Technology, Partner, Deloitte Global
sscotis@deloitte.com.au

Silas Hao Zhu
Trustworthy AI, Partner, China
silzhu@deloittecn.com.cn

Toyohiro Sometani
Trustworthy AI Partner, Japan
toyohiro.sometani@tohmatsu.co.jp

Jessica Kim
Trustworthy AI Partner, South Korea
jessicakim@deloitte.com

Amy Dove
Trustworthy AI Partner, New Zealand
amydove@deloitte.co.nz

Jayant Saran
Trustworthy AI Partner, South Asia
jsaran@deloitte.com

Dishell Gokaldas
Trustworthy AI Partner, Southeast Asia
dgokaldas@deloitte.com

Chris Chen
Trustworthy AI Partner, Taiwan
chrisachen@deloitte.com.tw

Contributors

Nick Hull
Director
nhull@deloitte.com.au

Jennifer Wright
AP Eminence Director
jenniwright@deloitte.com

Sanjukta Mukherjee
AP Head of Research
sanjumukherjee@deloitte.com

Tory Rowley James
Senior Manager
trowleyjames@deloitte.com.au

Maud Dumont
Senior Analyst
madumont@deloitte.com.au

Dominic Behrens
Analyst
dobehrens@deloitte.com.au

Tara Naidu
Analyst
tarnaidu@deloitte.com.

Angela Watzdorf
Analyst
awatzdorf@deloitte.com.au

Deloitte.