All Actuaries Summit
Think bigger, live better
1-3 May 2024 • Gold Coast
Actuaries Institute.

AI in insurance and insuring AI: Navigating regulations, risks and opportunities

Prepared by Jonathan Cohen & Kushal Mithal

Presented to the Actuaries Institute
2024 All-Actuaries Summit
1-3 May 2024

Actuaries Institute
ABN 69 000 423 656
Level 2, 50 Carrington Street, Sydney NSW 2000
P +61 (0) 2 9239 6100 | actuaries.asn.au

Abstract

We explore three perspectives on the emerging relation between Artificial Intelligence (AI) and insurance, with a focus on how regulatory and legislative changes are likely to impact insurers' own use of AI, change the risk landscape for existing lines of business and introduce opportunities for new product innovations.

We cover:

1. **Impacts of emerging regulations and standards on insurance applications**: We explore the rapidly expanding legislative, regulatory and standards environment and some specific considerations for insurers.
2. **AI risks on existing insurance lines**: The use of and risks around AI by insureds will have ripple effects on established classes of business. We discuss the potential impacts of AI on a wide range of existing insurance classes, with a particular focus on liability-related classes including product liability, professional indemnity, directors & officers, and cyber liability.
3. **Insurance solutions for emerging AI risks**: We discuss the potential for insurance products that cover new and emerging AI risks, including existing emerging examples. This includes nascent product-warranty like cover, and cover for consequential losses arising from underperformance of AI models. We highlight several potential products and discuss some of the practical considerations around insurability and associated practical challenges including around product design, underwriting and claims.

Contents

1 Introduction

The use and development of Artificial Intelligence (AI) is expanding rapidly. AI presents opportunities for efficiency and improved service, with organisations increasingly looking at how they can deploy AI in their activities.

AI also presents new risks, with increasing concern around prevention of harm and ensuring measures are in place to address harm resultant from the use of AI.

Insurance plays a critical role in the economy, underwriting activity and providing a safeguard from the financial impact of loss. Insurers are in a unique position, impacted by AI in two fundamentally different ways:

- **Insurers' own use of AI** – Insurers have been leading the way for several years in using AI in their activities, with AI reshaping the entire insurance value chain.
- **Evolving risk profile of insured risks** – Insureds' use of AI is impacting the risk profile for existing lines of business and may have implications for insurance product offerings going forward. These may include the opportunity to underwrite new products that cover the unique risks of AI systems.

Insurers have a role to play in supporting the growth in AI and managing the risks that are emerging. Underwriting AI risks enhances the resilience of industry, and insurers may promote ethical and responsible adoption of AI as they engage with insureds through underwriting, monitoring and claims management processes.

This paper is written with two audiences in mind, members of the insurance industry, and individuals working in the AI industry more broadly that have an interest in the interaction of AI with insurance. Our aim is to highlight key issues around legislation, governance, and insurance relating to AI, rather than provide an exhaustive discussion of insurers' use of AI alone. We explore:

- The opportunities and risks associated with AI, including specific examples within the insurance industry.
- The fast expanding regulatory and legislative landscape, including emerging trends both locally and internationally.
- The nature of AI risks and how they manifest in existing lines that insurers underwrite, particularly liability classes.
- New product opportunities for insurers as risks of AI emerge, and practical considerations for new product development in this area.

2 AI history, usage and risks

AI capabilities have developed at a very fast rate over the past 20 years, with the introduction of ChatGPT in 2022 boosting interest in and adoption of AI by organisations.

What is AI?

Artificial Intelligence (AI) broadly refers to attempts to get computers to perform tasks that we would ordinarily associate with human intelligence.

We're yet to see universally accepted technical or legal definitions of AI (Digital.NSW, n.d.), and there has been considerable debate around how AI should be defined. The broad definition above covers all the cases we consider in this paper.

AI has rapidly become more capable, creating opportunities but also new risks

AI presents an abundance of opportunities for organisations and users, but also presents new risks.

In this section:

- We provide a quick recap of AI history
- Explore AI-related incidents and the risks related to use of AI
- Discuss how insurers are using AI.

2.1 A very brief recap of AI history

"Artificial Intelligence" (AI) broadly refers to attempts to get computers to perform tasks that we would ordinarily associate with human intelligence. It has been an area of research for almost as long as digital computers have existed, over 60 years. The intensity of focus and hype around AI has ebbed and flowed – we are currently living through a rapidly increasing hype and excitement period for AI.

The history of AI research can be roughly split into two broad areas:

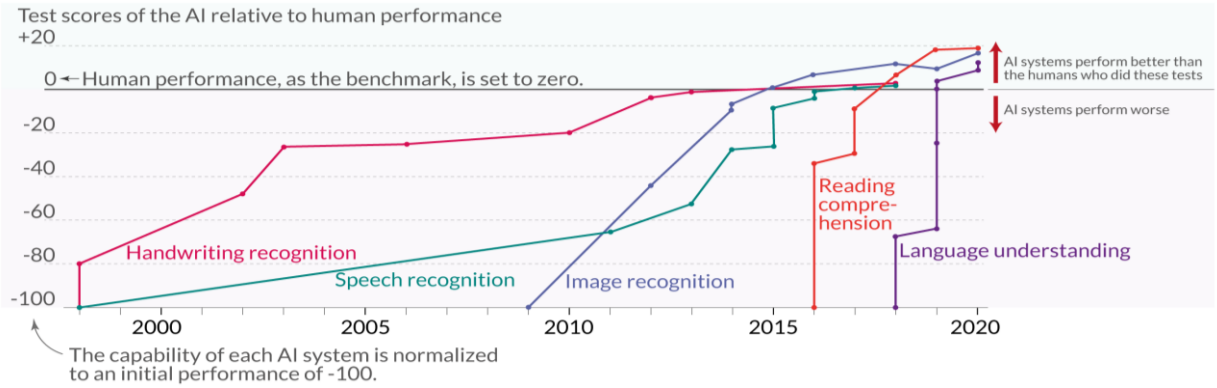
- Logic and deduction – aims to get computers to apply deductive reasoning in a relatively formal manner. This includes developments towards automated theorem provers and expert systems, which formed the basis for a prior peak of business interest in AI.
- Pattern recognition – aims to get computers to recognise patterns in the world around them, for example in images, sounds or text.

While this division is imperfect, with overlap between the two approaches to AI, it is a useful shorthand.

AI capabilities with respect to pattern recognition have received a significant boost from a period of discovery and improvements to neural networks, both in terms of how to structure them and how to train them on ever larger and more complex data sources. The invention of transformer networks and the attention mechanism in the seminal 2017 paper *"Attention is all you need"* provided a key inflection point towards the rise of large language models (LLMs) that have captivated public and business attention (Vaswani, et al., 2017).

To put the development in context, Figure 2.1 shows the progress over the past 20 years of performance in benchmark pattern recognition tasks, comparing AI systems to humans across five domains: handwriting recognition, speech recognition, image recognition, reading comprehension and language understanding (Roser, 2022).

Figure 2.1 – Test scores of AI relative to human performance



Source: OurWorldinData.org, *The brief history of artificial intelligence: The world has changed fast – what might be next?*

While no machine reliably performed better than the human level under standardised tests ten years ago, performance of AI systems is now better than humans across all tested domains (although performance outside of these standardised tests varies). Developments in reading comprehension and language understanding since 2015 have been rapid.

Current AI capabilities include impressive text to image generation, language recognition and generative AI that can be used to create new content, including text, images, audio and video.

In addition to rapidly advancing capabilities, the introduction of ChatGPT in November 2022 was a key driver of the increase in interest in generative AI (GenAI), with GenAI breaking free of the lab and entering the everyday lexicon of millions of people who use it for everything from generating computer code to writing mildly amusing limericks. Usage of ChatGPT has grown exponentially, with the conversational interface making AI immediately accessible to a large audience.

This has driven business attention to the opportunities presented by GenAI. Bloomberg Research forecasts the generative AI market will grow (AON, 2023) to $1.3 trillion over next 10 years, up from $40 billion in 2022.

2.2 How insurers are using AI

The insurance industry has been realising AI's potential for several years – improving customer experience, increasing efficiency and reducing costs. Applications for AI in insurance span a range of operational areas (Cohen & Wood, 2023). We summarise some of the impacts in Table 2.1.

Table 2.1 – Examples of use of AI by insurers

Process	Examples of use of AI
Distribution / sales	▪ AI-led efficiency improvements reducing the turnaround time for quotes ▪ Personalised recommendations to customers, often with cross-selling across multiple products, which are better calibrated to individual customers through use of GenAI ▪ Automation of dealing with simple customer enquiries using AI-based chatbots ▪ AI used to reduce the number of questions in quote forms, and in some cases used to pre-fill questions

Process	Examples of use of AI
Underwriting	▪ Swiss Re's Magnum platform provides automated risk assessment and underwriting capability for life and health insurance, reducing application process time and streamlining operations (Swiss Re, 2024) ▪ Analysis of new, large datasets (e.g. satellite images, vehicle telematics data) to enhance accuracy of risk assessment to support better pricing ▪ Where underwriting processes are still very manual (e.g. commercial lines), AI used to quickly extract information from documents
Pricing and reserving	▪ Analysis of large datasets and new data sources to better price risk ▪ Complex pricing models to better discriminate between risk groups, with more scope for personalised pricing (Gallagher Bassett, n.d.) ▪ Automated reserving techniques expedite estimation of reserves as experience emerges
Claims assessment and management	▪ Automated claims data entry – natural language models are being used to extract key information from documents submitted by claimants, which are automatically identified and converted into a structured format, speeding up the process and reducing human error ▪ Automated claims triage – claims automatically sorted according to information provided to then be handled accordingly, for example to specific teams for more complex claims ▪ Tech start-up Ravin AI's product offers automated motor vehicle damage and repair cost estimates using image recognition applied to customers' mobile phone images (Ravin AI, n.d.) ▪ Allianz's Neptune AI tool automates the assignment of marine claims to adjusters when notified, and provides real-time KPIs to claims managers, replacing manual claim assignment (Allianz, 2023) ▪ Fraud detection – machine learning methods have been used for fraud detection for many years, with the sophistication and automation behind these increasing as detection tools become more powerful with the use of AI ▪ Improvements to chatbots following recent advancements in large language models, such as those underpinning ChatGPT, with enhanced capability and performance

The use of AI by insurers, like any other technology, is subject to regulatory obligations and legislative requirements.

We explore these requirements and specific considerations for insurers in Section 3.

2.3 The use of AI comes with risks

While there is a lot of excitement around the potential for AI to enhance productivity and business outcomes, it brings with it a range of new and modified risks. AI systems are imperfect, they ingest and transform personal information, they are vulnerable to modification and misuse by malicious users, and they can produce outputs that are biased against certain groups of people.

Table 2.2 provides a brief summary of key areas of risk associated with AI systems.

Table 2.2 –Risks related to AI models

Risk	Definition
1. Hallucination and false information	False information, incorrect or misleading results generated by an AI model
2. Bias	Unfair or biased output generated by an AI model resulting in discrimination, or perpetuation of societal or political biases by an AI model
3. Privacy infringement	Reveal or leak of sensitive training data by an AI model
4. Copyright violations	Training of an AI model, without permission, on data that is protected by copyright laws, or when the output of an AI model contains copyrighted material, or mimics copyrighted material, without permission
5. Harmful content	Offensive or malicious content produced by an AI model (mainly applicable to GenAI)

We summarise four recent incidents below to provide a more tangible view of risks related to AI.

False output

Two attorneys in the US were found to have filings in a lawsuit against an airline (Mata v Avianca) that included references to past court cases that were thought to be real but were hallucinated by ChatGPT (ABS, 2023).

The court dismissed their client's case, fined the lawyers and their legal firm, and ordered them to notify each judge falsely identified as the author of the fake case rulings about the sanction.

A study found legal hallucinations are pervasive – hallucination rates range from 69% to 88% in response to specific legal queries for state-of-the-art language models (Dahl, Magesh, Suzgun, & Ho, 2024).

Copyright infringement

In December 2023, the New York Times sued OpenAI and Microsoft for copyright infringement, contending that millions of articles published by The Times were used to train automated chatbots that now compete with the news outlet as a source of reliable information. Similar lawsuits have been filed against OpenAI by groups of authors, on similar themes of ChatGPT being built on the back of IP belonging to others (Grynbaum & Mac, 2023).

OpenAI's response claims that the lawsuit is without merit, including stating their position that training a model using publicly available internet material is fair use, and that verbatim regurgitation of some articles is a rare bug that they're working to eliminate (OpenAI, 2024).

The UK regulator is also scrutinising the lawful basis for web scraping to train GenAI models (UK Information Commissioner's Office, 2024).

Algorithmic error

A proposed class action lawsuit filed in November 2023 claims that UnitedHealth Group, the largest health insurance provider in the US, used an AI algorithm called *nH Predict* that wrongfully denied elderly patients' claims for extended care such as nursing facility stays (Laney, 2023).

The lawsuit claims that approximately 90% of these decisions are reversed when the denials are appealed to federal administrative law judges, highlighting the alleged inaccuracy of the algorithm.

Model accuracy

Zillow, a US-based online real estate company, had made large investments in iBuying (instant-Buying, a strategy of very quick turnaround purchases directly from sellers without third-party real estate agent involvement) on the back of an algorithms they referred to as *Zestimates* to predict house prices.

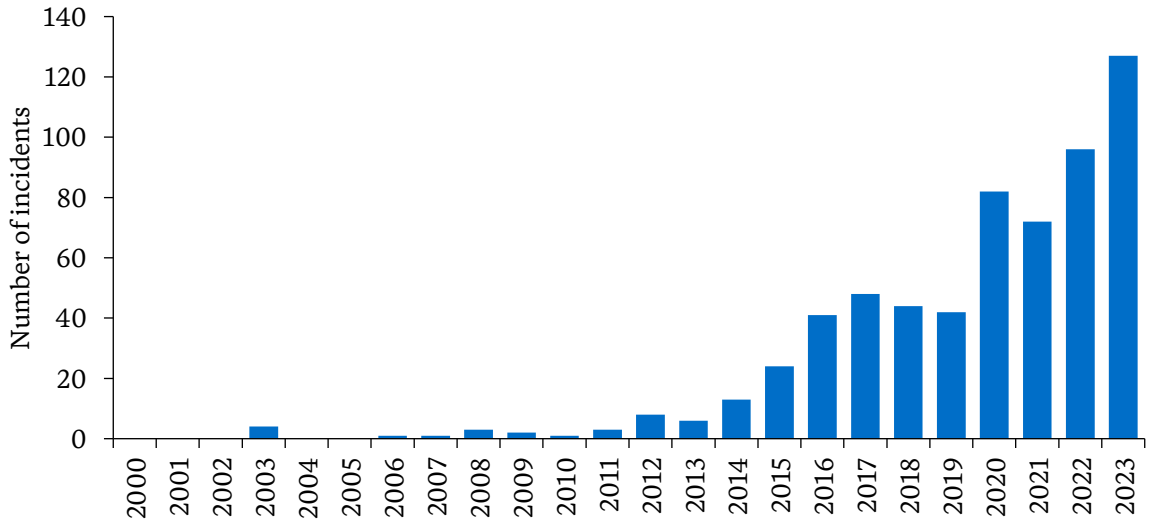
In 2021, the company announced it would be shutting down the algorithm-based buying and selling arm of the company and exit the iBuying business, writing off $569m in lost inventory value and laying off 25% of its staff (Langone, 2021).

Zillow attributed the losses to its inaccurate predictions of home values, with the effects of the pandemic contributing to the model's accuracy troubles (Olavsrud, 2023). The CEO noted an observed error rate that was far more volatile than expected (Stokel-Walker, 2021).

The AI Incident Database[1] collects, verifies, and classifies events reported by users in which harm was either caused or almost caused by AI (Surfshark, 2023).

Figure 2.2 shows the number of incidents by calendar year sourced from the incident database, highlighting a sharp increase in the number of AI incidents after 2019, which has continued to grow.

Figure 2.2 – Number of AI incidents over time



An increasing trend in the number of incidents reported can be caused by increasing use of AI, an increase in the rate of harm, or an increase in the rate of reporting of harm to the database. We'd expect the overall trend is likely a combination of these, but haven't attempted to attribute the drivers.

[1] AI Incident Database accessed at: https://incidentdatabase.ai/

3 Regulation, legislation and other requirements

The past few years have seen a rapid increase in the use of AI, more recently driven by advances in GenAI. This has come with a heightened concern around the ethical and responsible use of AI – preventing harm and ensuring there are measures in place to address harm resultant from the use of AI.

For insurers, the risks of harm from AI feature prominently on regulators' radar:

- ASIC's key projects per their 2023-2027 corporate plan include a review of the risks of consumer harm flowing from the potential misuse of consumer data, algorithms and AI in financial services, along with examination of how institutions are seeking to mitigate risks (ASIC, 2023)
- APRA's 2023-2024 corporate plan notes the growing use of AI (including GenAI) is transforming how financial services are structured and delivered to end users, and this amplifies risks about the potential misuse of AI, as well as data privacy and security (APRA, 2023).

In this section, we discuss:

- Provisions in existing broadly applicable regulations and legislation that relate to the use of AI
- International developments in a fast-developing global regulatory environment
- Emerging trends in regulation in Australia
- The role of ethical AI principles, AI standards and AI governance frameworks
- Technical approaches for responsible AI.
- Specific considerations for insurers' use of AI

3.1 Provisions in existing broadly applicable regulations and legislation

While there is significant focus on developing new regulations for AI both internationally and locally, and some debate around the need for AI-specific legislation, a fundamental principle that should be front of mind is that Australian legislation applies to AI in the same way that it does to all other technologies – that is, legislation is technology-neutral. This includes legislation relating to privacy, consumer rights, data security and other areas. At the time of writing, there have been no laws passed in Australia that apply specifically to AI technologies but, nonetheless, the use of AI by organisations is subject to comprehensive legislative requirements.

Table 3.1 shows the existing laws that may apply to key risks relating to AI technologies, drawing on the work by Solomon and Davis (2023).

Table 3.1 – Existing laws that may apply to AI-related harms

Harms	Privacy laws	Australian Consumer Law	Anti-discrimination Law	Risk management obligations	Data security, confidentiality or IP laws / obligations	Other
Misuses data or personal information	✔			✔	✔	
Produces an incorrect output	✔	✓				
Provides misleading advice or information		✔				
Provides unfair or unreasonably harsh treatment		✔				
Discriminates based on a protected attribute			✔			
Excludes an individual from access to a service			✔			✓
Restricts freedoms such as expression, association or movement						✓
Causes physical, economic or psychological harm		✓				✓

✓ Laws or obligations that may apply to common harms from an AI system

✔ Laws or obligations that may apply to common harms from an AI system, of particular significance to insurers' use of AI

Note: Other laws/obligations include essential service obligations, human rights acts or charters, negligence (if breach of duty of care causing harm), and work, health and safety laws.

3.2 International developments

The regulatory environment is fast-evolving across many jurisdictions. In this section, our aim is to highlight a few key developments in other jurisdictions rather than provide an exhaustive discussion of the global regulatory landscape.

The Productivity Commission expects to some extent for Australia to be a 'regulation taker', as a significant amount of AI technology is likely to be imported from overseas where it has been developed in accordance with the source country's legislation, and domestic developers are likely to seek sales in overseas markets (Productivity Commission, 2024). As such, international developments may be a leading indicator for the direction that local legislation takes.

Approaches to regulating AI differ significantly across different jurisdictions

The EU has approved legislation to regulate AI, while the US, UK and Singapore currently lean towards guidelines and standards rather than laws to govern AI.

Table 3.2 summarises developments in AI legislation in Europe, the UK, the US and Singapore.

Table 3.2 – Approaches to AI legislation and regulation in other jurisdictions

Country	Overview of approach
Europe	The EU parliament on 13 March 2024 approved the Artificial Intelligence Act (AI Act), which was endorsed by EU member states in December 2023. The AI Act represents the first legal framework on AI globally, aiming to maintain ethical standards around the use of AI. The AI Act follows a risk-based approach, with 4 levels of risk for AI systems: unacceptable, high risk, limited risk, and minimal risk. All AI systems that are considered a clear threat to the safety, livelihoods and rights of people will be banned (e.g. social scoring by governments). All other AI systems (that are not unacceptable risk) are risk-rated and subject to regulation that is based on the risk rating. AI systems intended to be used for risk assessment and pricing in relation to natural persons in the case of **life and health insurance** fall under the definition of high-risk AI systems of the AI Act (Annex III of the AI Act). The Act aims to strike a balance between protecting rights and encouraging innovation. The Council of the European Union is expected to officially adopt the text by the end of April 2024. The ban on prohibited uses will apply within six months, while general-purpose AI rules including governance will take effect in early 2025.
United Kingdom	The UK government published its response to consultation on AI regulation in February 2024 (UK Department for Science, Innovation & Technology, 2024), explaining its approach to regulation of AI in the UK. The government's proposed framework outlined five cross-sectoral principles that the UK's existing regulators are to interpret and apply within their remit: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress. The response acknowledged that, while the current response does not put forward binding statutory measures at this stage, challenges posed by AI may ultimately require legislative action once understanding of AI risk has matured.
United States	The Biden Administration passed an Executive Order (EO) in October 2023 (The White House, 2023) on Safe, Secure and Trustworthy Artificial Intelligence. The EO is guided by eight principles and priorities, with the National Institute of Standards and Technology (NIST) tasked with the development of guidelines, standards and best practices for "developing and deploying safe, secure and trustworthy AI systems" (Neill, Hallmark, Jackson, & Diasio, 2023). The EO does not categorise applications by risk as does the EU approach (Productivity Commission, 2024). In March 2024, it was announced that the White House Office of Management and Budget (OMB) is issuing a government-wide policy to mitigate risks of AI and harness its benefits, leading on from the EO in October 2023 (The White House, 2024). Federal agencies will be required to implement concrete safeguards when using AI, including a range of mandatory actions to assess, test, and monitor AI's impacts on the public, mitigate the risks of algorithmic discrimination, and provide the public with transparency into how the government uses AI. The OMB's guidance directs agencies to expand and upskill their AI talent. The White House also plans to hire AI professionals to promote the safe use of AI.

Country	Overview of approach
Singapore	Singapore launched the world's first Model AI Governance Framework in 2019 (subsequently updated in 2020). They also published their National AI Strategy (NAIS) in 2019 (updated to NAIS 2.0 in 2023). Singapore has not enacted AI-specific legislation, preferring instead to issue nonbinding guidelines and recommendations (Chng & Jones, 2024). NAIS 2.0 states the government aims to maintain a regulatory environment for AI that is pro-innovation while ensuring appropriate guardrails (Government of the Republic of Singapore, 2023). As part of this strategy, the government aims to: ▪ Regularly review and adjust frameworks like the Model AI Governance Framework to reflect emerging principles, concerns and technological developments ▪ Continue working translating guidelines into appropriate technical standards, tools and services, supported by policy measures such as regulatory sandboxes ▪ Design interventions that are risk-based, recognising different risk threshold and context-specific risk management approaches for different applications ▪ Consider updates to broader standards and laws.

3.3 Emerging trends in AI regulation in Australia

In June 2023, the government opened a consultation on *Safe and responsible AI in Australia* (Australian Government, 2023), seeking advice on steps the government can take to mitigate any potential risks of AI and support safe and responsible AI practices. The government published its interim response to this consultation in January 2024 (Australian Government, 2024).

A risk-based approach to AI guardrails

The government found consensus among submissions that a risk-based approach to adopting AI guardrails is appropriate. A risk-based regulatory framework imposes regulatory requirements that are commensurate to the level of risk posed by different AI development and applications. There are challenges to adopting a simple tiered risk-level categorisation in practice – for example, the Actuaries Institute's submission proposed risk-based regulation be targeted to specific situations rather than adopting the same interventions across vaguely defined risk levels, in part to address oversimplification and difficulty in categorising situations with multiple impacts (Actuaries Institute, 2023).

The government's response also identified that:

- Many applications of AI do not present risks that require a regulatory response, and there is a need to ensure the use of AI in low-risk applications is largely unimpeded
- The current regulatory framework does not sufficiently address risks presented by AI, particularly for high-risk applications and frontier models[2]
- Existing laws do not adequately prevent AI-facilitated harms before they occur, with more work needed to ensure there is an adequate response to harms after they occur.

[2] Frontier models refer to newer, powerful AI models that exceed the capacity of previous models and can generate new content quickly and easily (Australian Government, 2024).

A voluntary AI safety standard and potential strengthening of existing laws

The government has indicated it is working to strengthen existing laws to address known harms with AI, including implementation of privacy law reforms, a review of the Online Safety Act 2021, and introduction of new laws relating to misinformation and disinformation (Australian Government, 2024). The government is considering amendments to existing laws and a new dedicated legislative framework for introducing mandatory safety guardrails in high-risk settings.

Immediate actions flagged in the government's response include working with industry to develop a voluntary AI Safety Standard and develop options for voluntary labelling and watermarking of AI-generated materials, and establishing an expert advisory body.

On 26 March 2024, the Senate resolved that the *Select Committee on Adopting Artificial Intelligence (AI)*, be established to inquire into and report on the opportunities and impacts for Australia arising out of the uptake of AI technologies in Australia (Parliament of Australia, 2024).

Risks created by or amplified by AI are already to some extent covered under the existing regulatory framework. Where specific risks are not sufficiently addressed by the existing framework, the government's current approach is to first develop voluntary standards, strengthen existing laws and then consider where AI-specific legislation may be required, particularly for high-risk applications.

3.4 Principles, standards and governance frameworks

Under a mostly technology-neutral regulatory framework, AI governance is currently managed by organisations through their broader risk management frameworks. These frameworks may draw on:

- Ethical AI Principles: broad guidelines for how AI systems can be ethically developed and deployed, allowing context-specific interpretations and operationalisation.
- AI Standards: provide guidance towards best practice in AI. Organisations can gain certification to demonstrate conformity with some standards.
- Government frameworks: translate principles into recommendations that can practically be adopted by organisations to deploy AI responsibly.

Ethics principles

AI ethics principles are published to promote the use of AI that is trustworthy. Despite being voluntary, we see value in these principles guiding risk management framework updates to ensure AI risks are appropriately accounted for. The principles are intended to complement existing regulations.

While a consistent core set of ethical principles is emerging, there is lots of variation across jurisdictions and industry sectors (Singapore PDPC, 2020a). Commonly referenced examples include:

- OECD's five value-based AI Principles (OECD, 2019).
- Ethics principles within Singapore's AI governance testing framework (Singapore PDPC, 2020b)
- The US National Institute of Standards and Technology (NIST) building blocks of AI trustworthiness, (US NIST, n.d.).

Locally, the government published Australia's Artificial Intelligence Ethics Framework in 2019. The example below shows the eight AI Ethics Principles published as part of the framework, designed to ensure safer, more reliable and fairer outcomes from the use of AI (Department of Industry, Science and Resources, 2019).

Example: Australia's eight AI Ethics Principles

1. Human, societal and environmental wellbeing - AI systems should benefit individuals, society and the environment
2. Human-centred values - AI systems should respect human rights, diversity, and the autonomy of individuals.
3. Fairness - AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.
4. Privacy protection and security - AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.
5. Reliability and safety - AI systems should reliably operate in accordance with their intended purpose.
6. Transparency and explainability - There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI, and can find out when an AI system is engaging with them.
7. Contestability - When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
8. Accountability - People responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

Large insurers may have ethics frameworks that form part of their risk management strategy. The AI Ethics Principles can serve as a guide to updating these frameworks towards responsibly developing and implementing AI.

Standards

Many government agencies, standards bodies and professional bodies have published standards to offer guidance to the use of AI, often across common themes of promoting transparency, explainability, trustworthiness and ethical use of AI.

Examples include:

- The International Organization for Standardization (ISO) standards
- The Institute of Electrical and Electronics Engineers (IEEE) standards for Autonomous and Intelligent Systems (AIS).

The government's interim response to its 2023 *Safe and responsible AI consultation* demonstrates that even with a voluntary AI Safety Standard, changes to existing legislation and/or new regulation to address gaps in AI regulation are likely (Australian Government, 2024).

The effectiveness of voluntary standards is uncertain given interpretations and adherence will vary across organisations. International standards that organisations can demonstrate conformity to have the potential to offer significant value to risk assessment for insurers. As such, we discuss the ISO standards in more detail below.

ISO standards

The International Organization for Standardization (ISO) is an independent organisation made up of members from national standards bodies of 170 countries. The ISO brings together experts from these member countries to develop and publish international standards that provide guidance towards best practice in several fields, including AI (ISO, n.d.).

Table 3.3 summarises two ISO standards that relate to risk management and use AI.

Table 3.3 – ISO standards relating to AI

Standard	Description
ISO/IEC 42001:2023 Information technology, Artificial intelligence, Management system (ISO, 2023)	▪ For organisations of any size involved in developing, providing, or using AI-based products or services. ▪ Specifies *requirements* for establishing, implementing, maintaining and continually improving an AI management system within organisations. ▪ Organisations can receive ISO certification for this standard. The ISO believes that conforming with the requirements of the standard can provide evidence of an organisation's responsibility and accountability regarding its role with respect to AI systems. ▪ The standard aims to help organisations responsibly perform their role with respect to AI systems, covering: – **Understanding the context** of an organisation – Issues relevant to the organisation, needs and expectations of interested parties, scope of the AI management system – **Leadership** – Roles, responsibilities, establishment of an AI policy – **Planning** – Actions to address risks and opportunities, AI objectives and planning to achieve them, planning of changes to the system – **Support** – Resources, competence, communication, etc. – **Operation** – Operational planning and control, assessment and treatment of the organisation's AI risks, AI impact assessment – **Performance evaluation** – Monitoring, measurement, analysis and evaluation, internal audit of the AI system, management review – **Improvement** – Continuous improvement for suitability, adequacy and effectiveness of the AI management system.
ISO/IEC 23894:2023 Information technology, Artificial intelligence, Guidance on risk management (ISO, 2023)	▪ Provides *guidance* on how organisations that develop, produce, deploy or use products, systems and services that utilise AI can manage risk specifically related to AI. ▪ Aims to assist integration of risk management into AI-related activities and functions, and describes processes for the effective implementation and integration of AI risk management.

The ISO AI standards could turn out to very useful to insurers for:

- **Managing AI risk within the organisation**
  Insurers' risk management frameworks can be enhanced by aligning to international standards, particularly in identifying and enhancing areas where the existing systems and processes may be deficient.
- **Assessing risk as part of underwriting criteria**
  Insurers can have more confidence in systems and processes around managing AI risk of organisations that are ISO certified. ISO/IEC 42001 certification would demonstrate an insured's responsibility and accountability regarding its role with respect to AI systems and could be an important rating factor in insurers' underwriting processes.

While the adoption of standards is voluntary, they have the potential to provide significant improvement for insurers' own risk management processes, and in their assessment of insureds' riskiness in relation to their management of AI risk.

Governance frameworks

Governance frameworks translate ethical principles into practical recommendations that organisations can readily adopt to deploy AI responsibly. Examples of frameworks include:

- US National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (US NIST, n.d.)
- Singapore Model Artificial Intelligence Governance Framework (Singapore PDPC, 2020a)
- NSW AI Assurance Framework (NSW Government, 2022).

Organisations may mold their risk management frameworks around published principles, standards and governance frameworks. In the next section, we discuss what practical approaches to implementing responsible AI might look like.

3.5 Technical approaches for responsible AI

In this section, we discuss some of the growing range of tools being developed towards operationalising responsible AI, which are the practical considerations that sit under the broader aspiration that ethics principles provide.

Table 3.2 provides examples of some objectives of responsible AI and potential tools and/or measures that can be used in achieving these, picking out some of the methods put forward by the CSIRO (n.d.) and Ferrara (2023). The table is not intended to represent an exhaustive list, but to highlight some of the commonly used approaches.

Table 3.4 – Objectives and potential technical approaches for responsible AI in practice

Objective	Examples of technical approaches
Mitigate bias and discrimination / enhance fairness	▪ Selecting appropriate fairness metrics to explicitly measure fairness, such as demographic parity (compare likelihood of positive outcomes across protected attributes), equalised odds (measure the quality of true positive and false positive rates between across protected attributes), etc. ▪ To mitigate algorithmic discrimination, there are techniques that can be applied at different stages of the modelling process, including: – Pre-processing data to identify and address biases in the data before training the model (e.g. oversampling, under-sampling, synthetic data generation) – Model selection considerations, such as addition of fairness constraints or employing regularisation that penalises discriminatory predictions, during model training – Post-processing decisions, which adjusts output after the model is trained to remove unwanted bias in deployment, such that fairness metrics as described above are met

Objective	Examples of technical approaches
Enhance privacy	▪ Mitigate the risk of sensitive training data from being revealed using techniques such as homomorphic encryption, which enables computation on encrypted text which results in the same outcome as if performed on the original data ▪ Techniques such as differential privacy help preserve privacy by adding tuned amounts of random noise to the dataset
Enhance model explainability	▪ Use of methods to explain predictions include Local Interpretable Model-Agnostic Explanations (LIME) and Shapley Additive exPlanations (SHAP) values ▪ There are many commercial offerings (e.g. from IBM, Google, etc.) to aid interpretation, often including methods to visualise the relationship between input variables and AI model outputs which sit under the '*explainable AI*' umbrella
Cyber security	▪ Several tools are available to assess AI models for vulnerabilities to cyber security risks, for example the risk of data breaches through AI models.

3.6 Specific considerations for insurers' use of AI

Insurance is highly regulated in Australia

Insurers already have sophisticated risk management frameworks and processes, and are subject to a stringent regulatory regime. These regulations are technology-agnostic, and extend to the use of AI by insurers. As such, insurers will need to ensure that their use of AI continues to meet applicable requirements.

Regulation of insurers is mainly within the purview of two government bodies (Andrews & Bartlett, 2024):

- Australian Securities and Investments Commission (ASIC) – corporate regulator, responsible for the administration and enforcement of the Insurance Contracts Act 1984 (Cth), whose role is to ensure insurers operate efficiently, honestly and fairly.
- Australian Prudential Regulation Authority (APRA) – prudential regulator, responsible for administration and enforcement of the Insurance Act 1973 (Cth), including licensing and regulatory oversight to protect interests of policyholders and ensuring financial stability.

In addition, the Australian Competition and Consumer Commission (ACCC) can take action against private health insurers for breaking competition and consumer laws, and against general insurers for breaking competition law (ACCC, n.d.).

The insurance industry also commits to deliver certain standards of practice through various codes of conduct, such as the General Insurance Code of Practice, the Life Insurance Code of Practice, etc.

The use of AI in insurance sits under a comprehensive regulatory framework, and as such insurers are already expected to manage risks related to their use of AI under their current regulatory obligations.

> ***Responsibility towards good governance is not changed just because the technology is new****….*
> *And businesses, boards, and directors shouldn't allow the international discussion around AI regulation to let them think AI isn't already regulated. Because it is. For this reason, and within our remit, ASIC will continue to act, and act early, to deter bad behaviour whenever appropriate and however caused.*
>
> Joe Longo, ASIC Chair, Keynote address at UTS Symposium (2024)

For example, a risk management framework is a requirement under APRA's Prudential Standard *CPS 220 Risk Management*, which applies to all APRA-regulated institutions (which includes insurers).

Example: APRA Risk Management Framework (APRA, 2019)

The risk management framework (RMF) is the totality of systems, structures, policies, processes and people within an institution that identify, measure, evaluate, monitor, report and control or mitigate all internal and external sources of material risk.

APRA stipulates eight requirements of the RMF (at a minimum), which include:

- A risk management strategy
- Policies and procedures supporting clearly defined and documented roles, responsibilities and formal reporting structures for the management of material risks throughout the institution,
- A designated risk management function
- An Internal Capital Adequacy Assessment Process (ICAAP)
- A management information system for measuring, assessing and reporting on all material risks across the institution
- A review process to ensure that the risk management framework is effective in identifying, measuring, evaluating, monitoring, reporting, and controlling or mitigating material risk

Insurers' risk management frameworks may form the foundation of their approach to appropriately govern and manage the use of AI through the organisation, with international frameworks and standards providing a reference point for areas that may need strengthening or modification.

Like all entities, insurers are subject to compliance with the current regulatory framework in their own use of AI. As the use of AI across the insurance value chain continues to increase, it is critical that insurers understand their legal obligations, and have processes and measures in place to ensure compliance with these.

Robust risk management is needed across the insurance value chain

In Section 2.2 we discussed how insurers are using AI across the different parts of the insurance value chain. Insurers need to ensure that risk relating to the use of AI is appropriately managed across the value chain, in cases where:

- *Use of AI to some extent will be covered under the risk management framework for insurers – but there may be gaps to be addressed to ensure AI risk is appropriately managed*

  Pricing and underwriting have traditionally been areas that employ sophisticated analytics models. As such, insurers' risk management frameworks typically already include measures to address risks relating to the use of these models, which extend to the use of AI.

  For example, if the use of AI in insurance pricing unlocks the ability to use new data sources or variables, under the existing framework requirements, insurers will need to continue to ensure that the models continue to comply with anti-discrimination laws, regardless of the model type.

- *Operational areas in which use of advanced analytics and AI is relatively new*

  Operational areas outside of pricing and underwriting have traditionally had less mature use of data and models, and consequently are likely to have less visibility in risk management frameworks. Insurers should evaluate where their risk management frameworks require bolstering to ensure that systems and processes are in place to manage risks related to the use of AI in these areas.

Use of AI is subject to obligations under consumer and anti-discrimination law

Consumer Law obligations

The Australian Consumer Law (ACL) establishes consumer protections, which include unfair contract terms, unfair business practices, and misleading or deceptive conduct. The ACCC can take action against private health insurers for breaking consumer laws, while general insurers and other financial service providers are regulated by ASIC under consumer law (ACCC, n.d.).

Insurers need to ensure that their use of AI does not impede compliance with ACCC and ASIC requirements relating to Australian Consumer Law. Insurers' consumer law obligations include not misrepresenting:

- When an AI system is used
- How the output from the use of AI was determined
- Accuracy of outputs from an AI model.

Anti-discrimination laws

Anti-discrimination laws make it unlawful to discriminate on the basis on a number of protected factors (Attorney-General's Department, n.d.).

There are exemptions in the legislation for general insurers relating to discrimination in certain circumstances when reasonable and based on actuarial or statistical data, for example in pricing insurance policies.

Insurers need to ensure that their use of AI does not result in a breach of legislative requirements:

- For processes like underwriting and pricing, this means ensuring the use of AI does not inadvertently introduce discrimination across protected variables
- For all uses outside of processes where exemptions might apply, insurers' obligations to anti-discrimination laws are no different to all other organisations.

3.7 Regulation outside the insurance industry

There is greater uncertainty in the governance practices and processes around the use of AI in other industries, relative to insurers who have a history of regulatory scrutiny around their management of model risk. The regulation of the use of AI outside insurance, and indeed outside financial services, varies materially by industry.

Insurers need to be aware of the risks surrounding development and use of AI in other industries, and shouldn't assume that practices in other industries are as robust as their own. This may lead to significant risk in existing lines of insurance business that insurers write, for example around product liability. We discuss the impacts of AI on existing lines of business in the next section, including risks and how insurers are responding to these, and follow this up with a discussion of new product opportunities for insurers in Section 5.

4 Impacts on existing insurance products

In this section we address the ripple effects of AI on existing lines of business.

The risk profile for certain lines of business written will be impacted by insureds' use of AI, with likely impacts on both claim frequency and severity. We discuss:

- The potential impacts of AI on insurance lines of business, with a discussion of the complexities for liability products, including where existing policies may provide cover for AI risk despite not specifically being designed to do so (silent cover)
- Relevant international developments and examples, including the EU's Artificial Intelligence Liability Directive, which seeks to update the EU liability framework to make it easier for individuals to bring claims for harms caused by AI

How insurers might respond to emerging AI risk by excluding coverage or actively providing cover for AI risk, which leads into our discussion of new product opportunities in Section 5.

4.1 Overview

The increasing rate of development and use of AI, by insureds and more generally, has meant that insurers are facing challenges in managing AI risk for existing lines, including:

- A changing in risk profile with increasing use of AI, creating additional uncertainty in claims experience
- Low visibility of coverage/exposure due to varying rates of AI adoption among insureds, coupled with a fast-changing technological environment
- Limited exclusions and/or ambiguous wording in relation to coverage for AI use by insureds in existing policies, with potential for significant silent cover exposure.

Table 4.1 provides an overview of the impacts of AI specific to seven insurance products.

We follow this up with a more detailed discussion of the risks for liability products (1 to 4 in Table 4.1) to highlight the complexities in proving liability with the use of AI.

Table 4.1 – Overview of impact on existing lines of business

	Insurance product	Impacts of AI
1	Directors and Officers	A heightened risk of claims for financial loss due to reliance on advice/outputs from AI models as use of AI in corporate decision-making increases.
2	Professional Indemnity	Added risk of alleged negligence or breach of duty as advice and/or services provided may make use of AI (insureds' own model or use of third-party models).
3	Product Liability	AI is being incorporated into physical products at an increasing rate, so in addition to existing risks are the risks of design issues relating to AI, including performance of the AI models used.
4	Cyber Liability	A heightened risk of more advanced, larger-scale cyber attacks from malicious use of AI, along with risk of data breach from AI models trained on large amounts of data.

	Insurance product	Impacts of AI
5	Workers Compensation	Changes to underlying risk of physical harm (e.g. increased use of robotics in manufacturing, or intensification/acceleration of pace of work due to increased surveillance via AI model) and psychological harm (e.g. lack of transparency and explainability of AI-based recommendations may cause anxiety and stress to workers), with flow-on impact to claims management and claims costs (Cebulla, Szpak, Knight, Howell, & Hussain, 2021). To date, the literature suggests that harm from AI systems seems more likely to impact workers psychologically than physically (Cebulla et al., 2021).
6	Motor	The direct impact of increased use self-driving technology, which includes AI systems, will likely be an increase in repair costs. A 2018 report from the American Automobile Association found that vehicles with advanced driver assistance systems can cost twice as much to repair following a collision due to expensive sensors and their calibration requirements (Edmonds, 2018). The risk profile will also change over time as semi-autonomous and autonomous vehicles account for a larger proportion of cars on the road. The impact on motor insurance relating to autonomous vehicles is still emerging, with questions remaining around attribution of liability (to the owner, manufacturer, or developer of the autonomous driving system) for injury or damages from an accident. Questions around negligence and product liability in these cases are complex and may vary significantly across jurisdictions.
7	Compulsory Third Party (CTP)	CTP provides cover for costs related to injuries sustained in motor accidents. An indirect impact of AI on CTP claims may emerge with changes in frequency of claims and severity of injuries as motor safety advances and autonomous vehicles become more mainstream.

4.2 Considerations for liability related classes

Section 4.1 provided a summary of the impacts of AI on existing lines of business. In this section, we take a more detailed look at the impact on the liability lines. Additional complexity arises because use of AI has immediate implications for establishment of liability, including determining what an appropriate level of duty of care is and proving negligence or a breach of that duty of care.

The components of liability

Liability insurance products provide coverage for instances where damages are claimed due to personal injury and/or financial loss, including loss arising from property damage. Core to these products then is establishment of liability for injury or financial loss, which generally requires three main conditions to be present to establish fault and/or negligence (Wright, 2022):

- **Duty of care** – the legal obligation of individuals and organisations to act reasonably and prudently to avoid causing harm to others
- **Breach of duty of care / proof of negligence** – the responsible individual or organisation fails to exercise reasonable care or acts negligently in their obligations
- **Causation** – a direct link is identified between the responsible party's breach of duty and the injury or damages suffered.

The main risk to insurers in the current environment relates to existing policies for liability products potentially providing coverage for harms relating to the use of AI, despite not specifically being designed to do so. This is referred to as *silent cover* for AI risks in existing insurance products, which we explore with consideration to the establishment of liability for four lines of business:

- Product Liability Insurance
- Professional Indemnity Insurance
- Directors and Officers Insurance
- Cyber Insurance.

Product Liability Insurance

For organisations involved in the production, supply or sale of products to members of the public, product liability insurance provides cover against claims of personal injury or property damage that a third party suffers as a result of the business's product.

Where AI is incorporated into physical products, cover for physical injury and third-party damage due to design defects related to AI may be available under product liability insurance policies. For example, cars, drones, household appliances and other products are increasingly using AI to make decisions.

Proving liability for AI-related harm in this area is challenging for individuals who have suffered harm. The large number of people involved in the design, development, deployment and operation of AI systems makes it difficult for plaintiffs to identify who is potentially liable for damage caused and to prove the conditions for a claim for damages (European Parliament, 2023), which is ultimately decided by courts. The EU has issued an AI Liability Directive in a bid to address this issue, which aims to make it easier for claims to be brought for harm caused by AI systems and the use of AI.

The EU Artificial Intelligence Liability Directive

On 28 September 2022, the European Commission released the proposal for an Artificial Intelligence Liability Directive (the Directive). The aim of the Directive is to introduce new rules specific to damages caused by AI systems, to ensure that persons harmed by AI systems enjoy the same level of protection as persons harmed by other technologies in the EU. The Directive applies to AI systems that are available on the EU market or operating within the EU market.

The AI Liability Directive complements the Artificial Intelligence Act. While the AI act aims to reduce risks for safety and fundamental rights, such rules do not prohibit AI systems posing a residual risk to safety and fundamental rights being placed on the market.

The effective timeframe for the proposal is uncertain – the proposal is still going through the EU legislative process. Once adopted by the EU, the Directive will need to be transposed into local law by member states to take effect.

Key provisions of the Directive

The two key elements of the Directive are:

- **Presumption of causation** – The Directive would create a rebuttable presumption of causation (if certain conditions are met) that gives claimants seeking compensation for damage caused by AI systems a more reasonable burden of proof. This means that if victims can show that someone was at fault for not complying with a certain obligation relevant to the harm, and that a causal link with the AI performance is reasonably likely, the court can presume that this non-compliance caused the damage. The liable person, on the other hand, can rebut such presumption (European Commission, 2022).
- **Disclosure of evidence** – National courts would have the power to order disclosure of evidence from developers of high-risk AI systems that are suspected of having caused damage. The claimant must present sufficient evidence to support the claim and make proportionate effort to obtain evidence from the defendant.

What the Directive means for insurers

The Directive ultimately aims to make it easier for claims to be brought for harm caused by AI systems and the use of AI (Stephenson Harwood, 2023).

It will be some time until the Directive becomes law, and would need to be enacted separately by member states. Insurers should monitor emerging developments to understand their exposure, particularly where exposure for silent cover may exist. In response, we anticipate tightening of policy wordings to make clear the circumstances in which coverage is being offered, potential affirmative coverage for AI risks, and underwriting and pricing changes.

The Directive will apply to developers outside the EU if their AI systems are sold to and accessible within the EU, so would apply to coverage for developers that sell into the European market.

Professional Indemnity Insurance

Professional Indemnity insurance provides cover for claims made for alleged negligence or breach of duty arising from an act, error or omission in the performance of the professional advice or service, for businesses that give professional advice or provide services.

Existing policies may already provide silent cover for advice or services provided that make use of AI, either with the insured's own models or use of a third-party AI models, as called out in the example below.

Example – An assessment of AI's impact on Legal Services Professional Liability (Cracknell & Felipe, 2023)

AI proves helpful for carrying out legal research, contract comparison, due diligence, FAQs, and increased access to legal services. However, there is no control over accuracy and the data is sourced using algorithms.

On the insured's part, any work produced by AI should undergo the same or greater scrutiny as work conducted by a trainee solicitor/junior lawyer. The use of AI does not remove the need for supervision and checking the quality and accuracy of the work.

For insurers, discussing how AI is employed, including the insured's policy, protocols, and controls, with underwriters is imperative. This not only raises awareness of potential exposure but also highlights risk mitigation through disciplined and effective technology utilisation.

Underwriters' concerns in AI usage are centred on professionals recklessly using chatbots which can result in inaccurate advice and wrongful professional acts.

The use of AI does not remove the need for supervision and checking the quality and/or accuracy of the work.

In practice, use and hygiene around nascent AI models will vary vastly across organisations. Monitoring use of AI by insureds is a critical first step to insurers being able to mitigate the risk.

Directors and Officers Insurance

Directors and Officers (D&O) Insurance provides personal liability coverage for company executives to protect them from claims which may arise from decisions and actions taken as part of their duties.

Directors' duty of care – *Corporations Act 2001*

Sections 180-181 of the Act require directors to perform their duties with care and diligence, in good faith and in the best interests of the corporation for a proper purpose. This includes a requirement for directors to be informed to the subject matter to judgements made.

Execution of these principles-based duties under the Corporations Act naturally extends to decision-making and management relating to use of AI by organisations.

Where AI is used in corporate decision-making, the risk emerges that claims may be made against business leaders for financial loss due to decisions or actions on their part that relied on advice from an AI model, where a breach of duty of care can be established.

With the increasing use of AI by organisations, monitoring of exposures related to AI risk is becoming more important for insurers. While the insurance industry has a strong risk management culture, insurers should recognise that standards in the other industries that their insureds' operate in may not share the same robust model risk management frameworks, and that exposure to AI risk may very quickly surpass an insurer's risk appetite.

The Professional Indemnity insurance example above discusses how insurers can engage with policyholders to understand and manage their exposure – the same considerations apply for D&O products too.

Cyber Insurance

Cyber insurance provides cover for a business's financial losses as a result of a cyber attack, which can include cover for a wide range of cyber related risks, such as financial losses for the business (first party cover), as well as losses suffered by third parties as a result of the incident (third party cover), along with costs of business interruption, system damage, ransom, etc.

Under existing cyber insurance policies, AI would potentially be treated as advanced software (i.e. similar treatment to other software). Cyber policies may provide cover for AI-related risk related to malicious attacks (data breaches, business interruption due to attack and privacy liability).

As AI continues to develop and advance, new types of cyber threats but also cyber defences are emerging (SecureOps, 2023). The development of AI has lowered barriers for less sophisticated hackers to do more harm, while more advanced hackers may harness the potential from AI to launch advanced attacks against networks, for example through advanced malware generation (Pearson, 2024). The risk of data breach is heightened too – while organisations may have robust data governance frameworks in place, there is uncertainty to the extent of protection built into AI models which may be trained on large amounts of data and the risk of data breach from within these models.

4.3 How insurers are starting to respond

Insurers are starting to define their strategy in response to the evolving landscape due to AI (AON, 2023) by:

- Clarifying coverage and addressing silent AI coverage through revised policy language related to AI risk
- Building out their underwriting requirements, but aware that the process has the potential to become onerous with the many potential applications that could be created and deployed
- Expanding their capability in AI organically and through partnerships and acquisitions to support underwriting and pricing through technical assessments and monitoring.

Insurers may also respond to emerging AI risks by offering AI insurance solutions to explicitly underwrite these risks. We discuss new product opportunities in the next section.

5 Insurance solutions for emerging AI risks

In the previous section, we discussed the impacts on existing lines of business from insureds' use of AI, and that strategies for insurers to respond to emerging AI risks.

In this section, we:

- Provide an overview of three new products in the market that provide cover for AI risk
- Explore new product opportunities for insurers and the key considerations developing these products:
  - We consider four potential new insurance products
  - We discuss the insurability of coverage for AI-related risk against insurability criteria
  - We note practical considerations for insurers when considering introduction of new products covering emerging AI risks, drawing out parallels with the development of cyber risk insurance.

5.1 Opportunities for insurers

The emerging impacts on insurance products due to AI present strategic opportunities for insurers to consider as they define their strategy in response. These include:

- **Carve-outs** – Insurers may choose to exclude coverage related to AI risk from existing products. For example, AON has made changes to some of their D&O coverage by augmenting definitions of key terms such as "Loss" and "Insured Person," and enhancing typical exclusionary language to carve back coverage for AI-related exposures (AON, 2024).
- **Riders** – Insurers looking to provide affirmative coverage for AI risks may do so through the addition of provisions to explicitly make this cover available within existing products.
- **New product opportunities** – Increasing development and use of AI coupled with growing concern of its risks creates a potential new market for insurers.
- **Bundles / packages** – Changes to existing products and the emergence of new products covering specific AI-related risks mean that insurers have enhanced ability to package and customise their offerings to customers, similar to how the cyber insurance offerings evolved.

We provide an overview of nascent product-warranty like cover and liability products for AI risk that have recently come to market in Section 5.2 and then explore new product opportunities in Section 5.3.

5.2 Examples of existing products

New products offering AI insurance or warranty-type products for AI models have recently come to market. Table 5.1 provides a snapshot of three AI insurance offerings.

Table 5.1 – Existing AI insurance products

Munich Re	Armilla AI	Vouch AI Vertical
Munich Re is a German multinational insurance company, and the world's largest reinsurer	Armilla AI is a startup founded in 2020, based in Toronto, Canada	Vouch is a US-based insurance provider founded in 2018, specialising in insurance for tech companies and startups
Liability product for AI developers/providers: an insurance-backed performance guarantee for AI models (aiSure), including coverage for damage caused For self-developed AI solutions, insurance against risk of model underperformance	Warranty product (Armilla Assurance) that covers the investment cost of the vendor's (insured's) customers should the AI model fail, providing protection against third-party AI risk. This warranty product is backed by SwissRe, Greenlight Re and Chaucer (Riehl, 2024) Audit product – Armilla also offers an automated AI auditing service to assess AI models for safety and trustworthiness	Liability product that provides cover for lawsuits associated with the insured's AI product, covering risks such as errors, discrimination, regulatory violations, intellectual property disputes, and can include cover for defence costs and damages, irrespective of fault

5.3 New product opportunities

A rapidly evolving technological environment for AI brings opportunities but also risks. A fast-changing regulatory landscape adds to the uncertainty for AI developers.

We explore the potential for new insurance products offering coverage for AI risks, and then weigh these against insurability criteria.

Algorithmic liability cover

In Section 2.3, we discussed a range of risks relating to use of AI models. Developers and users of models can employ several technical and procedural measures to mitigate these risks such as those discussed in Section 3.5, however residual risk of models not performing as intended remain.

An algorithmic liability insurance product provides coverage for liability to the developer of an AI model that arises when an AI model does not perform as required, resulting in injury or financial loss.

We explore opportunities and risks relating to the algorithmic liability product below, then discuss the main aspects of insurability for each product.

Opportunities	Risks
▪ A growing market – increasing use of AI in decision-making related to loan approval, health care, employment, etc. also means more exposure for developers and users of these systems to potential claims related to privacy and discrimination. AI risk awareness has grown (Munich Re, 2023a), and while regulatory changes will come to be implemented over time, liability products	▪ The risks discussed in 2.3 are all applicable in assessing model performance – if these materialise, then we essentially have deviations of model output from expected output. ▪ Where downstream applications make use of foundation models, the insured does not maintain the underlying AI model

Opportunities	Risks
offer an immediate solution for developers and users to gain confidence in using AI ▪ An increasing appetite to deploy AI coupled with persisting concern around accuracy may mean that organisations will look to insurance to mitigate some of the risk and grow their confidence in adopting AI. For example, a 2023 survey of over 2,500 business leaders found 98% of CEOs said there would be some immediate benefit to businesses from use of AI and ML, with 67% of CEOs saying potential errors are a top risk of AI and ML integration (Workday, 2023).	themselves and relies on the original model developer. This reliance also increases the level of concentration risk for insurers, especially if few foundational models are common across a large proportion of their insured book.

The relatively new products discussed in Section 5.1 demonstrate that there already is some appetite from insurers and reinsurers to provide coverage for algorithmic liability.

Intellectual Property infringement cover

Intellectual Property (IP) infringement relates to training of AI models on material that is copyright protected without permission and/or the generation of content by AI models that is similar to licensed material.

IP infringement – *Copyright Act 1968 (Cth)* and recent developments

Copyright provides legal protection for people who express ideas and information in an original way in certain forms such as writing, visual images, music and moving images (Attorney-General's Department, n.d.).

AI models trained on data that is protected by copyright laws, which may also produce outputs containing copyrighted material, are subject to liability for infringement where permission to use that data was not sought. There are also considerations around use of AI to create imitative works, particularly with the rapid increase in use of GenAI, and whether AI-generated work should receive copyright protection.

In December 2023, the Attorney General announced a copyright and artificial intelligence reference group to prepare for future copyright challenges emerging from AI (Dreyfus, 2023). The reference group will be a mechanism for the government to engage with stakeholders across a wide range of sectors (including creative, media, and technology sectors).

The legal landscape around copyright and GenAI is still in flux. For example, in December 2023, the New York Times sued OpenAI and Microsoft (Grynbaum & Mac, 2023) for copyright infringement, contending that millions of articles published by The Times were used to train automated chatbots that now compete with the news outlet as a source of reliable information. This case is still making its way through court. The application of law in this area is still developing as outcomes of this case and similar lawsuits emerge.

Intellectual Property coverage insurance would provide cover for developers of AI models and developers of systems relying on foundation models against damages relating to IP infringement.

Opportunities	Risks
▪ Legal uncertainties pose a market opportunity as companies look to limit exposure to liability relating to IP infringement. ▪ In 2023, Microsoft committed to pay for legal damages relating to AI copyright challenges on behalf of customers of its Copilot services. In early 2024, they extended this commitment to include coverage for their Azure OpenAI services (Microsoft, 2023). This sort of initiative from a developer like Microsoft may be indicative of concern in the market around IP infringement, and there may be a market and role for insurers to underwrite this risk in cases where developers do not offer a similar commitment, or in partnership with a developer.	▪ Uncertainty around appropriate use of copyrighted material as case law on this issue is still unresolved – we expect more lawsuits to emerge over time. ▪ Reliance on foundation models increases the level of concentration risk for insurers, especially if few foundational models are common across a large proportion of their insured book.

Regulatory compliance cover

As discussed in Section 3, the regulatory framework around AI is still developing, with a number of Australia's existing laws applicable to AI as would be any other technology, but with consideration also being given to the introduction of AI-specific laws and regulations where appropriate.

It is expected that regulation introduced to address harm related to AI will include penalties for non-compliance (for example, penalties for non-compliance under the EU AI Act can be up to the higher of €35m or 7% of annual turnover (European Parliament, 2023)). In addition, developers and users of AI should be alert to potential costs of brand damage if found to be non-compliant with regulations.

Regulatory compliance insurance would provide cover for the cost of penalties/fines from accidental non-compliance with government regulations, along with potential cover for reputational damage stemming from non-compliance and/or breach of regulations. This is a feature in some existing cyber policies. Moral hazard concerns are inherent in such a product, which we explore further below.

Opportunities	Risks
▪ Uncertainty around interpretation of compliance requirements relating to AI under the existing regulatory framework creates a market for an insurance product as companies look to manage this risk. ▪ Regulation of AI may include significant penalties, particularly for higher-risk AI applications, which companies may seek protection against.	▪ Regulatory/legislative uncertainty brings challenges around the extent of exposure for insurers in an environment where case law is still developing, and where laws in the home country and foreign markets that developers sell into need to be considered. ▪ Moral hazard and adverse selection could be elevated for a new line of business compared to mature classes, but can be managed through strict underwriting and risk assessment by the insurer.

Cover for liability to firms assessing AI models and providing assurance

Section 5.1 discusses Armilla AI's Assurance product which provides an assessment of AI models for safety and trustworthiness, ultimately offering a quality assurance certification for AI models sold by their customers.

Companies such as Armilla AI may be subject to liability claims for cases where the certified AI model is found to be non-compliant with their criteria or regulatory requirements.

We view these certification services as having relatively low barriers to entry, and as such the growth in AI, combined with significant mistrust in AI, has the potential to drive an increase in the number of companies offering similar certification. In turn, this could create a market for an insurance product that provides coverage for liability relating to cases where certified models fail in practice. This may take the form of standalone professional indemnity type cover for organisations that exclusively offer these services, or amendments to cover for organisations that offer broader services, such as audit firms.

Opportunities	Risks
▪ Despite the enthusiasm and growing adoption of AI, concerns around trust of AI remain. A 2023 survey found 61% of people to be wary of trusting AI (KPMG, 2023). Certification of AI models may emerge as a solution to build confidence in organisations and consumers, creating a market for a specialised version of professional indemnity cover.	▪ Low barriers to entry for certification services may mean a wide range of competence across insureds, with significant underwriting risk for insurers. ▪ Expertise to appropriately assess relative riskiness of insureds and price the product, as insurers will need an understanding of how AI is advancing and of how well-equipped insureds are to certify systems.

5.4 Practical considerations for new products

In addition to the opportunities and risks discussed in Section 5.3, we explore some of the practical considerations for insurers developing new products that provide cover for AI risk. We draw parallels with the development of cyber insurance products as similar uncertainties were often applicable to an immature cyber insurance market a few years ago.

Insurability

We assess the new product opportunities discussed in the section above against insurability criteria, drawing on the framework adopted by Khanna, Fannin and Wei (2021) shown in Table 5.2.

Table 5.2 – Insurability criteria

Insurability criteria			Requirements for insurability
Actuarial	1	Fortuitous loss	Timing and location of future events must be uncertain and accidental in timing and location
	2	Measurable	Losses must be well defined and verifiable upon occurrence
	3	Independent	There must be weak or no correlation within a portfolio of insureds
	4	Market-bearable	Maximum possible losses (per event) in an accident year from the insured event must not be excessive for insurance markets to absorb
	5	Predictable	Ideally, costs must be estimable, which requires a sufficient number of insureds across a sufficiently large number of historical events to be used as sample data
Economic	6	Fair	There should be no potential for *adverse selection* or *moral hazard* in the policy portfolio, and the contracts should not be unfairly discriminatory to individual insureds
	7	Affordable	The transfer price must be attractive to both the insurers and the insureds

Table 5.3 provides a summary of our assessment for each of the products discussed in Section 5.3, with the rationale for these assessments discussed in further detail below.

Table 5.3 – Assessment of insurability for coverage of AI risk

Insurability criteria	Assessment
1. Fortuitous loss	Not problematic
2. Measurable	Manageable
3. Independent	Problematic but manageable
4. Market-bearable	Manageable
5. Predictable	Problematic but manageable
6. Fair	Problematic but manageable
7. Affordable	To become increasingly less problematic

We discuss each criterion below:

1. **Fortuitous loss** – On randomness of individual loss events alone, we do not assess any material risk to the requirement not being met for future events to be uncertain and accidental.
2. **Measurable** – Challenges to satisfying the measurability criterion mainly relate to coverage where there may be uncertainty in quantifying losses incurred and defining whether there has been a claim event. Insurers can mitigate this risk with clear policy wording that specifies the conditions for the insured loss.

For example, algorithmic liability coverage products will require clear definitions of the criteria that is to be used to evaluate model performance (i.e. what would constitute a drop in model performance), and the damages covered where a loss event is defined. MunichRe's approach (Munich Re, 2024) to mitigating these risks includes:

- Developing a model evaluation pipeline with the insured (the model developers/providers)
- Tying model evaluation to specific tasks as model performance can differ materially for different tasks
- Clearly defining and agreeing to model performance metrics and thresholds.

3. **Independent** – A central requirement for providing insurance against a specific risk is the independence of those risks (Biener, Eling, & Wirfs, 2014). Correlation of risks across AI systems remains a significant risk, especially in cases where few foundation models are common across the insured book.

   For products that may insure GenAI applications such as IP infringement cover, satisfying the independence criterion can be particularly challenging – however insurers can mitigate this risk by defining conditions around monitoring of and linking coverage to performance of foundation models.

   For example, where the insured's AI models rely on foundation models, MunichRe requires higher standards of continuous monitoring and model improvement from the insured, and further considers contract conditions that pause the insurance guarantee and/or adjust the coverage and premium in line with fluctuating exposure as performance of the foundation model varies (Munich Re, 2024).

4. **Market-bearable** – Excessive per-event loss exposure can be managed through policy limits for damages paid, agreed sums insured and contract conditions.

5. **Predictable** – For new lines of business covering AI risk, historical data is limited, and accelerating developments in AI mean that the data too may quickly become outdated. While such an environment makes meeting the predictability criterion challenging, insurers may be guided by approaches employed in developing cyber insurance products to manage this risk – initial cyber products were offered with limited coverage to enable evaluation of risk as experience emerged, and data was shared between partners/clients to gain more insight of the underlying risk.

6. **Fair** – *Adverse selection* refers to demand for insurance from higher-risk applicants, mostly due to information asymmetry between the insurer and applicant. The risk of adverse selection has been prevalent in many established insurance products (for example, riskier drivers in motor insurance). We assess this risk for AI risk insurance products as similarly manageable to other mature lines of business through appropriate pricing and underwriting practices.

   Moral hazard results from the insured's lack of incentive to take self-protective measures that would reduce the probability of loss or the size of a loss once it happened subsequent to purchasing insurance (Biener, Eling, & Wirfs, 2014). Comprehensive risk assessment at policy inception and renewal, clear underwriting criteria to assess risks and use of policy conditions and limits are used by insurers to mitigate this risk.

7. **Affordable** – assessment of affordability for a very new class of business is inherently difficult and subjective. Early cyber insurance products were often described as too costly due to early novelty of the product translating to a small risk pool, limited market participants, large risk loadings to premiums due to limited data and information asymmetry causing costly verification and upfront risk assessment (Biener, Eling, & Wirfs, 2014). We think that largely the same considerations apply to insurance of AI risk, and similar to cyber insurance, affordability should improve as the market grows.

Capital

APRA's capital requirements are intended to reflect the risk borne by regulated entities. For insurers, this means risks relating to variability in estimated insurance claims, and also risk related to variability in the value of assets.

The nature of insuring AI risk is inherently volatile – this is a nascent line of business with significant opacity and information asymmetry between insurers and insureds. As such, first movers in this market may be organisations with large capital bases (e.g. reinsurers) and organisations with broad risk appetites (e.g. Lloyd's syndicates). Of the three new products discussed in Section 5.3, two have direct reinsurer involvement (Munich Re) or reinsurer backing (Armilla warranty product backed by Swiss Re and others).

Product design and underwriting

Practical considerations around product design and underwriting of nascent liability and warranty products offering coverage for AI related risks include:

- **Policy wording**: For a new line of business, the insurers' strategy may be to initially offer limited coverage, allowing evaluation of risk as experience emerges and then deciding on whether to expand their offering. This was a consideration for early cyber policies too, as discussed under the '*predictable*' insurability criterion above. To successfully achieve this, insurers need to ensure policy wordings are clear and conditions of loss are clearly defined.
- **Limited data availability and a fast-evolving risk profile**: May dampen insurer appetite to underwrite cover for AI-related risk. The sentiment for cyber risk products a few years ago was similar – at the time, insufficient data was seen to undermine insurer confidence in underwriting and pricing, prompting insurers to offer modest limits and restricted coverage (Friedman & Thomas, 2017). Similar concerns could emerge for insurance of AI risk, with relatively few products coming to market thus far, but with significant potential for future growth.
- **Onerous underwriting and tailored products**: Similar to the offering from MunichRe (Munich Re, n.d.), we anticipate early products will be heavily tailored to each client, with significant cost incurred in understanding the AI models being developed and assessing the insurance risk. Cyber offerings continue to vary materially across insurers (Granato & Polacek, 2019) and clients – we anticipate this trend to reflect similarly in AI insurance products, with potential for standardization across products as the market matures.
- **Expertise of the underwriting team** is critical to insurers being able to appropriately evaluate and price policies. Specialist knowledge is required to effectively underwrite and manage claims (Landers & Rogers, 2024).

The role of standards

In Section 3.4 we discussed the ISO/IEC 42001 AI management system standard. Certification for meeting this standard may be used by insurers as an indicator of the robustness of an insured's systems and processes around their AI systems. Insurers may use certification as criteria for risk assessment in underwriting, which has the potential to reduce some the onerous risk assessment work that insurers would do themselves when underwriting these policies. This would echo the use of ISO 27001 in underwriting cyber insurance policies.

Pricing

Pricing of AI insurance products is constrained by limited availability for a new and fast-evolving line of business. Approaches to drive success in a similar environment for cyber risk include collaboration with clients and partners to share data and risk insights (Munich Re, 2023b), and strategically working to improve quality and quantity of data on exposures, trends and losses over time.

The insurance premium will likely also factor in robustness of the insured's AI model (Munich Re, 2024), type of AI technology used, industry the insured operates in, size of the insured, etc. A limited loss history means that insurers will likely rely on indirect factors for their pricing, for example market estimates of the cost of model failure, questionnaires to determine the riskiness of the insured, their own (often limited) underwriting experience, and pricing by other insurers (Granato & Polacek, 2019).

Claims assessment and management

Handling AI risk claims may be quite different to traditional lines. Insurers should consider the expertise required in claims assessment and management. Legal expertise in managing claims must also be considered as the regulatory landscape, both locally and globally, evolves and case law emerges.

Accumulation of losses

Insurers need to be cognizant of accumulation stemming from underlying foundation models employed by policyholders in their models and/or processes. In cases where few foundational models are common across a large proportion of the insured book, there is significant concentration risk, and potential for a catastrophe-like claims scenario. Accumulation can also materialise if a large proportion of insureds' models depend on few open source libraries – for example, in 2023, the popular PyTorch package was compromised by a malicious attack (Burt, 2023).

Drawing a parallel to cyber insurance, a related example would is failure of a large cloud computing platform used by a large proportion of policyholders (Granato & Polacek, 2019),. This encouraged cyber insurers to write policies that limited the amount of coverage, as well as the risks that were insured.

Insurers will need a clear understanding of their risk appetite, and regularly monitor exposures and insurability of products offered for potential accumulation.

Reinsurance

Two of the three existing AI insurance products discussed in Section 5.1 have significant reinsurer involvement – MunichRe directly underwrites their AI insurance offering, and three reinsurers are backing the warranty product offered by Armilla AI.

Reinsurers may drive the initial growth in AI insurance, in a similar way to their role in the cyber insurance market. S&P in 2021 estimated that 35% to 45% of global cyber premium was passed to reinsurers, with insurers relying on them for their expertise in managing potential accumulation risk and exposure to cyber risk. Their survey of global multiline insurers and reinsurers suggested that growth in cyber insurance will depend heavily on reinsurance to provide capital and manage accumulation risk (S&P, 2021).

Reinsurers will also have the scope to absorb losses from a small AI risk portfolio within a diversified overall portfolio.

6 Conclusion

The use and development of AI is expanding rapidly. AI presents an abundance of opportunities, but also comes with risks.

The regulatory and legislative framework around AI is evolving. Insurers should be aware of provisions already existing in legislation, and may draw on existing standards and governance standards to guide their ethical and responsible use of AI.

Insurers have a role to play in supporting the growth in AI and managing the emerging risks. Underwriting AI risks enhances the resilience of industry, and insurers may promote ethical and responsible adoption of AI as they engage with insureds through underwriting, monitoring and claims management processes.

Considerations for insurers include:

- Updating risk management frameworks to appropriately manage risks relating to the use of AI and ensure compliance with regulatory/legislative requirements across the organisation
- The implications of a changing risk profile on existing lines of business, including complex changes to liability risk where there is an interaction with AI
- New product opportunities to offer cover for emerging AI risk.

7 References

ABS. (2023, June). *Lawyers in the United States blame ChatGPT for tricking them into citing fake court cases.* Retrieved from ABS.

ACCC. (n.d.). *Insurance.* Retrieved from Australian Competition & Consumer Commission: https://www.accc.gov.au/by-industry/insurance

Actuaries Institute. (2023, July). *Response to Department of Industry, Science and Resources - Supporting Responsible AI Discussion Paper.* Retrieved from https://www.actuaries.asn.au/Library/Submissions/2023/2320725SubDoISRAI.pdf

Allianz. (2023, November). How AI could change insurance. *Global Risk Dialogue - 02/2023.* Retrieved from Allianz: https://commercial.allianz.com/news-and-insights/expert-risk-articles/AI.html

Andrews, M., & Bartlett, A. (2024). *Insurance & Reinsurance Laws and Regulations Australia.* Retrieved from ICLG: https://iclg.com/practice-areas/insurance-and-reinsurance-laws-and-regulations/australia

AON. (2023, November). *Generative AI: Emerging Risks and Insurance Market Trends.* Retrieved from AON: https://www.aon.com/en/insights/articles/how-is-the-insurance-market-responding-to-generative-ai

AON. (2024, April). *The Growing Use of Artificial Intelligence: D&O Risks and Potential Coverage Solutions.* Retrieved from AON: https://www.aon.com/risk-services/financial-services-group/the-growing-use-of-artificial-intelligence-d-and-o-risks-and-potential-coverage-solutions

APRA. (2019, July). *Prudential Standard CPS 220 Risk.* Retrieved from Australian Prudential Regulation Authority: https://www.apra.gov.au/sites/default/files/cps_220_risk_management_effective_from_1_july_2019.pdf

APRA. (2023). *APRA Corporate Plan 2023-24.* Retrieved from APRA: https://www.apra.gov.au/apra-corporate-plan-2023-24

Armilla AI. (n.d.). Retrieved from Armilla AI: https://www.armilla.ai/

ASIC. (2023, August). *Corporate Plan 2023-27.* Retrieved from ASIC: https://download.asic.gov.au/media/2cshqbxb/asic-corporate-plan-2023-27-focus-2023-24-published-28-august-2023.pdf

Attorney-General's Department. (n.d.). *Australia's anti-discrimination law.* Retrieved from Australian Government, Attorney-General's Department: https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/australias-anti-discrimination-law

Attorney-General's Department. (n.d.). *Copyright.* Retrieved from Australian Government, Attorney-General's Department: https://www.ag.gov.au/rights-and-protections/copyright

Australian Government. (2023). *Supporting responsible AI: discussion paper.* Retrieved from Australian Government, Department of Industry, Science and Resources: https://consult.industry.gov.au/supporting-responsible-ai

Australian Government. (2024). *Australian Government's interim response.* Retrieved from Safe and responsible AI in Australia consultation: https://storage.googleapis.com/converlens-au-industry/industry/p/prj2452c8e24d7a400c72429/public_assets/safe-and-responsible-ai-in-australia-governments-interim-response.pdf

Biener, C., Eling, M., & Wirfs, J. (2014, August). *Insurability of Cyber Risk: An Empirical Analysis.* Retrieved from The Geneva Association: https://www.internationalinsurance.org/sites/default/files/2018-03/Insurability%20of%20Cyber%20Risk.pdf

Burt, J. (2023, January). *PyTorch dependency poisoned with malicious code.* Retrieved from The Register: https://www.theregister.com/2023/01/04/pypi_pytorch_dependency_attack/

Cebulla, A., Szpak, Z., Knight, G., Howell, C., & Hussain, S. (2021). *Ethical use of artificial intelligence in the workplace.* NSW Government Centre for Work Health and Safety, The University of Adelaide, Flinders University.

Chng, D. G., & Jones, J. (2024, February). *Global AI Governance Law and Policy: Singapore.* Retrieved from iapp: https://iapp.org/resources/article/global-ai-governance-singapore/

Cohen, J., & Wood, S. (2023, October). *How AI is transforming insurance.* Retrieved from Taylor Fry: https://taylorfry.com.au/articles/how-ai-is-transforming-insurance/

Cracknell, J., & Felipe, R. (2023, October). *Navigating AI risks in Professional Liability*. Retrieved from WTW: https://www.wtwco.com/en-au/insights/2023/10/navigating-ai-risks-in-professional-liability

CSIRO. (n.d.). *Responsible AI Pattern Catalogue.* Retrieved from CSIRO: https://research.csiro.au/ss/science/projects/responsible-ai-pattern-catalogue/

Dahl, M., Magesh, V., Suzgun, M., & Ho, D. E. (2024, January). *Hallucinating Law: Legal Mistakes with Large Language Models are Pervasive.* Retrieved from Stanford University: https://hai.stanford.edu/news/hallucinating-law-legal-mistakes-large-language-models-are-pervasive

Department of Industry, Science and Resources. (2019, November). *Australia's Artificial Intelligence Ethics Framework.* Retrieved from Australian Government, Department of Industry, Science and Resources: https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-framework/australias-ai-ethics-principles

Digital.NSW. (n.d.). *A common understanding: simplified AI definitions from leading standards.* Retrieved from NSW Government: https://www.digital.nsw.gov.au/policy/artificial-intelligence/a-common-understanding-simplified-ai-definitions-from-leading

Dreyfus, M. (2023, December). *Copyright and AI reference group to be established.* Retrieved from Attorney-General's portfolio: https://ministers.ag.gov.au/media-centre/copyright-and-ai-reference-group-be-established-05-12-2023

Edmonds, E. (2018, October). *New Vehicle Technologies Double Repair Bills for Minor Collisions.* Retrieved from Newsroom: https://newsroom.aaa.com/2018/10/new-vehicle-technologies-double-repair-bills-minor-collisions/

Emerging Technology from the arXiv. (2015, September). *King – Man + Woman = Queen: The Marvelous Mathematics of Computational Linguistics.* Retrieved from MIT Technology Review: https://www.technologyreview.com/2015/09/17/166211/king-man-woman-queen-the-marvelous-mathematics-of-computational-linguistics/

EU AI Act. (n.d.). *Annex III - High-Risk AI Systems Referred to in Article 6(2).* Retrieved from EU Artifical Intelligence Act: https://artificialintelligenceact.eu/annex/3/

European Commission. (2022, September). *Questions & Answers: AI Liability Directive.* Retrieved from European Commission: https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_5793

European Parliament. (2023, December). *Artificial Intelligence Act: deal on comprehensive rules for trustworthy AI.* Retrieved from European Parliament: https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

European Parliament. (2023, February). *Artificial intelligence liability directive.* Retrieved from BRIEFING: EU Legislation in Progress: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/739342/EPRS_BRI(2023)739342_EN.pdf

Ferrara, E. (2023). Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies. p. https://arxiv.org/ftp/arxiv/papers/2304/2304.07683.pdf.

Friedman, S., & Thomas, A. (2017). *Demystifying cyber insurance coverage: Clearing obstacles in a problematic but promising growth market.* Retrieved from Deloitte Centre for Financial Services: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/financial-services/deloitte-nl-fsi-demystifying-cyber-insurance-coverage-report.pdf

Gallagher Bassett. (n.d.). *Insurance personalisation for today's policyholders.* Retrieved from Gallagher Bassett: https://blog.gallagherbassett.com.au/blog/insurance-personalisation-for-todays-policyholders

Government of the Republic of Singapore. (2023, December). *NAIS 2.0 Singapore National AI Strategy.* Retrieved from Government of the Republic of Singapore: https://file.go.gov.sg/nais2023.pdf

Government of the Republic of Singapore. (2023). *NAIS 2.0 Singapore National AI Strategy*. Retrieved from Government of the Republic of Singapore: https://file.go.gov.sg/nais2023.pdf

Granato, A., & Polacek, A. (2019). *The Growth and Challenges of Cyber Insurance.* Retrieved from Federal Reserve Bank of Chicago: https://www.chicagofed.org/publications/chicago-fed-letter/2019/426

Grynbaum , M. M., & Mac, R. (2023, December). *The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work.* Retrieved from The New York Times: https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html

ISO. (2023, February). *ISO/IEC 23894:2023.* Retrieved from International Organization for Standardization: https://www.iso.org/standard/77304.html

ISO. (2023, December). *ISO/IEC 42001:2023.* Retrieved from International Organization for Standardization: https://www.iso.org/standard/81230.html

ISO. (n.d.). *Structure and governance.* Retrieved from International Organization for Standardization: https://www.iso.org/structure.html

Joe Longo. (2024, January). *We're not there yet: Current regulation around AI may not be sufficient.* Retrieved from ASIC: https://asic.gov.au/about-asic/news-centre/speeches/we-re-not-there-yet-current-regulation-around-ai-may-not-be-sufficient/

Khanna, A., Fannin, B. A., & Wei, T. (2021). *On Insurability and Transfer of Pandemic Business Interruption Risk.* Retrieved from CAS Research Brief: https://www.casact.org/sites/default/files/2021-04/Research-Brief-Uninsurable-Risks.pdf

KPMG. (2023). *Trust in artificial intelligence, 2023 Global study on the shifting public perceptions of AI.* Retrieved from KPMG: https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/09/trust-in-ai-global-study-2023.pdf

Landers & Rogers. (2024, March). *Cyber insurance trends to look out for in 2024 and beyond.* Retrieved from Landers & Rogers: https://www.landers.com.au/legal-insights-news/cyber-insurance-trends-to-look-out-for-in-2024-and-beyond

Laney, D. B. (2023, November). *AI Ethics Essentials: Lawsuit Over AI Denial of Healthcare.* Retrieved from Forbes: https://www.forbes.com/sites/douglaslaney/2023/11/16/ai-ethics-essentials-lawsuit-over-ai-denial-of-healthcare/?sh=13fe5a743ac6

Langone, A. (2021, November). *What happened at Zillow? How a prized real estate site lost at iBuying.* Retrieved from CNET: https://www.cnet.com/personal-finance/mortgages/what-happened-at-zillow-how-a-prized-real-estate-site-lost-at-ibuying/

Microsoft. (2023, September). *Microsoft announces new Copilot Copyright Commitment for customers.* Retrieved from Microsoft: https://blogs.microsoft.com/on-the-issues/2023/09/07/copilot-copyright-commitment-ai-legal-concerns/

Mikolov, T., Sutskever, I., Chen, K., Corrado, G. S., & Dean, J. (n.d.). Distributed Representations of Words and Phrases and their Compositionality. *Advances in Neural Information Processing Systems 26 (NIPS 2013)*.

Munich Re. (2023a). *How Munich Re Assesses AI Performance Risks - Insights Into Our Due Diligence Process.* Retrieved from https://www.munichre.com/content/dam/munichre/contentlounge/website-pieces/documents/MunichRe-De-Risking-AI-Ventures-Whitepaper.pdf/_jcr_content/renditions/original./MunichRe-De-Risking-AI-Ventures-Whitepaper.pdf

Munich Re. (2023b). *Cyber insurance: Risks and trends 2023.* Retrieved from Munich Re: https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.html

Munich Re. (2024). *Insuring Generative AI: Risks and Mitigation Strategies, Balancing creativity and responsibility to enable adoption.* Retrieved from Munich Re: https://www.munichre.com/en/solutions/for-industry-clients/insure-ai/ai-whitepaper.html

Munich Re. (n.d.). *Insure AI.* Retrieved from Munich Re: https://www.munichre.com/en/solutions/for-industry-clients/insure-ai.html

Neill, B., Hallmark, J. D., Jackson, R. J., & Diasio, D. (2023, October). *Key takeaways from the Biden administration executive order on AI.* Retrieved from EY: https://www.ey.com/en_us/public-policy/key-takeaways-from-the-biden-administration-executive-order-on-ai

NSW Government. (2022, March). *NSW Artificial Intelligence Assurance Framework.* Retrieved from NSW Government: https://www.digital.nsw.gov.au/policy/artificial-intelligence/nsw-artificial-intelligence-assurance-framework

OECD. (2019). *OECD AI Principles overview.* Retrieved from OECD: https://oecd.ai/en/ai-principles

Olavsrud, T. (2023, September). *9 famous analytics and AI disasters.* Retrieved from CIO: https://www.cio.com/article/190888/5-famous-analytics-and-ai-disasters.html

OpenAI. (2024, January). *OpenAI and journalism.* Retrieved from OpenAI: https://openai.com/blog/openai-and-journalism

Parliament of Australia. (2024). *Select Committee on Adopting Artificial Intelligence (AI).* Retrieved from Parliament of Australia: https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Adopting_Artificial_Intelligence_AI

Pearson, J. (2024, January). *AI rise will lead to increase in cyberattacks, GCHQ warns.* Retrieved from Reuters: https://www.reuters.com/technology/cybersecurity/ai-rise-will-lead-increase-cyberattacks-gchq-warns-2024-01-24/

Productivity Commission. (2024). Making the most of the AI opportunity. *Research paper 2 - The challenges of regulating AI.*

Ravin AI. (n.d.). *Solutions - AI Insurance Claims and Underwriting System.* Retrieved from Ravin: https://www.ravin.ai/solutions-insurance-claims

Riehl, A. (2024, February). *Y Combinator and Yoshua Bengio-backed Armilla AI secures $6 million cad in new funding.* Retrieved from Betakit: https://betakit.com/y-combinator-and-yoshua-bengio-backed-armilla-ai-secures-6-million-cad-in-new-funding/

Roser, M. (2022, December). *The brief history of artificial intelligence: The world has changed fast – what might be next?* Retrieved from Our World In Data: https://ourworldindata.org/brief-history-of-ai

S&P. (2021, September). *Cyber Risk In A New Era: Reinsurers Could Unlock The Cyber Insurance Market.* Retrieved from S&P Global Ratings: https://www.spglobal.com/ratings/en/research/articles/210929-cyber-risks-in-a-new-era-reinsurers-could-unlock-the-cyber-insurance-market-12118547

SecureOps. (2023, September). *The Use of Artificial Intelligence in Cyber Attacks and Cyber Defense.* Retrieved from SecureOps: https://secureops.com/blog/ai-offense-defense/

Singapore PDPC. (2020a). *Model Artificial Intelligence Governance Framework, Second Edition.* Retrieved from Singapore Personal Data Protection Commission: https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

Singapore PDPC. (2020b). *Singapore's Approach to AI Governance.* Retrieved from Singapore Personal Data Protection Commission: https://www.pdpc.gov.sg/help-and-resources/2020/01/model-ai-governance-framework

Solomon, L., & Davis, N. (2023). *The State of AI Governance in Australia.* UTS Human Technology Institute. Retrieved from https://www.uts.edu.au/human-technology-institute/news/report-launch-state-ai-governance-australia

Stephenson Harwood. (2023, June). *EU Artificial Intelligence Liability Directive.* Retrieved from Stephenson Harwood: https://www.shlegal.com/insights/eu-artificial-intelligence-liability-directive

Stokel-Walker, C. (2021, November). *Why Zillow Couldn't Make Algorithmic House Pricing Work.* Retrieved from WIRED: https://www.wired.com/story/zillow-ibuyer-real-estate/

Surfshark. (2023, June). *The start of this decade marks a sharp rise in AI incidents.* Retrieved from Surfshark: https://surfshark.com/research/chart/statistics-of-ai-incidents

Swiss Re. (2024). *Swiss Re's Magnum: Automated underwriting platform.* Retrieved from Swiss Re: https://taylorfry.com.au/articles/how-ai-is-transforming-insurance/

The White House. (2023, October). *FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.* Retrieved from The White House: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

The White House. (2024, March). *FACT SHEET: Vice President Harris Announces OMB Policy to Advance Governance, Innovation, and Risk Management in Federal Agencies' Use of Artificial Intelligence.* Retrieved from The White House: https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/28/fact-sheet-vice-president-harris-announces-omb-policy-to-advance-governance-innovation-and-risk-management-in-federal-agencies-use-of-artificial-intelligence/

UK Department for Science, Innovation & Technology. (2024, February). *A pro-innovation approach to AI regulation: government response.* Retrieved from UK Department for Science, Innovation & Technology: https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response

UK Information Commissioner's Office. (2024, January). *ICO consultation series on generative AI and data protection.* Retrieved from UK Information Commissioner's Office: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-series-on-generative-ai-and-data-protection/

US NIST. (n.d.). *AI Risk Management Framework.* Retrieved from US National Institute of Standards and Technology: https://airc.nist.gov/AI_RMF_Knowledge_Base/AI_RMF

US NIST. (n.d.). *Trustworthy and responsible AI.* Retrieved from US National Institute of Standards and Technology: https://www.nist.gov/trustworthy-and-responsible-ai

Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., . . . Polosukhin, I. (2017). Attention Is All You Need. *31st Conference on Neural Information Processing Systems (NIPS 2017).* Long Beach.

Vouch. (n.d.). Retrieved from Vouch: https://www.vouch.us/verticals/ai

Workday. (2023). *C-Suite Global AI Indicator Report: AI is the Ultimate Level-Up.* Retrieved from Workday: https://forms.workday.com/en-au/reports/indicator-to-the-digital-future-with-ai-and-ml-sngl/form.html?step=step1_default

Wright, B. (2022, July). *Negligence, liability and damages.* Retrieved from The Law Handbook: https://fls.org.au/law-handbook/accidents-insurance-and-compensation/negligence-and-injury/negligence-liability-and-damages/